ArubaOS 6.4.4.0

Release Notes

aruba®
NETWORKS
an HP company

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 Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Company

Attn: General Counsel

3000 Hanover Street

Palo Alto, CA 94304

USA

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at dl-gplquery@arubanetworks.com.

Contents

ArubaOS 6.4.4.0 is a software maintenance release that includes new hardware support, several new features and enhancements, and fixes to issues identified in previous releases.

Chapter Overview

- New Features on page 10 provides a description of features and enhancements introduced in ArubaOS 6.4.4.x release versions.
- Regulatory Updates on page 16 lists the regulatory updates in ArubaOS 6.4.4.x release versions.
- Resolved Issues on page 18 lists and describes the issues resolved in ArubaOS 6.4.4.x release versions.
- Known Issues and Limitations on page 36 lists and describes the known and outstanding issues identified in ArubaOS 6.4.4.x release versions.
- Upgrade Procedure on page 40 describes the procedures for upgrading a controller to this release.

Important Points to Remember

If you modify the configuration of an AP, those changes take effect immediately; you do not need to reboot the controller or the AP for the changes to affect the current running configuration. Certain commands, however, automatically force the AP radio to restart.

AirGroup

Support for Wired Users

Starting from ArubaOS 6.4.3.0, AirGroup does not support wired users.

AP Settings Triggering a Radio Restart

Changing the following settings triggers the radio to restart on the AP-200 Series, AP-205H, AP-210 Series, AP-220 Series, AP-270 Series and AP-320 Series access points. When the radio restarts, wireless services will be briefly interrupted. Clients will automatically reconnect to the network when the radio is again up and running.

Table 1: *Profile Settings in ArubaOS 6.4.x*

Profile	Settings
802.11a/802.11g Radio Profile	• Channel • Enable Channel Switch Announcement (CSA) • CSA Count • High throughput enable (radio) • Very high throughput enable (radio) • TurboQAM enable • Maximum distance (outdoor mesh setting) • Transmit EIRP • Advertise 802.11h Capabilities • Beacon Period/Beacon Regulate • Advertise 802.11d Capabilities
Virtual AP Profile	• Virtual AP enable • Forward Mode • Remote-AP operation

SSID Profile	• ESSID
	• Encryption
	• Enable Management Frame Protection
	• Require Management Frame Protection
	• Multiple Tx Replay Counters
	• Strict Spectralink Voice Protocol (SVP)
	• Wireless Multimedia (WMM) settings
	  ▪ Wireless Multimedia (WMM)
	  ▪ Wireless Multimedia U-APSD (WMM-UAPSD) Powersave
	  ▪ WMM TSPEC Min Inactivity Interval
	  ▪ Override DSCP mappings for WMM clients
	  ▪ DSCP mapping for WMM voice AC
	  ▪ DSCP mapping for WMM video AC
	  ▪ DSCP mapping for WMM best-effort AC
	  ▪ DSCP mapping for WMM background AC

High-throughput SSID Profile	• High throughput enable (SSID) • 40 MHz channel usage • Very High throughput enable (SSID) • 80 MHz channel usage (VHT)
802.11r Profile	• Advertise 802.11r Capability • 802.11r Mobility Domain ID • 802.11r R1 Key Duration • key-assignment (CLI only)
Hotspot 2.0 Profile	• Advertise Hotspot 2.0 Capability • RADIUS Chargeable User Identity (RFC4372) • RADIUS Location Data (RFC5580)

Supported Browsers

The following browsers are officially supported for use with ArubaOS 6.4.4.0 WebUI:

- Microsoft Internet Explorer 10.x and 11 on Windows 7 and Windows 8
- Mozilla Firefox 23 or later on Windows Vista, Windows 7, Windows 8, and Mac OS
- Apple Safari 5.1.7 or later on Mac OS

Contacting Support

Table 2: *Contact Information*

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

This chapter describes the new features and enhancements introduced in this release. For more information about these features, refer to the *ArubaOS 6.4.4.x User Guide*.

AP-Platform

Support for AP-320 Series Access Points

The AP-320 Series (AP-324 and AP-325) wireless access points support IEEE 802.11ac standards for high-performance WLAN, and is equipped with two dual-band radios, which can provide access and monitor the network simultaneously. MU-MIMO (Multi-User Multiple-In Multiple-Output) technology allows this access point to deliver high-performance 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while also supporting 802.11a/b/g wireless services. The AP-324 and AP-325 access points work in conjunction with an Aruba controller.

The AP-320 Series wireless access points are not supported in 600 Series controllers.

The AP-320 Series wireless access points provide the following capabilities:

- Dual wireless transceiver
- 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
- Compatibility with IEEE 802.3at and 802.3af PoE
- Centralized management configuration and upgrades using a controller
- Integrated Bluetooth Low Energy (BLE) radio

For more information, see the *AP-320 Series Access Point Installation Guide*.

