ArubaOS 8.0.1.0

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
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Contents

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 description of 156755.
Revision 03	Added the list of APs that support MutiZone.
Revision 02	Updated symptom of bugs 151740 and 151906, added workaround for bugs 152148 and 152252, and added description of bug 151915
Revision 01	Initial release.

This release of ArubaOS includes fixes to issues identified in previous releases.

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

Use the following links to navigate to the corresponding topics:

- New Features and Enhancements on page 8 describes the new features and enhancements introduced in this release.
- Supported Hardware Platforms on page 15 describes the hardware platforms supported in this release.
- Regulatory Updates on page 17 lists the regulatory updates in this release.
- Resolved Issues on page 18 lists the issues resolved in this release.
- Known Issues on page 25 lists the issues identified in this release.
- Upgrade Procedure on page 33 describes the procedures for upgrading your WLAN network to the latest ArubaOS version.

Related Documents

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

- *ArubaOS Release Notes*
- *ArubaOS Quick Start Guide*
- *ArubaOS User Guide*
- *ArubaOS CLI Reference Guide*
- *ArubaOS API Guide*
- *ArubaOS 8.x Syslog Message Guide*
- *Aruba Mobility Master Licensing Guide*
- *Aruba Mobility Master and VMC Installation Guide*
- *Aruba Wireless Access Point Installation Guide*

Supported Browsers

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

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10
- Firefox 48 and higher on Windows 7, Windows 8, Windows 10 and Mac OS
- Apple Safari 8.0 or later on Mac OS
- Google Chrome

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	hpe.com/networking/support
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: sirt@arubanetworks.com

This chapter describes the features and/or enhancements introduced in ArubaOS 8.0.1.0 release.

AirMatch and ClientMatch RF Management

AirMatch WebUI Changes

In ArubaOS 8.0.1.0, the AirMatch WebUI is located in the **Configuration > Services > AirMatch** page of the Mobility Master WebUI. This is a change from ArubaOS 8.0.0.0, where the AirMatch WebUI is located in the **Configuration > Services > More > AirMatch** page.

ClientMatch WebUI Changes

ArubaOS 8.0.1.0 introduces a new WebUI page to upload a custom Client-Match rule update package. Starting with ArubaOS 8.0.1.0, you must upload a ClientMatch rule update package via the **Diagnostics > Technical Support > Client Match Rules** page of the Mobility Master WebUI. This is a change from ArubaOS 8.0.0.0, where ClientMatch rule packages are uploaded via the **Configuration > Services > More > ClientMatch** page.

Improved AirMatch Channel Assignment Logic

In ArubaOS 8.0.0.0, AirMatch moved a radio to a random channel when a radar event was detected, or if a high noise floor was detected on a non-static channel. Starting with ArubaOS 8.0.1.0, AirMatch introduces improved channel assignment logic if a radar or high noise level event triggers a channel change.

Table 3: *Channel Assignment Logic in ArubaOS 8.0.1.0*

Issue Prompting Channel Change	Channel Selection Criteria
Detected radar	AirMatch selects a channel with a minimum interference index from the channels without high noise or a radar condition.
High channel noise	The channel selection criteria varies between static and non-static channels. • If static channel is configured, the channel does not change due to a high noise condition. • For a non-static channel, AirMatch selects a channel with a minimum interference index from the channels without high noise or a radar condition.

Quality Improvement Thresholds for AirMatch Scheduled Updates

ArubaOS 8.0.1.0 introduces the AirMatch channel quality improvement threshold, which allows you to select the minimum channel improvement that can trigger a new scheduled channel solution. The default threshold value is a 15% improvement. If a proposed channel change will not produce an improvement that meets or exceeds this threshold, AirMatch will not trigger a channel change.

This channel quality setting only applies to scheduled updates. If you manually trigger an update using the **airmatch runnow** command, AirMatch will deploy the new solution regardless of the level of improvement.

AP-Platform

Support for 310 Series Access Points

The 310 Series (AP-314 and AP-315) access points support IEEE 802.11ac standards for a high-performance WLAN. This device is equipped with two single-band radios, which provide network access and monitor the network simultaneously. This access point can deliver high-performance 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while also supporting 802.11a/b/g wireless services. Multi-User Multiple-Input Multiple-Output (MU-MIMO) is enabled when operating in 5 GHz mode for optimal performance. The 310 Series access points work in conjunction with a managed device.

The 310 Series access points provide the following capabilities:

- IEEE 802.11a/b/g/n/ac wireless access point
- IEEE 802.11a/b/g/n/ac wireless air monitor
- IEEE 802.11a/b/g/n/ac spectrum monitor
- Compatible with IEEE 802.3at and 802.3af PoE
- Support for MCS8 and MCS9
- Centralized management, configuration, and upgrades
- Integrated Bluetooth Low Energy (BLE) radio

For more information, see the *310 Series Access Point Installation Guide*.

Support for 330 Series Access Points

The 330 Series (AP-334 and AP-335) access points support IEEE 802.11ac standards for high-performance WLAN. This device is equipped with two dual-band radios, which provide network access and monitor the network simultaneously. This access point delivers high-performance 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while also supporting 802.11a/b/g wireless services. Multi-User Multiple-Input Multiple-Output (MU-MIMO) is enabled when operating in 5 GHz mode for optimal performance. The 330 Series access points work in conjunction with a managed device.

The 330 Series access points provides the following capabilities:

- IEEE 802.11a/b/g/n/ac wireless access point
- IEEE 802.11a/b/g/n/ac wireless air monitor
- IEEE 802.11a/b/g/n/ac spectrum monitor

- Compatible with IEEE 802.3at power sources
- Centralized management, configuration, and upgrades
- Integrated Bluetooth Low Energy (BLE) radio

For more information, see the *330 Series Access Point Installation Guide*.

Configuration

Change Configuration Node using Hostname of Managed Device

ArubaOS 8.0.1.0 allows a user to change the configuration node by using the hostname of the managed device. Device name aliasing allows the use of aliased hostname in commands which use node-path as argument.

Seamless Login to Managed Device

ArubaOS 8.0.1.0 allows a user to log in to a managed device without requiring username and password after logging in to the Mobility Master. After logging in to the managed device, a user can execute only show commands.

Controller-Platform

7200 Series Master Controller Mode

ArubaOS 8.0.1.0 supports 7200 Series controllers to run as a master controller. In this mode, you can retain the existing ArubaOS 6.x master-local architecture and migrate to ArubaOS 8.x. Services like AirGroup, AppRF, ARM, NBAPI, UCM, WebCC, and WMS will remain distributed across managed devices. All features in ArubaOS 6.5.x and ArubaOS 8.x are supported in this mode, except the following:

- AP termination on the master controller
- Loadable Service Module
- AirMatch
- Cluster
- North-bound API
- Multi-version ArubaOS support
- Centralized visibility
- IP reputation and geo-location
- Centralized licensing domain
- Seamless logon

To gain access to these features, replace the master controller with Mobility Master.

.

IPFIX

IPFIX Enhancements

Starting with ArubaOS 8.0.1.0, IPFIX supports wireless export. When wireless export is enabled, a new template is defined to gather and export information about wireless clients, in addition to the standard attributes exported through the existing, pre-defined template.

Licensing

Changes to the Virtual Mobility Controller License

Starting with ArubaOS 8.0.1.0, the Virtual Mobility Controller (VMC) license is a sharable license required to terminate APs on a VMC. In ArubaOS 8.0.0.0, the VMC license is a non-sharable license required to install ArubaOS as a controller on a VM.

Mobility Master License Enforcement

Starting with ArubaOS 8.0.1.0, The Mobility Master license is required to terminate devices (managed devices or APs) on Mobility Master. If Mobility Master has more associated managed devices and APs than its Mobility Master license capacity, the managed devices will have higher priority access to the MM license than the APs.

Per-Device License Usage Statistics

In ArubaOS 8.0.1.0, the Global License Pool table and the output of the show license-usage client verbose command displays license usage statistics for each configuration pool, as well as the license usage for the devices associated to those license pools. In ArubaOS 8.0.0.0, the Global license pool table and the show license-usage client does not display license usage data at the device level.