The following features are not supported in AP-320 Series access points:

- Enterprise Mesh
- 802.11k
- 256-QAM on the 2.4 GHz band
- Modem Support
- Radio Frequency Test (RFT)
- Real-time Transport Protocol (RTP) Analysis

AP Console Password

Starting from ArubaOS 6.4.4.0, the AP console password is enabled by default. If the console password is configured, you must enter this password to get AP console access. If not configured, the controller generates a default random password which can be viewed by executing the **encrypt disable** command followed by the **show ap system-profile <profile-name>** command.

Adaptive Radio Management (ARM)

New Default ARM profiles

ArubaOS 6.4.4.0 introduces two new default ARM profiles, **default-a**, for 5 Ghz radios, and **default-g**, for 2.4 GHz radios. Previous 6.4.x releases support a single **default** ARM profile applicable to both radio bands. Some of the configuration parameters in these two new ARM profiles have different default values than the **default** ARM profile in previous releases. View a list of these values in Table 3.

When you upgrade to ArubaOS 6.4.4.0 or later from a pre-6.4.4.0 release, any changes you made to the **default** ARM profile will be applied to both the new **default-a** and **default-g** profiles. If the **default** profile was *not* modified, that profile will be removed when the new **default-a** and **default-g** profiles are created.

Any user-created ARM profiles will not be modified during the upgrade, and will retain all their existing values.

Table 3: *ARM Profile Default Value Changes*

New default-a profile settings	New default-g profile settings	Original default profile settings
• max-tx-power 18 dBm • min-tx-power 12 dBm • error-rate-threshold 70% • error-rate-wait-time 90 sec	• max-tx-power 9 dBm • min-tx-power 6dBm • error-rate-threshold 70% • error-rate-wait-time 90 sec	• max-tx-power 127 dBm • min-tx-power 9 dBm • error-rate-threshold 50% • error-rate-wait-time 30 sec

Base OS Security

MOBIKE Support for Remote Access Clients

ArubaOS supports IKEv2 Mobility and Multihoming (MOBIKE) protocol for remote access clients. This support updates IPsec and datapath entries after failover of clients performing IKEv2 VPN from:

- wireless to cellular with MOBIKE
- one wireless network to another wireless network (that is, whenever IP address of remote access VPN client changes)

Branch Controllers

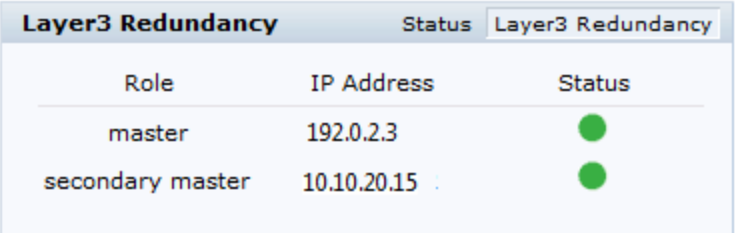
Redundant Master Controller

An 7000 Series branch controller can be configured for a redundant secondary master controller. This prevents a scenario where a master controller acts as a single point of failure if the link to the master goes down, or a co-located Master-Standby VRRP controller pair fail due to a network failure or local natural disaster.

The IP address of a secondary, backup master controller can be defined for a branch controller during the Zero-touch provisioning process, and is either defined in a DHCP server, is manually entered into the branch controller during the initial startup dialog, or defined via an Activate server.

The status of the branch's connection to a primary and secondary master controller appears in the Layer 3 Redundancy section of the WAN dashboard page of the branch controller WebUI

Figure 1 *Branch Controller Redundancy Status*



Override Local Network Destination

This feature provides a scalable solution to create a local net destination override. To implement this feature, a new sub-command, **host vlan – offset** under the **netdestination** configuration command is introduced.

Scalable FQDN based site to site IPSEC tunnels

This feature supports scalable solution to deploy Site-to-Site tunnels. The enhancement provides flexibility of configuring FQDN as peer-ip which allows the user to configure same FQDN across different branches which resolve to different IP addresses locally based on the local DNS setting, allows configuring of src-net within crypto map as VLAN and provides support for factory certificates for Site-to-Site that allows the customer to use TPM certs and reduce complication of certificate configuration process.

IP NAT Outside

Starting from ArubaOS 6.4.4, all outbound traffic now can enable NAT with the IP address of the VLAN interface as the source address; while the locally routed traffic is sent without any address translation.

Client Match

MU-MIMO Steering

Multi-user MIMO (MU-MIMO) Steering, groups multi-user-capable (MU-capable) clients to maximize the likelihood of MIMO transmissions, which increases downstream throughput performance in 802.11ac Wave 2 (gen 1) APs. MU-MIMO runs on MU-capable clients with traffic flows and PHY channels compatible for multi-user transmissions. Client Match steers and aligns MU-MIMO-capable clients with MU-MIMO-capable radios using SNR values. Multiple MU-MIMO-capable clients can be grouped together on a MU-MIMO-capable radio.

Controller-Platform

7240XM Controller

The 7240XM controller is a variant of the 7240 controller. It has an eXtended Memory (XM) of 16 GB Random Access Memory (RAM) and flash memory space enabling better throughput and scaling capabilities. The 7240XM controller has the same number of Input/Output (I/O) ports and other hardware capabilities as that of the 7240 controller.

Modem Support on 7000 Series Controllers

The following USB modems are supported on the 7000 Series controllers:

- Pantech 4G LTE Global USB modem UML290
- Verizon 4G LTE USB modem UML295
- Netgear AirCard 313U USB modem
- Netgear AirCard 320U USB modem
- Netgear AirCard 330U USB modem

For up-to-date information on inter-operation with popular Wi-Fi devices and other non-Wi-Fi peripherals, refer to the interoperability web page located here.

Controller Flash Wipe Out

Starting from ArubaOS 6.4.4.0, the **wipe out flash** command is introduced. This command erases all data including configuration, logs, license keys, flash backup files and formats the flash file system in the controller.

Execute this command only when the controller is taken out of service or decommissioned.

Controller-Routing

Associate Routing ACLs to Site-to-Site VPNs

A new configuration parameter in the **Configuration > Advanced Services > VPN Services > Site-to-Site** page allows you to associate a routing policy to an IPsec map for a site-to-site VPN. When you associate a routing ACL to inbound traffic on the VPN tunnel interface, that ACL can forward traffic as normal, route traffic to a nexthop router on a nexthop list, or redirect traffic over an L3 GRE tunnel or tunnel group.

Associate Routing ACLs to L3 GRE tunnels

A new configuration parameter in the **Configuration** > **Network** > **IP** > **GRE Tunnels** page allows you to associate a routing policy to a L3 GRE tunnel. When you associate a routing ACL to inbound traffic on a controller terminating an L3 GRE tunnel, that ACL can forward traffic as normal, route traffic to a nexthop router on a nexthop list, or redirect traffic over an L3 GRE tunnel or tunnel group.

VPNs

Compression in Site-to-Site VPNs

IKEv2 site-to-site VPNs between master and local 7000 Series controllers support traffic compression between those devices. Select the **IP Compression** checkbox on the **Configuration > Advanced Services > VPN Services > Site-to-Site** page to enable compression on an IPsec map for traffic in a site-to-site tunnel. When this hardware-based compression feature is enabled, the quality of unencrypted traffic (such as Lync or Voice traffic) is not compromised by increased latency or decreased throughput.

Voice and Video

Skype for Business SDN Interface 2.2 Support

The controller supports Skype For Business SDN Interface 2.2. This API provides an interface to the controller to access network diagnostic data in order to monitor Lync/Skype for Business traffic and optimize the quality of service. This API applies to Lync Server 2010, 2013, and Skype for Business 2015.

Skype for Business Media Classification Support

The controller supports Microsoft's new Skype for Business solution. this was earlier called Microsoft Lync. Starting from this release, the controller supports media classification for Skype for Business.

High Throughput 20 MHz Support for Video Multicast

You can now configure Modulation Coding Scheme (MCS) rates for video multicast. MCS is an important setting because it provides for potentially greater throughput. You can configure the **multicast-rate** parameter from the **wlan ssid-profile**.

NOTE

This feature is supported in all 802.11n -capable APs. This feature is not supported in 320 Series AP.

WebUI Enhancements

Uplink Manager

You can now configure the uplink manager settings on master and local controllers using the **Configuration>Network > Controller > System Settings** page of the controller WebUI. In previous releases, this feature was only configurable through the command-line interface of a master or local controller. The uplink manager also includes the **health-check** parameter to monitor the availability and quality of the connection between a master controller and branch controller over each of the WAN interfaces.

WebUI Absolute Session Timeout

Starting from ArubaOS 6.4.4.0, you can set an absolute session time for WebUI after which the WebUI session times out post a successful authentication.

WLAN Management System (WMS) Enhancements

Optimizing Classification Behavior

You can now configure APs to periodically send WMS a list of monitored devices that are still unclassified. Once the WMS receives this list, a classification message is sent from the WMS to the AP, to classify each unclassified device.

Managing List of Valid Exempt Clients

The administrator can now configure clients to be exempted from valid station protection and valid station misassociation detection by adding the mac-address of those devices to the validexempt-list.

Chapter 3
Regulatory Updates

This chapter describes the regulatory update in this release.

Contact your local Aruba sales representative about device availability and support for your country.

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.

The following Downloadable Regulatory Table (DRT) file versions are supported in ArubaOS 6.4.4.0:

- DRT-1.0_51685

For a complete list of countries certified with different AP models, refer to the respective DRT release notes at support.arubanetworks.com.

This section describes the issues resolved in this release.