Serial Number not Required to Generate Mobility Master or VMC License

Starting with ArubaOS 8.0.1.0, a VM serial number is not required to generate a Mobility Master or VMC license. This is a change from ArubaOS 8.0.0.0, as a Mobility Master or virtual managed device running ArubaOS 8.0.0.0 *does* require a serial number to generate a Mobility Master or VMC license via the licensing website.

Use the Mobility Master passphrase in the licensing website to generate a Mobility Master license, or to generate a sharable license that can be added to Mobility Master license pools. To identify the Mobility Master passphrase, access Mobility Master via the command-line interface and issue the command **show license passphrase**.

Stand-alone Controllers Configurable as Licensing Clients

ArubaOS 8.0.1.0 allows you to configure a stand-alone controller as a licensing client. You can associate a stand-alone license client with an external license server via the **Connect to external license server** option on the **Configuration > System > Licensing** page of the WebUI, or via the **license server-ip** command in the command-line interface.

Security

Device Type Classification

ArubaOS 8.0.1.0 is integrated with the ClearPass Policy Manager Insight server to enhance device type classification in order to gather device profile information. This helps in improving the accuracy of device type data, determining firewall policies, and customizing to the meet the requirement of the end user.

PAPI Enhanced Security

The PAPI Enhanced Security configuration provides protection to Aruba devices, Mobility Access Switches, HPE-ArubaOS Switch-based switches, Mobility Master, managed devices, AirWave, and Analytics and Location Engine (ALE) against malicious users sending fake messages that results in security challenges.

Support for VIA-Published Subnets

This new feature, when enabled, allows Mobility Master and managed devices to accept the subnets published by VIA clients. This feature is disabled by default.

Services

AirGroup

ArubaOS 8.0.1.0 supports 7200 Series controllers to run as a master controller. AirGroup is supported in master controller mode.

Captive Portal

ArubaOS 8.0.1.0 supports 7200 Series controllers to run as a master controller. Captive Portal is supported in master controller mode.

UCC

ArubaOS 8.0.1.0 supports 7200 Series controllers to run as a master controller. UCC is supported in master controller mode.

Station Management

MultiZone Support

MultiZone is supported on 100 Series, 130 Series, 200 Series, 210 Series, 220 Series, 310 Series, 320 Series, and 330 Series access points but it is not supported on 90 Series access points.

MultiZone Limitation

MultiZone is not supported on a VMC.

WebUI

AP Group Radio Mode

Starting with ArubaOS 8.0.1.0, the configuration of AP Group radio mode parameters depends on the radio mode selected.

Dashboard

In ArubaOS 8.0.1.0 the dashboard feature is supported in the master controller mode.

The centralized visibility feature is not supported in the master controller mode, which means, you cannot view the **Dashboard** of a managed device from the master controller. To view the **Dashboard** page of a managed device, log in to the managed device.

The following table shows the dashboard pages available in master controller and managed device:

Table 4: *Dashboard Pages in Master Controller and Managed Device*

Pages	Master Controller	Managed Device
Performance	—	Yes
Network	Yes	—
Usage	—	Yes
Potential Issues	—	Yes
Traffic Analysis	—	Yes
AirGroup	—	Yes
Security	Yes	—
UCC	—	Yes
Controller	Yes	Yes
WLANs	—	Yes
Access Points	Yes	Yes
Clients	Yes	Yes

Modifying Profiles Associated with WLANs and AP Groups

Starting from ArubaOS 8.0.1.0, users can modify profiles and parameters associated with AP groups. You can also modify the parameters of profiles that are associated to a WLAN when it was created.

Personalizing Captive Portal

The WebUI for personalizing the captive portal page is enhanced where the user can now select custom login or welcome page, background images, logos, Acceptable Use Policy (AUP) texts, and so on with responsive design. Also, starting from ArubaOS 8.0.1.0, the AUP text is displayed only if the AUP text was previously entered.

This chapter describes the hardware platforms supported in ArubaOS 8.0.1.x.

Controller Platforms

The following table displays the controller platforms supported in ArubaOS 8.0.1.x.

Table 5: *Supported Controller Platforms in ArubaOS 8.0.1.x*

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

AP Platforms

The following table displays the AP platforms supported in ArubaOS 8.0.1.x.

Table 6: *Supported AP Platform in ArubaOS 8.0.1.x*

AP Family	AP Model
90 Series	AP-92, AP-93
—	AP-93H
—	AP-103, AP-103H
100 Series	AP-104, AP-105
110 Series	AP-114, AP-115
130 Series	AP-134, AP-135

Table 6: *Supported AP Platform in ArubaOS 8.0.1.x*

AP Family	AP Model
200 Series	AP-204, AP-205
—	AP-205H
210 Series	AP-214, AP-215
220 Series	AP-224, AP-225
—	AP-228
270 Series	AP-274, AP-275, AP-277
310 Series	AP-314, AP-315
320 Series	AP-324, AP-325
330 Series	AP-334, AP-335
—	RAP-155, RAP-155P
RAP 100 Series	RAP-108, RAP-109
—	RAP-3WN, RAP-3WNP

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 certified with different AP models, refer to the DRT release notes at support.arubanetworks.com.

The following default DRT file version is part of ArubaOS 8.0.1.0:

- DRT-1.0_57023

This chapter describes the issues resolved in ArubaOS 8.0.1.0.

Table 7: *Resolved Issues in ArubaOS 8.0.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
129826	**Symptom:** MultiZone AP on the data zone managed device was unable to take the channels from primary zone. This issue is resolved by sending the power change and status report to all the active zones. **Scenario:** This issue occurred when the primary channels, data zone channels, and the power values were different. This issue was observed in managed devices running ArubaOS 8.0.0.0.	Station Management	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
131117	**Symptom:** Client was deauthenticated due to inconsistency in the bucket map. This issue is resolved by introducing the **num-nodes** parameter, with a default value of 1 and a maximum value of 11, and setting up one controller in the primary zone. **Scenario:** Load balancing algorithm was not functional when a data zone with more than 12 zones was marked with an **L** flag and was disabled. This issue was observed in managed devices running ArubaOS 8.0.0.0.	AP-Platform	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
132544	**Symptom:** Wi-Fi Calling ALG continued to prioritize an already ended Wi-Fi call. Due to this, the CDR record remained active even after a call ended. The fix ensures that the ALG does not prioritize a call that has ended and no CDR is recorded for such calls. **Scenario:** This issue was occasionally observed on Apple iPhones. This issue was observed in Mobility Master running ArubaOS 8.0.0.0.	UCC	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
139098 139157	**Symptom:** A snmp-server trap configuration was not disabled when the **no snmp-server trap** command was executed. This issue is resolved by adding snmp-server trap commands to the data store, for traps that are enabled and thereby ensuring that the **no snmp-server trap** command to delete the configuration is executed successfully. **Scenario:** This issue occurred because most of the snmp-server trap configurations were enabled by default but they did not contain any configuration. This issue was observed in Mobility Master running ArubaOS 8.0.0.0.	SNMP	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0

Table 7: *Resolved Issues in ArubaOS 8.0.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
139330	**Symptom:** Access points were operating in deleted channels. The fix ensures that the removed channels are deleted on the managed device. **Scenario:** This issue occurred when the commands for deleting the channels from the regulatory domain profile were working as expected but these changes were not getting updated in the managed device. This issue was observed in managed devices running ArubaOS 8.0.0.0.	Configuration	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
139994	**Symptom:** On executing the **show ucc client-info** command, the **ap-name** field for a RAP was displayed as **NA**. The fix ensures that the **ap-name** field for a RAP displays the appropriate value. **Scenario:** This issue was seen when a wired client was connected to a RAP in split-tunnel forwarding mode. This issue was observed in Mobility Master running ArubaOS 8.0.0.0.	UCC	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
140686	**Symptom:** The CLI commands were case sensitive. The fix ensures that the CLI commands are case insensitive. **Scenario:** This issue was observed in Mobility Master running ArubaOS 8.0.0.0.	AirGroup	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
141121 151089	**Symptom:** An AP did not fail over to an IPv6 backup LMS. The fix ensures that the AP successfully fails over to an IPv6 backup LMS. **Scenario:** This issue was observed when primary and backup LMS were configured on the managed device with CPsec enabled. This issue was observed in AP-215 access point running ArubaOS 8.0.0.0 or later versions.	IPsec	AP-215 access points	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
142041	**Symptom:** Data Zone on the Mobility Master displayed standby IP for the MultiZone APs that were down. The fix ensures that the managed devices clean the standby IP before updating the AP information to the Mobility Master when the AP is down. **Scenario:** This issue occurred when the Mobility Master did not remove the standby IP even after removing the MultiZone profile from the Primary Zone. This issue was observed in Mobility Master running ArubaOS 8.0.0.0 in a MultiZone topology.	Station Management	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
142334	**Symptom:** The original WMM and DSCP values were not displayed for remote Lync/Skype for Business calls. The fix ensures that the values are displayed for remote calls.	UCC	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0