802.1X

Table 4: *802.1X Fixed Issues*

Bug ID	Description
121447 122157	**Symptom:** Users were not able to establish connectivity and the logs display **received eapol-pkt before assos** error message. This issue is resolved by resetting a timer. **Scenario:** This issue was observed when users tried to connect to a 802.1X SSID and was observed in controllers running ArubaOS 6.4.2.8. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.8.

AirGroup

Table 5: *AirGroup Fixed Issues*

Bug ID	Description
118239 118318 119634 119648 120107 120940 122388 123003 124336 124483	**Symptom:** A multicast DNS (mDNS) memory leak was observed in controllers. This issue is resolved by removing an invalid missing record timer. **Scenario:** This issue was observed when the global credit timer used to clean up the memory allocated for AirWave messages was terminated. This issue was observed in controllers running ArubaOS 6.4.2.6 but was not limited to any specific controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.6.
123510	**Symptom:** When connecting, AirGroup users were randomly assigned logon roles. This issue is resolved by changing the mechanism that checks if an AirGroup user receives an IP address and assigns employee roles. **Scenario:** This issue was observed when the AirGroup user role rolled back from employee role to logon role because the 802.1X authentication took more than 15 seconds or 3 re-transmits (for example, when changing from AP low RADIUS server, poor RF environment, or so on). This issue was observed in controllers running ArubaOS 6.4.3.1, but was not limited to any specific controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.1.

Air Management-IDS

Table 6: *Air Management-IDS Fixed Issues*

Bug ID	Description
115601	**Symptom:** The **Age** field in the Real-time Locating Systems (RTLS) station report displayed incorrect values. This issue is resolved by fixing the byte ordering when converting the value from host network order to network byte order. **Scenario:** This issue was observed in AP-200 Series access points connected to controllers running ArubaOS 6.4.1.0 or later versions. **Platform:** AP-200 Series access points. **Reported Version:** ArubaOS 6.4.2.3.
120280	**Symptom:** AP-200 Series access points were unable to detect neighbor SSIDs in the Air Monitor mode (AM-mode). This issue is resolved by disabling the VAP for bridge or d-tunnel only for AP mode and enabling the VAP for monitoring mode. **Scenario:** This issue was observed in AP-200 Series access points connected to controllers running ArubaOS 6.4.3 FIPS version. **Platform:** AP-200 Series access points. **Reported Version:** ArubaOS 6.4.3.2.

AP Datapath

Table 7: *AP Datapath Fixed Issues*

Bug ID	Description
115787	**Symptom:** Users were unable to get an IP address from some APs, when they connected to a split-tunnel Service Set Identifier (SSID). The fix ensures that VLAN/multicast entries are changed according to the L2 user entry and not an L3 user entry when setting the Access Control List (ACL). **Scenario:** This issue was observed in AP-225 access points connected to 7210 controllers running ArubaOS 6.4.2.5. **Platform:** AP-225 access points. **Reported Version:** ArubaOS 6.4.2.5.
116474	**Symptom:** Access Control Lists (ACLs) using firewall rules with domain names did not work with AP-205 access points. This issue is resolved by modifying the data sequence. **Scenario:** This issue was caused by a failed DNS resolution. This issue was observed in AP-205 access points connected to controllers running ArubaOS 6.4.2.5 in a split-tunnel forwarding mode. **Platform:** AP-205 access points. **Reported Version:** ArubaOS 6.4.2.5.

AP-Platform

Table 8: *AP-Platform Fixed Issues*

Bug ID	Description
100296	**Symptom:** A controller displayed the error message **An internal system error has occurred at file sapd_sysctl.c function sapd_sysctl_write_param line 102 error Error opening /proc/sys/net/aruba000/11r: No such file or directory** repeatedly. This issue is resolved by adding a check before resetting the **dot11r/hotspot** parameter when the radio is operating in soft-ap mode. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.1.6 but was not limited to any specific controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.6.
107806	**Symptom:** When a wireless client associated with a bridge forwarding mode Service Set Identifier (SSID), some of the Gratuitous ARP (GARP) packets from the client had an incorrect VLAN tag ID. This issue is resolved by sending GARP packets with the VLAN ID when the client successfully associates with the bridge forwarding mode SSID. **Scenario:** To support mobility, the AP counterfeited GARP requested for the clients, but the GARP request did not use the VLAN tag ID. This issue was observed in 7200 controllers running ArubaOS 6.2.1.7. **Platform:** 7200 controllers. **Reported Version:** ArubaOS 6.2.1.7.
109542	**Symptom:** The access point rebooted multiple times due to a crash in the Station Management (STM) module. This issue is resolved by parsing AIE (ARUBA STM IE) first when processing association and re-association requests. **Scenario:** This issue was observed when the client sent malformed association request to the STM module. This issue was observed in AP-220 Series access point connected to controllers running ArubaOS 6.4.1.0. **Platform:** AP-200 Series access points. **Reported Version:** ArubaOS 6.4.1.0.
110139	**Symptom:** A non-CPSec Access Point (AP) terminating on a backup controller failed to fallback to the primary controller although it lost connection with the backup controller. However, after the non-CPSec AP rebooted, it connected to the primary controller. This issue is resolved by updating the non-CPSec AP so that it switches between primary and backup controller during connection loss. **Scenario:** This issue was observed when CPSec was disabled. This issue is not limited to a specific controller model or ArubaOS release version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.13.
111587	**Symptom:** The master controller did not respond when the **show ap tech-support** command was executed after a access point (AP) terminated on the local controller. This issue is resolved by making code level changes to the SAPM process. **Scenario:** This issue was observed when the CLI request was blocked by the AP firewall as it did not have IPsec connection to the master controller. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.8.
112019	**Symptom:** A crash was observed on a DFS channel supported by AP-115 access point. The log files listed the reason for the crash as **<4>ath data bus error: cause 0xc080841c** . The fix ensures that the radio is not accessed during radio reset or sleep. **Scenario:** This issue was observed in AP-115 access points connected to controllers running ArubaOS 6.4.2.3. **Platform:** AP-115 access points. **Reported Version:** ArubaOS 6.4.2.3.