Table 7: *Resolved Issues in ArubaOS 8.0.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
	Scenario: This issue was observed when two Lync/Skype for Business clients connected to a RAP initiated a call in split-tunnel forwarding mode. This issue was observed in Mobility Master running ArubaOS 8.0.0.0.				
142737	**Symptom:** A Remote AP (RAP) failed to reestablish the tunnel in Ethernet uplink. This fix ensures that RAP establishes tunnel in Ethernet uplink in lesser time. **Scenario:** An RAP established tunnel using cellular uplink (with USB modem) where cellular link had higher priority than Ethernet link. When the USB modem from RAP was physically plugged out, the RAP took very long (5 to 30 mins or even more) to establish the tunnel on Ethernet uplink. The issue persisted even with Mobility Master providing the public IP address or FQDN in the AP provisioning profile attached to the AP group. This issue was observed in Mobility Master running ArubaOS 8.0.0.0.	Remote Access Point	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
142987	**Symptom:** The option to disable dynamic map was not available in the **IKEv1** or **IKEv2 IPSEC Dynamic Maps** section under the **Configuration > Services > VPN** page of the WebUI. This issue is resolved by adding the option to enable or disable dynamic map in the WebUI. **Scenario:** This issue was observed in Mobility Master running ArubaOS 8.0.0.0.	WebUI	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
143138	**Symptom:** A client dropped a call when it roamed to another managed device and both IP mobility and RTP analysis was enabled. The fix ensures that the call remains intact. **Scenario:** When RTP analysis was enabled, the roamed client's audio RTP traffic failed to get tunneled from foreign agent to home agent. This issue was observed in Mobility Master running ArubaOS 8.0.0.0.	UCC	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
143276	**Symptom:** When OpenFlow version lower than 1.3 was detected, AirGroup IPv6 flows did not install for the remaining managed devices with OpenFlow version greater than 1.3. The fix ensures that AirGroup IPv6 flows are installed on the remaining managed devices. **Scenario:** This issue occurred when an OpenFlow enabled managed device was configured with OpenFlow version lower than 1.3. This issue was observed in Mobility Master running ArubaOS 8.0.0.0.	AirGroup	Mobility Master	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
143316	**Symptom:** Whitelisting of sites failed to bypass Captive Portal authentication. This issue is resolved by removing conversion of ID to HBO before downloading it to SOS.	Base OS Security	VMC	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0

Table 7: *Resolved Issues in ArubaOS 8.0.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
	Scenario: This issue occurred when Captive Portal profile was configured with whitelisted sites This issue was observed in VMC and ArubaOS 8.0.0.0.				
143439	**Symptom:** After a session was classified as blocked, it was listed in the blocked session in the UI, even when there was no traffic. This issue is resolved by placing the blocked session processing as part of the outer loop to move all the SOS imported sessions together instead of moving the sessions separately. **Scenario:** This issue was observed in managed devices running ArubaOS 8.0.0.0.	Firewall	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
143604	**Symptom:** A managed device failed to initialize successfully when the Mobility Master was reloaded and configuration was being updated to the configuration files on flash. This issue is resolved by temporarily saving the node configuration file first. After the configuration is successfully saved, the previous node configuration file is replaced with the new file. If the Mobility Master is being reloaded in the middle of creating a new node file, only the last configuration update is lost and the Mobility Master boots successfully with the previous configuration file. **Scenario:** This issue was observed in managed devices running ArubaOS 8.0.0.0.	Configuration	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
144140	**Symptom:** Rebootstrap messages from the AP were printed on the Primary zone when the AP rebootstrapped on the Data zone. The fix ensures that the AP rebootstrap messages are printed on the appropriate zone. **Scenario:** This issue was observed in managed devices running ArubaOS 8.0 in a MultiZone topology.	AP-Platform	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
144446	**Symptom:** The Captive Network Assistant displays a blank page on the Apple devices, when the Captive Portal authentication was used on the VMC. The fix ensures that the blank page is not displayed. **Scenario:** This issue occurred due to the way the meta tag was handled if the original URL requested had a hostname instead of an IP address. This issue was observed in managed devices running ArubaOS 8.0.0.0.	Captive Portal	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0

Table 7: *Resolved Issues in ArubaOS 8.0.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
144570 148449	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt**. This issue is resolved by directly accessing the saved context data when crypto context is cleared. **Scenario:** This issue occurred when IPsec tunnels were closed and the queued crypto context was cleared. This issue was observed in 200 Series, 210 Series, or 220 Series access points running ArubaOS 8.0.0.0.	AP-Platform	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
144830	**Symptom:** Captive portal upload configurations were not present after migration. The fix ensures that the captive portal related configuration are available. **Scenario:** This issue was observed in 7000 Series managed devices running ArubaOS 8.0.0.0.	Captive Portal	7000 Series managed devices	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
144883	**Symptom:** The multicast traffic was not forwarded to a client. The fix ensures that multicast traffic is forwarded to a client. **Scenario:** This issue occurred when IGMP proxy was disabled and no multicast VLAN is configured. When the UAC was changed (AAC and UAC are different for the client) because of cluster client load balancing feature, multicast traffic was not forwarded to the client. This issue was observed in cluster topology running ArubaOS 8.0.0.0.	Multicast	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
145042	**Symptom:** A customer defined application (custom-app) did not work. This fix ensures that the custom-app works as expected. **Scenario:** This issue was observed in a Mobility Master with multiple managed devices that were part of a cluster. This issue was observed in Mobility Master running ArubaOS 8.0.0.0.	Controller-Datapath	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
145328 145330	**Symptom:** The startup script did not migrate the **airgroupservice disable** command and did not parse an airgroupservice name with more than one word. The fix ensures that the startup script migrates the **airgroupservice disable** command with **no enable** parameter. **Scenario:** This issue occurred when the **airgroupservice disable** command or a airgroupservice name with more than a word was migrated. Only the first word in the airgroupservice name was migrated. This issue was observed in Mobility Master running ArubaOS 8.0.0.0.	AirGroup	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
145331	**Symptom:** Managed Devices using the **ip nat outside** configuration with uplink VLAN lost connectivity to the Mobility Master. The fix ensures that the managed devices that use the **ip nat outside** configuration with uplink VLAN do not lose connectivity to the Mobility Master.	Configuration	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0

Table 7: *Resolved Issues in ArubaOS 8.0.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
	Scenario: This issue was observed when **ip nat outside** configured under an interface VLAN was not collected by the **interface vlan** command. As a result, the configuration line **ip nat outside** was not sent to the managed devices.				
145725	**Symptom:** IKE/IPSEC tunnel establishment was failing when the management MAC address was added as the peer MAC address in the managed device. The fix ensures that the IKE/IPSEC tunnel is established when the management MAC address is added as the peer MAC address in the managed device. **Scenario:** This issue was observed in Mobility Master running ArubaOS 8.0.0.0.	Base OS Security	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
150631	**Symptom:** When a user tried to configure a large number of devices and then executed the **write memory** command, the operation timed out though the command was still running. This issue is resolved by ensuring that the number of lines of pending configuration and the number of devices where the configuration will be applied is bound for each write memory operation. **Scenario:** This issue was observed when the user tried to configure more than 500 VLANs for 200 devices together and then running the **write memory**. This issue was observed in 7200 Series and 7030 controllers running ArubaOS 8.0.1.0.	Controller-Datapath	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0
151369	**Symptom:** The throughput in a VMC was inconsistent. The fix ensures that the VMC offers optimized throughput. For optimal performance, incorporate the following configuration: ESXi host settings: Remove tx completion processing from rx thread by creating an independent thread for the same. 1. Execute **esxcli system settings advanced set -o /Net/NetNetqRxQueueFeatPairEnable -i 0** command. 2. Reboot the ESXi host. VM settings: By default, only one tx thread is created for entire VM. For higher throughput, create one tx per port. 1. **VM Settings > Options > Advanced (General) > Configuration (button) > Add row (button)**. Add ethernet0.ctxPerDev (first column) and 1 (second column). 2. Repeat previous step on ports 0 through 3 for VMC and ports 0 and 1	Controller-Datapath	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.0.1.0

Table 7: *Resolved Issues in ArubaOS 8.0.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
	for Mobility Master. **Scenario:** This issue was observed in VMC and ArubaOS 8.0.0.0.				

This chapter describes the issues identified in ArubaOS 8.0.1.0.

Table 8: *Known Issues in ArubaOS 8.0.1.0*

Bug ID	Description	Component	Platform	Reported Version
130735	**Symptom:** AP is **UP** in the Primary zone device with **Z** flag, if the Data zone and the Primary zone IPs are similar in the managed devices. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0 **Workaround:** Provide the appropriate configuration, as this is a misconfiguration issue.	AP-Platform	All platforms	ArubaOS 8.0.0.0
130741	**Symptom:** Chromecast applications do not work when AirGroup is enabled on a Mobility Master. **Scenario:** This issue occurs because of changes to how the Google cast supported applications query for Chromecast. This issue is observed in Mobility Master and stand-alone controllers running ArubaOS 8.0.0.0. **Workaround:** None.	AirGroup	All platforms	ArubaOS 8.0.0.0
131133	**Symptom:** When the primary Local Mobility Switch (LMS) is down, AP does not failover to the backup LMS. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0 only in MultiZone mode, with Backup LMS configured. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.0.0.0
131390	**Symptom:** Client is deauthenticated due to inconsistency in the bucket map. **Scenario:** Load balancing algorithm is not functional when a Data zone with more than 12 zones is marked with an **L** flag and is disabled. This issue is observed in managed devices running ArubaOS 8.0.0.0 **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.0.0.0
138254	**Symptom:** The client which is not involved in UAC failover is deleted after its flapped uplink is up. The log files for the event lists the reason as **observed ip_user delete** in Mobility Master.	Base OS Security	All platforms	ArubaOS 8.0.0.0

Table 8: *Known Issues in ArubaOS 8.0.1.0*

Bug ID	Description	Component	Platform	Reported Version
	Scenario: This issue occurs when shut is performed on the standby-UAC, and the sta/user/mac user/ip user entries are activated on the standby-UAC because it loses connectivity with the active UAC. This issue is observed in a cluster setup in Mobility Master running ArubaOS 8.0.0.0 **Workaround:** The workaround is as follows: • Decrease the user idle timer to 30 secs in the cluster setup. • Once shut is performed, wait for at least a minute before performing no shut. This helps stabilizing the cluster environment.			
140678	**Symptom:** The SNMP CLI commands are not case sensitive. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0.0.0 **Workaround:** None.	SNMP	All platforms	ArubaOS 8.0.0.0
141640	**Symptom:** The WebUI navigation freezes when a user clicks on the **?** icon on the top right corner of the **Configuration** page in the WebUI. **Scenario:** By clicking on the **?** icon, some of the WebUI fields are supposed to turn green indicating that the mouseover help is enabled. However, there is no indication of enabling the help system because the help system is not completely integrated into the **Configuration** pages of the WebUI. This issue is observed in Mobility Master running ArubaOS 8.0 or later versions. **Workaround:** Click on the **?** icon once again to unfreeze the WebUI navigation.	WebUI	All platforms	ArubaOS 8.0.0.0
141856	**Symptom:** The buddy list disappears from the messages application. **Scenario:** This issue occurs when AirGroup and chat service are enabled in Mobility Master running ArubaOS 8.0.0.0. **Workaround:** Disable AirGroup.	AirGroup	All platforms	ArubaOS 8.0.0.0
142097	**Symptom:** User session terminates and the user is automatically logged out **Scenario:** This issue is observed when the user is on any page of Dashboard and when the WebUI remains idle for longer than the set Idle Timeout value. This issue is observed in Mobility Master running ArubaOS 8.0.0.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.0.0.0
142463	**Symptom:** Clients are disconnected and reconnected randomly. **Scenario:** This issue is observed when the radio on the Data Zone Mobility Master is enabled or disabled resulting in resetting of the Basic Service Set (BSS). This issue is observed in Mobility Master running ArubaOS 8.0.0.0 **Workaround:** None.	Station Management	All platforms	ArubaOS 8.0.0.0

Table 8: *Known Issues in ArubaOS 8.0.1.0*

Bug ID	Description	Component	Platform	Reported Version
143244	**Symptom:** Zone statistics are not segregated in the CLI output for the command, **show ap debug radio-stats ap-name <ap-name> radio <radio name> advanced**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0. **Workaround:** None.	Station Management	All platforms	ArubaOS 8.0.0.0
143826	**Symptom:** In a cluster deployment, media classification fails to classify and prioritize Lync/Skype for Business calls. **Scenario:** This issue is observed if a managed device acts as the User Anchor Controller (UAC) for one user on the call and also as a standby UAC for the other user on the same call. **Workaround:** None.	UCC	All platforms	ArubaOS 8.0.0.0
143888	**Symptom:** Unable to configure MAC address for IPsec authentication while setting master IP deployment from managed device. **Scenario:** This issue is observed in all groups and managed devices in Mobility Master running ArubaOS 8.0.0.0. **Workaround:** Configure from CLI using the following command: `(host)[md](config) #masterip 10.15.92.5 ipsec ****** peer-mac-1 00:0C:29:D4:FF:D4 interface vlan 92`	WebUI	All platforms	ArubaOS 8.0.0.0
144344	**Symptom:** The **client** page and the **performance** page in the dashboard of the Mobility Master display incorrect distribution of clients among 2.4 GHz and 5 GHz band in comparison to the information on the dashboard of the managed device. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0 **Workaround:** None.	Monitoring	All platform	ArubaOS 8.0.0.0
144432	**Symptom:** In the WebUI, **WLANs** and **Usage** pages in **Dashboard** shows incorrect data. **Scenario:** This issue is observed when two managed devices has the same SSID and clients associated. In the **WLANs** or **Usage** pages, the graphs loaded only shows data for one SSID instead of aggregated. This issue is observed in managed devices running ArubaOS 8.0.0.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.0.0.0
144643	**Symptom:** When the data zone is a virtual mobility controller (VMC), access points do not come up on the data zone managed device. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0. **Workaround:** None.	IPsec	All platforms	ArubaOS 8.0.0.0