Table 8: *AP-Platform Fixed Issues*

Bug ID	Description
113103	**Symptom:** AP-103H access point rebooted randomly without displaying the reboot cause in the event logs. This issue is resolved by increasing the buffer size. **Scenario:** This issue was observed only after executing the **show ap blacklist-clients** command, which caused memory overflow and rebooted the access point. **Platform:** AP-103H access points. **Reported Version:** ArubaOS 6.4.2.0.
114495	**Symptom:** An access point (AP) transmitted DHCPv6 solicit messages even when the **M** flag in Router Advertisement (RA) was set to 0 and the **O** flag was set to 1. This issue is resolved by implementing internal code changes to ensure that the AP sends an **Information-Request** message to obtain only the configuration settings. **Scenario:** This issue occurred when an AP sent a solicit message instead of a DHCPv6 information request. This issue was observed in an IPv6 network in 600 Series controllers running ArubaOS 6.4.2.3. **Platform:** 600 Series controllers. **Reported Version:** ArubaOS 6.4.2.3.
115235	**Symptom:** The **ap show tech support <ap-name>** command displayed the message **kernel message-OS_CANCEL_TIMER failed!!**. This issue is resolved by removing the error log which indicates a harmless event and using a debug counter as an alternative. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.2.5 but was not limited to any specific controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.5.
116882	**Symptom:** All access points in the network failed to respond and displayed **2ID** flags in the **Monitoring > CONTROLLER > Access Points** page of the controller WebUI. This issue is resolved by rejecting clients with a spurious MAC address. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.2.0 in a master-standby topology. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.0.
117507	**Symptom:** The AP packet capture tool did not insert a dummy FCS when sending a TX frame. This issue is resolved by inserting a dummy FCS when sending a TX frame. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.3.1. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.1.

Table 8: *AP-Platform Fixed Issues*

Bug ID	Description
118120	**Symptom:** Multiple DHCP processes were running even though the access points were connected to a network with no DHCP in the AP VLAN. This issue is resolved by terminating all others process except the DHCP process when restarting the DHCP process. **Scenario:** This issue was observed when configuring the static IPv6 addresses on the access points and connecting them to a network without a DHCP server. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.6.
121740 122374 122539 122542 122914 123026 123126 123152 123563 123761 124000 124439 124605	**Symptom:** Clients failed to associate with an Access Point (AP) because the **Station Management** (STM) process in the AP was busy. This issue is resolved by enhancing the WLAN driver. **Scenario:** This issue was observed when client match was enabled and a controller moved the clients from one AP to another. This issue was observed on AP-110 Series, AP-120 Series, and AP-130 Series access points connected to controllers running ArubaOS 6.3.1.x, 6.4.2.x, or 6.4.3.x. **Platform:** AP-110 Series, AP-120 Series, and AP-130 Series access points. **Reported Version:** ArubaOS 6.4.2.9.
121937	**Symptom:** A user was unable to configure AP-200 Series access points in bridge mode for ArubaOS 6.4.3.2-FIPS. This issue is resolved by deleting the bridge mode restrictions. **Scenario:** This issue was observed only in ArubaOS 6.4.3.2-FIPS version as a bridge mode restriction was applied to disable bridge and d-tunnel mode on AP-200 Series access points. **Platform:** AP-200 Series access points. **Reported Version:** ArubaOS 6.4.3.2.

AP-Wireless

Table 9: *AP-Wireless Fixed Issues*

Bug ID	Description
105089	**Symptom:** The wireless clients experienced packet loss when connected to AP-100 Series and AP-130 Series access points where the multicast used Dynamic Multicast Optimization (DMO). This issue is resolved by reducing the retry transmission rate for AP-105/AP-135 access points using DMO mode. **Scenario:** This issue was observed in AP-100 Series and AP-130 Series access points where the DMO enabled an SSID profile and the client did not send ACK packets when receiving high 11n rate data. **Platform:** AP-100 Series and AP-130 Series access points. **Reported Version:** ArubaOS 6.4.1.0.
108650	**Symptom:** When clients associated with an AP, some of them exhibited high retry rates than expected. The retry rates were observed in the controller dashboard, CLI, or AP radio statistics. This issue is resolved by reducing the retry transmit rate for AP-90 Series, AP-100 Series, and AP-130 Series access points. **Scenario:** This issue was observed in APs running ArubaOS 6.1.x, ArubaOS 6.3.x, or ArubaOS 6.4.x. **Platform:** AP-90 Series, AP-100 Series, and AP-130 Series access points. **Reported Version:** ArubaOS 6.3.1.9.
109200 111257	**Symptom:** AP-225 access point crashed occasionally after upgrading to ArubaOS 6.3.1.12. This issue is resolved by validating Socket Buffer (SKB) and recording information from invalid SKB. **Scenario:** This issue was observed in AP-225 access points connected to controllers running ArubaOS 6.3.1.12 with AirTime Fairness (ATF) enabled. **Platform:** AP-220 Series access points. **Reported Version:** ArubaOS 6.3.1.12.
110939 114326	**Symptom:** The CPU load on AP-135 access point was high when there was an increase in the number of customers using video meetings. This issue is resolved by calculating the CPU usage correctly. **Scenario:** This issue was observed in AP-135 access points connected to controllers running ArubaOS 6.3.1.5. **Platform:** AP-135 access points. **Reported Version:** ArubaOS 6.3.1.5.
112246	**Symptom:** The **show ap remote bss-table** command displayed the Effective Isotropic Radiated Power (EIRP) value as 0. This issue is resolved by adding the actual EIRP and the maximum EIRP in the SAPD message. **Scenario:** This issue occurred when a new VAP was added and the **show ap remote bss-table** command was issued. This issue was observed in controllers running ArubaOS 6.x and was not specific to any controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.10.
112640	**Symptom:** A user experienced loss of multicast and unicast data. This issue is resolved by clearing the Network Allocation Vector (NAV) radio register when beacon fails. **Scenario:** This issue was observed rarely in specific RF environments with very short intervals of WiFi/non-WiFi spurs in the air or because of a hardware problem. This issue was observed in AP-125 access points connected to controllers running ArubaOS 6.4.2.3. **Platform:** AP-125 access points. **Reported Version:** ArubaOS 6.4.2.3.
113845	**Symptom:** The **show user-table** command output occasionally did not display bridge mode users. The fix ensures that the bridge mode users are always displayed when the command is executed. **Scenario:** This issue was observed when the client was in power save mode and the chipset driver did not send deauthentication frame with the reason, client-match. **Platform:** All RAPs. **Reported Version:** ArubaOS 6.3.1.10.

Table 9: *AP-Wireless Fixed Issues*

Bug ID	Description
114447	**Symptom:** Users experienced interference when they made calls using Ascom i75 voice phones. This issue is resolved by changing the value of the draining threshold from 2 to 5. **Scenario:** This issue was observed in controllers after upgrading them from ArubaOS 6.3.1.5 to ArubaOS 6.4.2.4. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4.
115865	**Symptom:** Clients experienced connectivity issues on the G radios of AP-200 Series access points. This issue is resolved by removing stale striping IP entries whenever ap-lacp profile is changed. **Scenario:** This issue was observed when striping-ip was configured in ap-lacp-striping-ip where the same striping-ip was earlier configured but removed on another controller. Hence, a stale route cache entry for the striping-ip was left over on the other controller. This issue was observed in AP-200 Series access points connected to 7240 controllers running ArubaOS 6.4.2.5. **Platform:** AP-200 Series access points. **Reported Version:** ArubaOS 6.4.2.5.
115999	**Symptom:** AP-114 access point crashed with **Enabling kernel refresh of watchdog** error. This issue is resolved by increasing the Linux kernel stack size. **Scenario:** This issue was observed due to Linux kernel stack overflow on AP-114 access points running ArubaOS 6.3.1.7. **Platform:** AP-114 access points. **Reported Version:** ArubaOS 6.3.1.7.
116247	**Symptom:** Alcatel-Lucent OMNITOUCH 8118 phones were unable to successfully place calls. The fix ensures that the clients are able to place calls through OMNITOUCH 8118 phones. **Scenario:** This issue was observed when the access points were upgraded from AP-135 to AP-225, This issue was not limited to a specific controller model or ArubaOS release. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.14.
116457	**Symptom:** A wrong NF value was displayed in beacon messages that were inaccessible. This issue is resolved by displaying the correct NF value. **Scenario:** This issue was observed in RAP-109 when connected to controllers running ArubaOS 6.3.1.3. **Platform:** RAP-109 access points. **Reported Version:** ArubaOS 6.3.1.3.
116532	**Symptom:** The **ap packet-capture** command failed to show all packets sent and received by the user. This issue is resolved by sending all MAC Protocol Data Units (MPDU) of Aggregated MAC Protocol Data Unit (AMPDU) to the ASAP module. **Scenario:** This issue was observed on AP-225 access points associated with controllers running ArubaOS 6.4.2.5. **Platform:** AP-220 Series access points. **Reported Version:** ArubaOS 6.4.2.5