Table 8: *Known Issues in ArubaOS 8.0.1.0*

Bug ID	Description	Component	Platform	Reported Version
144663	**Symptom:** When the background logo is updated from Mobility Master, it does not synchronize with the managed devices. **Scenario:** This issue occurs if Captive Portal is configured earlier on the managed device. This issue is observed in managed devices running ArubaOS 8.0.0.0 or later versions. **Workaround:** Make a configuration change in the Captive Portal profile to trigger a synchronization with the Mobility Master.	Captive Portal	All platforms	ArubaOS 8.0.0.0
145460	**Symptom:** The IPsec tunnel between the managed device and the VPNC goes down when load balancing is enabled. **Scenario:** This issue occurs only when the default gateway is configured before the uplink wired VLAN and when load balancing is enabled in managed devices running ArubaOS 8.0.0.0 or later versions. **Workaround:** Configure the default gateway only after configuring the uplink wired VLAN.	Controller-Datapath	All platforms	ArubaOS 8.0.0.0
145659	**Symptom:** AirGroup is disabled after migration to ArubaOS 8.0.1.0. **Scenario:** This issue occurs when a service-id is present in two services after migration to ArubaOS 8.0.1.0. This issue is observed in 7200 Series Master Controller Mode after upgrading to ArubaOS 8.0.1.0. **Workaround:** None.	AirGroup	All platforms	ArubaOS 8.0.1.0
147192	**Symptom:** A Mobility Master does not forward the response packets from the messages application. **Scenario:** This issue occurs when mDNS and chat service are enabled in Mobility Master running ArubaOS 8.0.0.0. **Workaround:** None.	AirGroup	All platforms	ArubaOS 8.0.0.0
147931	**Symptom:** The static channel bandwidth (40/80/160 MHz) for a radio profile with ARM disabled cannot be configured using the **Max channel bandwidth** parameter. **Scenario:** This issue is observed in 7200 Series Master Controller Mode and stand-alone controllers with ARM disabled. The maximum channel bandwidth is applicable only on Mobility Master running Air match. This issue is observed in 7200 Series Master Controller Mode and stand-alone controllers running ArubaOS 8.0.1.0. **Workaround:** Configure the maximum channel bandwidth directly in the radio channel. For example: 36+ (40 MHz), 36E (80 MHz), 36E+149E (80+80 MHz), 36S (for 160 MHz), 1+ (2.4 GHz 40 MHz).	WebUI	7200 Series Master Controller Mode and stand-alone controllers	ArubaOS 8.0.1.0

Table 8: *Known Issues in ArubaOS 8.0.1.0*

Bug ID	Description	Component	Platform	Reported Version
148110	**Symptom:** The client VLAN is not retained in AirGroup table. **Scenario:** This issue occurs when a client roams from one managed device to another across VLANs with IP mobility enabled. This issue is observed in 7200 Series Master Controller Mode and Managed Devices running ArubaOS 8.0.1.0. **Workaround:** None.	AirGroup	All platforms	ArubaOS 8.0.1.0
149041	**Symptom:** AP comes up with an ID flag when CPsec is enabled. **Scenario:** This issue is observed when an AP is connected to a controller through two VLANs, where VLAN1 is the controller IP and the AP is connected to VLAN2 on the same controller directly. This issue is observed when CPsec is enabled. **Workaround:** Remove the IPv6 address from the VLAN2.	AP-Platform	All platforms	ArubaOS 8.0.1.0
149222	**Symptom:** When you configure a managed device from the **/mm/mynode** node hierarchy of the CLI, Mobility Master does not display the devices in the WebUI. Only the devices configured from the **/mm** node hierarchy is displayed in the WebUI. **Scenario:** This issue is observed in the WebUI of Mobility Master running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	IPsec	Mobility Master	ArubaOS 8.0.0.0
149799	**Symptom:** Creation of a **license-pool-profile** fails if the name of the profile exceeds 63 characters. **Scenario:** This issue occurs only if the number of characters in the **license-pool-profile** name exceeds 63. This issue is observed in Mobility Master running ArubaOS 8.0.0.0 or later versions. **Workaround:** Create **license-pool-profile** with a name not exceeding 63 characters.	Licensing	Mobility Master	ArubaOS 8.0.1.0
150462	**Symptom:** The **Dashboard > WLANs** page in Mobility Master shows less number of clients in comparison to the **Clients** page in the Mobility Master and the **Clients** and **WLANs** page in a managed device. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0.1.0. **Workaround:** None.	Monitoring	Mobility Master	ArubaOS 8.0.1.0
151058	**Symptom:** Mobility Master supports one management and two data interfaces. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0.0.0. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.0.0.0
151180	**Symptom:** After migrating to ArubaOS 8.x, the global **airgroup disallow-vlan** command is not effective for service levels.	AirGroup	All platforms	ArubaOS 8.0.1.0

Table 8: *Known Issues in ArubaOS 8.0.1.0*

Bug ID	Description	Component	Platform	Reported Version
	Scenario: This issue occurs when ArubaOS 6.x deployment is migrated to ArubaOS 8.x. This issue is observed in Mobility Master running ArubaOS 8.0.0.0 or later versions. **Workaround:** Execute the **disallow-vlan** command at the service level.			
151316	**Symptom:** Cluster is getting disabled with respect to the AP when the managed device was upgraded from ArubaOS 8.0 to ArubaOS 8.0.1.0 with cluster as Data Zone. **Scenario:** This issue occurs due to the num-nodes added in the ArubaOS 8.0.1.0. This issue is observed in managed devices running ArubaOS 8.0.1.0. **Workaround:** Add the num-nodes based on the number of the nodes in the Data Zone cluster.	AP-Platform	All platforms	ArubaOS 8.0.1.0
151333	**Symptom:** IPv6 routes with link local address are not migrated from ArubaOS 6.x deployment to ArubaOS 8.x. setup. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Migration	All platforms	ArubaOS 8.0.1.0
151689	**Symptom:** WLAN deployments running ArubaOS 6.2.x or earlier versions fail to upgrade to ArubaOS 8.x. **Scenario:** This issue is observed in WLAN deployments running UCC application on ArubaOS 6.2.x or earlier versions. **Workaround:** None.	UCC	All platforms	ArubaOS 8.0.1.0
151701	**Symptom:** IPv6 ACLs applied on an interface from an ArubaOS 6.x deployment are not effective after migrating to ArubaOS 8.x. setup. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.0.1.0
151740	**Symptom:** The **Dashboard > Traffic Analysis** page does not show all WLANs at node level. The WLAN details in the **Traffic Analysis** page can contain duplicated WLANs when selecting the Managed Device or a group on a Mobility Master. **Scenario:** This issue is observed at Mobility Master node level dashboard running ArubaOS 8.0.1.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.0.1.0
151742	**Symptom:** The **Dashboard > Managed Network** page shows more clients than actual number of clients.	Monitoring	All platforms	ArubaOS 8.0.1.0

Table 8: *Known Issues in ArubaOS 8.0.1.0*

Bug ID	Description	Component	Platform	Reported Version
	Scenario: This issue is observed in managed devices running ArubaOS 8.0.1.0. **Workaround:** None.			
151817	**Symptom:** After migration, the entries of the APs that were in **Down** status in the ArubaOS 6.x setup are missing from the global AP database of ArubaOS 8.x setup. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0.1.0. **Workaround:** None.	Migration	All platforms	ArubaOS 8.0.1.0
151906	**Symptom:** Application classification does not work on managed devices if unique application ID or name is not used. **Scenario:** This issue occurs when custom application scripts are added, deleted, and re-added with the same custom application ID or name. This issue is observed in managed devices running ArubaOS 8.0.1.0. **Workaround:** If you are upgrading from ArubaOS 8.0.0.0 with custom applications configured, delete the customer applications and re-add them after upgrading to ArubaOS 8.0.1.0. If you are adding, deleting, and re-adding custom applications in ArubaOS 8.0.1.0, do not reuse the custom application ID or name. Instead, use different unique (previously unused) application ID or name.	Controller-Datapath	All platforms	ArubaOS 8.0.1.0
151915	**Symptom:** A client cannot view the background image present in the Captive Portal profile. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0 when a managed device is migrated from ArubaOS 6.x where the Captive Portal profile has a background logo configured. **Workaround:** None.	Captive Portal	All platforms	ArubaOS 8.0.1.0
151952	**Symptom:** When the managed device reboots, APs and clients boot without IP address 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
152148	**Symptom:** The **Dashboard > Traffic Analysis** page is not updated with WLANs, web content, and so on when a user roams to a different SSID. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0 **Workaround:** The **Traffic Analysis** page is updated after 10 minutes.	Monitoring	All platforms	ArubaOS 8.0.1.0
152252	**Symptom:** The management interface on the Mobility Master and managed device can be reached when the the interface is configured with an IP address even though the interface is shutdown. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0	Interface	All platforms	ArubaOS 8.0.1.0