Table 9: *AP-Wireless Fixed Issues*

Bug ID	Description
116771	**Symptom:** An Access Point (AP) rebooted after an **Out of memory** message was displayed in the log file. This issue is resolved by modifying the counter that determines the out of memory condition. **Scenario:** This issue was observed in the upstream throughput test when an incorrect counter determined the out of memory condition. This issue was observed in AP-200 Series access points connected to controllers running ArubaOS 6.4.x.x. **Platform:** AP-200 Series access points. **Reported Version:** ArubaOS 6.4.2.6.
118343 118199	**Symptom:** AP-115 access point sent out of order multicast packets. Clients reported **TKIP MIC** error and disconnected during heavy multicast traffic. This issue is resolved by using software Temporal Key Integrity Protocol (TKIP) instead of split TKIP. **Scenario:** This issue was observed in AP-115 access points connected to 3600 controllers running ArubaOS 6.3.1.x. **Platform:** AP-115 access points. **Reported Version:** ArubaOS 6.3.1.x.
120117 123313 124081	**Symptom:** AP-225 access point crashed. This issue is resolved by changing how the BSS configuration is accessed. **Scenario:** This issue was observed when an access point received a management action frame of unsupported type. This issue was observed in AP-225 access points connected to controllers running ArubaOS 6.3.1.9. **Platform:** AP-225 access points. **Reported Version:** ArubaOS 6.3.1.9.

Base OS Security

Table 10: *Base OS Security Fixed Issues*

Bug ID	Description
119088	**Symptom:** Clients running iOS 9 were not able to authenticate with M3 controllers in EAP-TLS mode but clients running iOS 8 were able to authenticate with the same controller. This issue is resolved by using the TLS version from the handshake protocol header. **Scenario:** This issue was observed in clients running iOS 9 connected to controllers running ArubaOS 6.4.3.x. This issue was observed because of the use of negotiated TLS version instead of the TLS version from the handshake protocol to calculate the pre-master secret key. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.x.
120859	**Symptom:** Clients running iOS 9 and OS X 10.11 were not able to associate using EAP-PEAP. This issue is resolved by modifying the length field in the EAP header to accept a value greater than or equal to 6 bytes. **Scenario:** This issue was observed when both EAP-PEAP and EAP-TLS were configured on a controller and only EAP-PEAP was supported. This issue was observed in controllers running ArubaOS 6.4.2.9. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.9.
122055 123476	**Symptom:** The **extifmgr** process crashed frequently. The fix ensures that the **extifmgr** process does not crash. **Scenario:** This issue is observed in access points connected to controllers running ArubaOS 6.4.2.7. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.7.

Table 10: *Base OS Security Fixed Issues*

Bug ID	Description
123937	**Symptom:** On the AirWave WebUI, the Connection Mode for wireless clients was displayed as 802.11b although the clients were connected to either the 802.11a or 802.11g band in the controller. This issue is resolved by sending the PhyType and HTMode MIBs as per the MIB definition while using SNMP traps. **Scenario:** The AirWave WebUI displayed incorrect values using SNMP traps for polling. Although the SNMP traps carried the PhyType and HTMode information, it was not part of the standard MIB definition. This issue was observed in controllers running ArubaOS 6.4.2.3 **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.3.

Captive Portal

Table 11: *Captive Portal Fixed Issues*

Bug ID	Description
115484	**Symptom:** When a custom background image was used in the captive portal configuration, the background image was not displayed although the functionality of captive portal worked as expected. This issue is resolved by changing how the background image is utilized in the captive portal. **Scenario:** This issue occurred when a custom background image was used for a captive portal. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.0.
116559	**Symptom:** The captive portal login page did not load properly for Apple devices that used iPass Wireless Internet Service Provider roaming (WISPr) clients or devices that used Boingo WISPr clients. This issue is resolved by adding validations to bypass the meta-refresh mechanism for clients that use the iPass or Boingo user-agent. **Scenario:** This issue was observed in ArubaOS 6.4.x and 6.3.x with captive portal page enhancements. The captive portal page enhancements that were introduced to serve an interim landing page with meta-refresh tag to filter non-browser-based clients did not work for some clients. This issue was not limited to any specific controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.6.