Table 8: *Known Issues in ArubaOS 8.0.1.0*

Bug ID	Description	Component	Platform	Reported Version
	Workaround: Remove the IP address configuration from management interface when the interface is shutdown.			
152270	**Symptom:** The loadable service modules like **airgroup, airmatch, appRF, arm, nbapi_helper, ucm, web,** or **wms** crash in a Mobility Master. **Scenario:** This issue occurs because of a mismatch of ArubaOS version and packages when a user boots the Mobility Master to a non-default partition from the grub boot menu. This issue is observed in Mobility Master running ArubaOS 8.0.1.0 **Workaround:** Re-copy the images to the respective partition and reload the Mobility Master.	WebUI	Mobility Master	ArubaOS 8.0.1.0
152360	**Symptom:** The **Dashboard > Traffic Analysis > WLAN** page shows repetitive WLANs. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.0.1.0
152445	**Symptom:** IPsec between Mobility Master and managed device fails when managed device uses PSK with MAC for authentication. **Scenario:** This issue occurs because the managed device uses the management address of the Mobility Master instead of the MAC address to establish IPsec connection with Mobility Master. This issue is observed in managed devices running ArubaOS 8.0.1.0 **Workaround:** Execute the **write erase all** command on the managed device and start **setup dialog** by using the MAC address of the Mobility Master.	IPsec	All platforms	ArubaOS 8.0.1.0
156755	**Symptom:** An AP does not download the ArubaOS image from a managed device and does not boot. **Scenario:** This issue is observed in 310 Series, 320 Series, and 330 Series access points running ArubaOS 8.0.1.0. **Workaround:** Disable Deep Packet Inspection (DPI) and reboot the managed device.	AP-Platform	310 Series, 320 Series, or 330 Series access points	ArubaOS 8.0.1.0

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 and Best Practices

Ensure a successful upgrade and optimize your upgrade procedure by taking the recommended actions provided in the following list. You should save this list for future use.

- 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 other 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 your network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** section of the WebUI, or by executing the **show ap active** and **show ap database** CLI commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS is currently on the managed device?
  - Are all managed devices running the same version of software?
  - Which services are used on the 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 software 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 problems occur 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 should it be required.
- Before you upgrade to this version of ArubaOS, assess your software license requirements and load any new or expanded licenses you may require. For a detailed description of these new license modules, see the "Software Licenses" chapter in the *ArubaOS User 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. To maintain the reliability of your WLAN network, the following compact memory best practices are recommended:

- Confirm that there is at least 60 MB of free memory available for an upgrade using the WebUI, or execute the **show memory** command to confirm that there is at least 40 MB of free memory available for an upgrade using the CLI. Do not proceed unless this much free memory is available. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Confirm that there is at least 75 MB of flash space available for an upgrade using the WebUI, or execute the **show storage** command to confirm that there is at least 60 MB of flash space available for an upgrade using the CLI.

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.

If the output of the **show storage** command indicates that there is insufficient flash memory space, you must free up some used memory. Any managed device logs, crash data, or flash backups should be copied to a location off the managed device, then deleted from the managed device to free up flash space. You can delete the following files from the managed device to free up some memory before upgrading:

- **Crash Data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 35 to copy the **crash.tar** file to an external server, and then 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 35 to back up the flash directory to a file named **flash.tar.gz**, and then execute the **tar clean flash** command to delete the file from the managed device.
- **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 35 to copy the **logs.tar** file to an external server, and then execute the **tar clean logs** command to delete the file from the managed device.

The following procedure deletes a file.

In the WebUI

Navigate to **Maintenance > File > Delete Files** and remove any aging log files or redundant backups which may have been created by administrator.

In the CLI

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

Backing up Critical Data

It is important to frequently back up all critical configuration data and files on the compact flash file system to an external server or mass storage device. At the very least, you should include the following files in these frequent backups:

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

Backing up and Restoring Compact Flash in the WebUI

The WebUI provides the easiest way to back up and restore the entire compact flash file system. The following steps describe how to back up and restore the compact flash file system using the WebUI on the managed device:

1. Click the **Configuration** tab.
2. Click **Save Configuration** at the top of the page.
3. Navigate to the **Maintenance > File > Backup Flash** page.
4. Click **Create Backup** to back up the contents of the compact flash file system to the **flashbackup.tar.gz** file.
5. Click **Copy Backup** to copy the file to an external server.

   You can later copy the backup file from the external server to the compact flash file system using the file utility in the **Maintenance > File > Copy Files** page.
6. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page and click **Restore**.

Backing up and Restoring Compact Flash in the CLI

The following steps describe the backup and restore procedure for the entire compact flash file system using the command line:

1. Make sure you are in the **enable** mode in the CLI, and execute the following command:

   ```
   (host) # write memory
   ```

2. Execute the **backup** command to back up the contents of the compact flash file system to the **flashbackup.tar.gz** file.

   ```
   (host) # backup flash
   Please wait while we tar relevant files from flash...
   Please wait while we compress the tar file...
   Checking for free space on flash...
   Copying file to flash...
   File flashbackup.tar.gz created successfully on flash.
   ```

3. Execute the **copy** command to transfer the backup flash 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 later transfer the backup flash file from the external server or storage device to the compact flash file system by executing the **copy** command.

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

4. Execute the **restore** command to untar and extract the **flashbackup.tar.gz** file to the compact flash file system.

   ```
   (host) # restore flash
   ```

Upgrading

The following sections provide the procedures for upgrading your WLAN network to the latest ArubaOS version using the WebUI or CLI.

ArubaOS 8.0.1.x Upgrade Notes

Before you upgrade Mobility Master from ArubaOS 8.0.0.0 to ArubaOS 8.0.1.x, take a note of the following points:

- ArubaOS 8.0.1.x supports only a maximum of 3 network adapters for Mobility Master and 4 network adapters for Virtual Mobility Controller. If you have 4 network adapters on your ArubaOS 8.0.0.0 Mobility Master ESXi server, you must remove one before upgrading to ArubaOS 8.0.1.x to avoid upgrade failure. To remove a network adapter from the ESXi server:

Before you remove the additional network adapter from the ESXi server, ensure that you copy the ArubaOS 8.0.1.x image on the system partition of Mobility Master.

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 8.0.1.x 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 virtual mobility controller or Mobility Master. Before reloading the new image on Mobility Master, alter the peer MAC address using the following procedure in the WebUI:
  1. From the **Managed Network** node hierarchy, select the managed device.
  2. Navigate to **Configuration > Controllers** and enter the management interface MAC address in the **Peer MAC address of master** field.
  3. Click **Submit** and click **Continue** in the reload popup.
  4. Click **Pending Changes**.
  5. In the **Pending Changes** window, select the check box and click **Deploy changes**.

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

  ```
  (host) [<device-mac-address>] (config) #masterip <ipaddr> ipsec <key> peer-mac-1 <mgmt-interface-mac> peer-mac-2 <mgmt-interface-mac> interface vlan <id>
  ```
- Before upgrading to ArubaOS 8.0.1.x from ArubaOS 8.0.0.0, move the **license-pool-profile-root** configuration from **/mm/mynode** to **/mm**.

In the WebUI

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash space available for an upgrade using the WebUI. For details, see Memory Requirements on page 34.

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

You can install the software image from a TFTP or FTP server using the same WebUI page.

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

The ArubaOS image file is digitally signed, and is verified using RSA2048 certificates preloaded at the factory. Therefore, even if you do not manually verify the SHA hash of a software image, the managed device will not load a corrupted image.

4. Log in to the ArubaOS WebUI from the PC or workstation.
5. Navigate to the **Maintenance > Controller > Image Management** page.
   a. Select the **Local File** option.
   b. Click **Browse** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Click the non-boot partition from the **Partition to Upgrade** option.
8. Click **Yes** in the **Reboot Controller After Upgrade** option to automatically reboot after upgrading. Click **No**, if you do not want to reboot immediately.

Note that the upgrade will not take effect until you reboot.

9. Click **Yes** in the **Save Current Configuration Before Reboot** option.
10. Click **Upgrade**.

    When the software image is uploaded, a popup window displays the **Changes were written to flash successfully** message.
11. Click **OK**.

    If you chose to automatically reboot in step 8, the reboot process starts automatically within a few seconds (unless you cancel it).
12. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > NETWORK > All WLAN Controllers** page to verify the upgrade.

When your upgrade is complete, perform the following steps to verify that the controller is functioning as expected.

1. Log in to the WebUI to verify all your controllers are up after the reboot.
2. Navigate to the **Monitoring > NETWORK > Network Summary** page to determine if your APs are up and ready to accept clients. In addition, verify that the number of access points and clients are what you would expect.
3. Verify that the number of access points and clients are what you would expect.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 35 for information on creating a backup. If the flash (Provisioning/Backup) image version string shows the letters *rn*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses.

In the CLI

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash space available for an upgrade using the CLI. For details, see Memory Requirements on page 34.

Upgrading From a Recent Version of ArubaOS

To install the ArubaOS software image from a PC or workstation using the CLI:

1. Download ArubaOS from the customer support site.
2. Open an SSH session on your master (and local) controllers.
3. Execute the **ping** command to verify the network connection from the target controller to the SCP/FTP/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 images are loaded on the controller's 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 onto 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 controller.

   ```
   (host)# reload
   ```

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

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

When your upgrade is complete, perform the following steps to verify that the controller is functioning as expected.

1. Log in to the CLI to verify that all your controllers 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 access points and clients are what you expected.
4. Test a different type of client for each access method that you use and in different locations when possible.

5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 35 for information on creating a backup.

Downgrading

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

Before You Begin

Before you reboot the controller with the pre-upgrade software version, you must perform the following steps:

1. Back up your controller. For details, see Backing up Critical Data on page 35.
2. Verify that the control plane security is disabled.
3. Set the controller to boot with the previously saved pre-ArubaOS configuration file.
4. Set the controller to boot from the system partition that contains the previously running ArubaOS image.

   When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file used on the next controller reload. An error message is displayed if system boot parameters are set for incompatible image and configuration files.
5. After downgrading the software on the controller, perform the following steps:
   - Restore pre-ArubaOS flash backup from the file stored on the controller. Do not restore the ArubaOS flash backup file.
   - You do not need to reimport the WMS database or RF Plan data. However, if you have added changes to RF Plan in ArubaOS, the changes do not appear in RF Plan in the downgraded ArubaOS version.
   - If you installed any certificates while running ArubaOS, you need to reinstall the certificates in the downgraded ArubaOS version.

Downgrading Using the WebUI

The following section describes how to use the WebUI to downgrade the software on the controller

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, copy the file to the controller by navigating to the **Maintenance > File > Copy Files** page.
   a. For **Source Selection**, select FTP/TFTP server, and enter the IP address of the FTP/TFTP server and the name of the pre-upgrade configuration file.
   b. For **Destination Selection**, enter a file name (other than default.cfg) for Flash File System.
2. Set the controller to boot with your pre-upgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the saved pre-upgrade configuration file from the **Configuration File** drop-down list.
   b. Click **Apply**.

3. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Controller > Image Management** page. If there is no previous software image stored on your system partition, load it into the backup system partition (you cannot load a new image into the active system partition) by performing the following steps:
   a. Enter the FTP/TFTP server address and image file name.
   b. Select the backup system partition.
   c. Click **Upgrade**.
4. Navigate to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the system partition that contains the pre-upgrade image file as the boot partition.
   b. Click **Apply**.
5. Navigate to the **Maintenance > Controller > Reboot Controller** page. Click **Continue**. The controller reboots after the countdown period.
6. When the boot process is complete, verify that the controller is using the correct software by navigating to the **Maintenance > Controller > Image Management** page.

Downgrading Using the CLI

The following section describes how to use the CLI to downgrade the software on the controller.

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the controller:
   ```
   (host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
   ```
   or
   ```
   (host) # copy tftp: <tftphost> <image filename> system: partition 1
   ```
2. Set the controller to boot with your pre-upgrade configuration file.
   ```
   (host) # boot config-file <backup configuration filename>
   ```
3. Execute the **show image version** command to view the partition on which your previous software image 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 controller.
   ```
   (host) # reload
   ```
6. When the boot process is complete, verify that the controller is using the correct software.
   ```
   (host) # show image version
   ```

Before You Call Technical Support

Before you place a call to Technical Support, follow these steps:

1. Provide a detailed network topology (including all the devices in the network between the user and the Aruba device with IP addresses and Interface numbers if possible).
2. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless Network Interface Card (NIC) make and model number, wireless NIC's driver date and version, and the wireless NIC's configuration.
3. Provide the logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
4. Provide the syslog file at the time of the problem. Aruba strongly recommends that you consider adding a syslog server if you do not already have one to capture the logs.
5. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have an outage in a network that worked in the past, a network configuration that has never worked, or a brand new installation.
6. Let the support person know if there are any recent changes in your network (external to the Aruba device) or any recent changes to your Aruba device and/or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
7. Provide the date and time (if possible) of when the problem first occurred. If the problem is reproducible, list the exact steps taken to re-create the problem.
8. Provide any wired or wireless sniffer traces taken during the time of the problem.
9. Provide the Aruba device site access information, if possible.

Appendix A
Acronyms and Abbreviations

The following table lists the acronyms and abbreviations used in Aruba documents.

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
3G	Third Generation of Wireless Mobile Telecommunications Technology
4G	Fourth Generation of Wireless Mobile Telecommunications Technology
AAA	Authentication, Authorization, and Accounting
ABR	Area Border Router
AC	Access Category
ACC	Advanced Cellular Coexistence
ACE	Access Control Entry
ACI	Adjacent Channel interference
ACL	Access Control List
AD	Active Directory
ADO	Active X Data Objects
ADP	Aruba Discovery Protocol
AES	Advanced Encryption Standard
AIFSN	Arbitrary Inter-frame Space Number
ALE	Analytics and Location Engine

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
ALG	Application Layer Gateway
AM	Air Monitor
AMON	Advanced Monitoring
AMP	AirWave Management Platform
A-MPDU	Aggregate MAC Protocol Data Unit
A-MSDU	Aggregate MAC Service Data Unit
ANQP	Access Network Query Protocol
ANSI	American National Standards Institute
AP	Access Point
API	Application Programming Interface
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
AVF	AntiVirus Firewall
BCMC	Broadcast-Multicast
BGP	Border Gateway protocol
BLE	Bluetooth Low Energy
BMC	Beacon Management Console
BPDU	Bridge Protocol Data Unit
BRAS	Broadband Remote Access Server

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
BRE	Basic Regular Expression
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CA	Certification Authority
CAC	Call Admission Control
CALEA	Communications Assistance for Law Enforcement Act
CAP	Campus AP
CCA	Clear Channel Assessment
CDP	Cisco Discovery Protocol
CDR	Call Detail Records
CEF	Common Event Format
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CLI	Command-Line Interface
CN	Common Name
CoA	Change of Authorization
CoS	Class of Service
CPE	Customer Premises Equipment

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
CPsec	Control Plane Security
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSA	Channel Switch Announcement
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSR	Certificate Signing Request
CSV	Comma Separated Values
CTS	Clear to Send
CW	Contention Window
DAS	Distributed Antenna System
dB	Decibel
dBm	Decibel Milliwatt
DCB	Data Center Bridging
DCE	Data Communication Equipment
DCF	Distributed Coordination Function
DDMO	Distributed Dynamic Multicast Optimization
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
DFT	Discreet Fourier Transform
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMO	Dynamic Multicast optimization
DN	Distinguished Name
DNS	Domain Name System
DOCSIS	Data over Cable Service Interface Specification
DoS	Denial of Service
DPD	Dead Peer Detection
DPI	Deep Packet Inspection
DR	Designated Router
DRT	Downloadable Regulatory Table
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSSS	Direct Sequence Spread Spectrum
DST	Daylight Saving Time
DTE	Data Terminal Equipment
DTIM	Delivery Traffic Indication Message
DTLS	Datagram Transport Layer Security
DU	Data Unit

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
EAP	Extensible Authentication Protocol
EAP-FAST	EAP-Flexible Authentication Secure Tunnel
EAP-GTC	EAP-Generic Token Card
EAP-MD5	EAP-Method Digest 5
EAP-MSCHAP EAP-MSCHAPv2	EAP-Microsoft Challenge Handshake Authentication Protocol
EAPoL	EAP over LAN
EAPoUDP	EAP over UDP
EAP-PEAP	EAP-Protected EAP
EAP-PWD	EAP-Password
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security
ECC	Elliptical Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EIGRP	Enhanced Interior Gateway Routing Protocol
EIRP	Effective Isotropic Radiated Power
EMM	Enterprise Mobility Management
ESI	External Services Interface
ESS	Extended Service Set

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
ESSID	Extended Service Set Identifier
EULA	End User License Agreement
FCC	Federal Communications Commission
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FIB	Forwarding Information Base
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
FQLN	Fully Qualified Location Name
FRER	Frame Receive Error Rate
FRR	Frame Retry Rate
FSPL	Free Space Path Loss
FTP	File Transfer Protocol
GBps	Gigabytes per second
Gbps	Gigabits per second
GHz	Gigahertz
GIS	Generic Interface Specification
GMT	Greenwich Mean Time
GPP	Guest Provisioning Page
GPS	Global Positioning System

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
GVRP	GARP or Generic VLAN Registration Protocol
H2QP	Hotspot 2.0 Query Protocol
HA	High Availability
HMD	High Mobility Device
HSPA	High-Speed Packet Access
HT	High Throughput
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAS	Internet Authentication Service
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IDS	Intrusion Detection System
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
IKE PSK	Internet Key Exchange Pre-shared Key
IoT	Internet of Things
IP	Internet Protocol
IPM	Intelligent Power Monitoring
IPS	Intrusion Prevention System
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
JSON	JavaScript Object Notation
KBps	Kilobytes per second
Kbps	Kilobits per second
L2TP	Layer-2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LDPC	Low-Density Parity-Check
LEA	Law Enforcement Agency
LEAP	Lightweight Extensible Authentication Protocol

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
LED	Light Emitting Diode
LEEF	Log Event Extended Format
LI	Lawful Interception
LLDP	Link Layer Discovery Protocol
LLDP-MED	LLDP–Media Endpoint Discovery
LMS	Local Management Switch
LNS	L2TP Network Server
LTE	Long Term Evolution
MAB	MAC Authentication Bypass
MAC	Media Access Control
MAM	Mobile Application Management
MBps	Megabytes per second
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MD5	Message Digest 5
MDM	Mobile Device Management
mDNS	Multicast Domain Name System
MFA	Multi-factor Authentication
MHz	Megahertz

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
MIB	Management Information Base
MIMO	Multiple-Input Multiple-Output
MLD	Multicast Listener Discovery
MPDU	MAC Protocol Data Unit
MPLS	Multiprotocol Label Switching
MPPE	Microsoft Point-to-Point Encryption
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSS	Maximum Segment Size
MSSID	Mesh Service Set Identifier
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
MU-MIMO	Multi-User Multiple-Input Multiple-Output
MVRP	Multiple VLAN Registration Protocol
NAC	Network Access Control
NAD	Network Access Device
NAK	Negative Acknowledgment Code
NAP	Network Access Protection
NAS	Network Access Server Network-attached Storage
NAT	Network Address Translation

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
NetBIOS	Network Basic Input/Output System
NIC	Network Interface Card
Nmap	Network Mapper
NMI	Non-Maskable Interrupt
NMS	Network Management Server
NOE	New Office Environment
NTP	Network Time Protocol
OAuth	Open Authentication
OCSP	Online Certificate Status Protocol
OFA	OpenFlow Agent
OFDM	Orthogonal Frequency Division Multiplexing
OID	Object Identifier
OKC	Opportunistic Key Caching
OS	Operating System
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
OVA	Open Virtual Appliance
OVF	Open Virtualization Format
PAC	Protected Access Credential

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
PAP	Password Authentication Protocol
PAPI	Proprietary Access Protocol Interface
PCI	Peripheral Component Interconnect
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PEAP-GTC	Protected Extensible Authentication Protocol-Generic Token Card
PEF	Policy Enforcement Firewall
PFS	Perfect Forward Secrecy
PHB	Per-hop behavior
PIM	Protocol-Independent Multicast
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PMK	Pairwise Master Key
PoE	Power over Ethernet
POST	Power On Self Test
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PPTP	PPP Tunneling Protocol

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
PRNG	Pseudo-Random Number Generator
PSK	Pre-Shared Key
PSU	Power Supply Unit
PVST	Per VLAN Spanning Tree
QoS	Quality of Service
RA	Router Advertisement
RADAR	Radio Detection and Ranging
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RAP	Remote AP
RAPIDS	Rogue Access Point and Intrusion Detection System
RARP	Reverse ARP
REGEX	Regular Expression
REST	Representational State Transfer
RF	Radio Frequency
RFC	Request for Comments
RFID	Radio Frequency Identification
RIP	Routing Information Protocol
RRD	Round Robin Database

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
RSA	Rivest, Shamir, Adleman
RSSI	Received Signal Strength Indicator
RSTP	Rapid Spanning Tree Protocol
RTCP	RTP Control Protocol
RTLS	Real-Time Location Systems
RTP	Real-Time Transport Protocol
RTS	Request to Send
RTSP	Real Time Streaming Protocol
RVI	Routed VLAN Interface
RW RoW	Rest of World
SA	Security Association
SAML	Security Assertion Markup Language
SAN	Subject Alternative Name
SCB	Station Control Block
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SDN	Software Defined Networking
SDR	Software-Defined Radio

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SDU	Service Data Unit
SD-WAN	Software-Defined Wide Area Network
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIRT	Security Incident Response Team
SKU	Stock Keeping Unit
SLAAC	Stateless Address Autoconfiguration
SMB	Small and Medium Business
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transport Protocol
SNIR	Signal-to-Noise-Plus-Interference Ratio
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SoC	System on a Chip

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SoH	Statement of Health
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
STBC	Space-Time Block Coding
STM	Station Management
STP	Spanning Tree Protocol
STRAP	Secure Thin RAP
SU-MIMO	Single-User Multiple-Input Multiple-Output
SVP	SpectraLink Voice Priority
TAC	Technical Assistance Center
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol/ Internet Protocol
TFTP	Trivial File Transfer Protocol
TIM	Traffic Indication Map
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TLV	Type-length-value
ToS	Type of Service

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
TPC	Transmit Power Control
TPM	Trusted Platform Module
TSF	Timing Synchronization Function
TSPEC	Traffic Specification
TTL	Time to Live
TTLS	Tunneled Transport Layer Security
TXOP	Transmission Opportunity
U-APSD	Unscheduled Automatic Power Save Delivery
UCC	Unified Communications and Collaboration
UDID	Unique Device Identifier
UDP	User Datagram Protocol
UI	User Interface
UMTS	Universal Mobile Telecommunication System
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VA	Virtual Appliance

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
VBN	Virtual Branch Networking
VBR	Virtual Beacon Report
VHT	Very High Throughput
VIA	Virtual Intranet Access
VIP	Virtual IP Address
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over IP
VoWLAN	Voice over Wireless Local Area Network
VPN	Virtual Private Network
VRD	Validated Reference Design
VRF	Visual RF
VRRP	Virtual Router Redundancy Protocol
VSA	Vendor-Specific Attributes
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WebUI	Web browser User Interface
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance
WIDS	Wireless Intrusion Detection System

Table 9: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
WINS	Windows Internet Naming Service
WIPS	Wireless Intrusion Prevention System
WISPr	Wireless Internet Service Provider Roaming
WLAN	Wireless Local Area Network
WME	Wireless Multimedia Extensions
WMI	Windows Management Instrumentation
WMM	Wi-Fi Multimedia
WMS	WLAN Management System
WPA	Wi-Fi Protected Access
WSDL	Web Service Description Language
WWW	World Wide Web
WZC	Wireless Zero Configuration
XAuth	Extended Authentication
XML	Extensible Markup Language
XML-RPC	XML Remote Procedure Call
ZTP	Zero Touch Provisioning