Controller-Datapath

Table 12: *Controller-Datapath Fixed Issues*

Bug ID	Description
114961	**Symptom:** A Remote AP (RAP) failed to associate with a controller. This issue is resolved by clearing stale user entries. **Scenario:** This issue was observed when multiple user entries were found after the controller was upgraded to ArubaOS 6.4.0.3. This issue was observed in controllers running ArubaOS 6.4.x. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.0.3.
116868	**Symptom:** A camera failed to communicate with the video server through IPsec tunnel. This issue is resolved by forwarding the second IPsec fragment correctly. **Scenario:** This issue was observed when clients sent packets through IPsec tunnel with **DF** flag set in the IP header. The IPsec frame was fragmented and was not handled correctly by the controller running ArubaOS 6.4.x.x. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.1.
117543	**Symptom:** AppRF failed to block restricted category sites randomly. This issue is resolved by improving the WebCC and AppRF rule resolution method to converge on the WebCC action faster. **Scenario:** This issue was observed when WebCC rules followed by AppRF rules in a user role ACL needed more packets to classify the application site correctly. As a result, the WebCC rule action was not taken or was delayed. This issue was observed in 7000 Series and 7200 Series controllers running ArubaOS 6.4.2.6. **Platform:** 7000 Series and 7200 Series controllers. **Reported Version:** ArubaOS 6.4.2.6.
118194 119060 123475	**Symptom:** A local controller crashed and rebooted unexpectedly. The log files for the event listed the reason for the reboot as **Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2)**. This issue is resolved by appropriately handling the AppRF application registration. **Scenario:** The SDK update to ArubaOS 6.4.2.7 did not include certain file changes. So, some AppRF applications added by Aruba were missed out. As a result, when the **show datapath session dpi counters** command was executed, fpapps crashed for app IDs that were out of range. This issue was observed in 7220 controllers running ArubaOS 6.4.2.7. **Platform:** 7220 controllers. **Reported Version:** ArubaOS 6.4.2.7.
118304	**Symptom:** After a controller rebooted, **Monitor Gratuitous ARP attack** and **STUN Based Traversal firewall** options were automatically enabled even though they were disabled before. The fix ensures that the **Monitor Gratuitous ARP attack** and **STUN Based Traversal firewall** options are not automatically enabled. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.2.6 or later versions. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.6.
119311	**Symptom:** A controller rebooted unexpectedly. The log file for the event listed the reason as **Reboot Cause: Datapath timeout (Intent:cause:register 56:86:0:2)**. This issue is resolved by not sending the packets for encryption if the station is not ready to accept data or on the verge of getting deleted. **Scenario:** This issue was observed only in 802.11ac clients with the **AMSDU Transmit** parameter enabled on a 7200 Series controller running ArubaOS 6.4.2.x or 6.4.3.x. This issue was observed under the following circumstances: • A race condition occurred when encrypting data of 802.11ac clients. • The client traffic was encrypted. • The station was disassociated simultaneously. **Platform:** 7200 Series controllers. **Reported Version:** ArubaOS 6.4.2.6.

Table 12: *Controller-Datapath Fixed Issues*

Bug ID	Description
120735	**Symptom:** Ascom phones connected to AP-125 access points aged out randomly. This issue is resolved by ensuring that the current time is greater than the time since the last frame was received from the client before performing the ageout check. **Scenario:** This issue is observed in AP-125 access points connected to 6000 controllers running ArubaOS 6.4.2.6. **Platform:** AP-125 access points. **Reported Version:** ArubaOS 6.4.2.6.
122120	**Symptom:** By default, the asterisk wildcard was appended to the **netdetsination** provided by the user. This issue is resolved by modifying the DNS snooping to check if the **netdestination** is an absolute URL or a wildcard URL. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.2.4. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4.
121252 124262	**Symptom:** The datapath module crashed when sending AirPlay audio packets (TCP port 5000) with policy-based routing feature enabled. This issue is resolved by rectifying an inconsistency in session states for AirPlay audio. **Scenario:** This issue was observed in standalone controllers running ArubaOS 6.4.3.2 with AirPlay audio traffic and policy-based routing configuration on user-role enabled. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.5.
122033	**Symptom:** Route-acl attachment to user role was not preserved after reloading a standby controller. This issue is resolved by generating the routing policy map on the standby controller after a configuration snapshot. **Scenario:** This issue was observed after reloading a standby controller with route-acl. This issue was observed in controllers running ArubaOS 6.4.3.x in master-standby topology. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.2.

Controller-Platform

Table 13: *Controller-Platform Fixed Issues*

Bug ID	Description
118599 123996 124152	**Symptom:** A controller rebooted unexpectedly. The log file for the event listed the reasons as **kernel panic**, **hard watchdog reset**, or **soft watchdog reset**. This issue is resolved by correcting the SOS coredump path. **Scenario:** This issue occurred when SOS coredump was triggered in 7000 Series or 7200 Series controllers running ArubaOS 6.4.x. **Platform:** 7000 Series and 7200 Series controllers. **Reported Version:** ArubaOS 6.4.2.6
118935	**Symptom:** Trivial File Transfer Protocol (TFTP) download did not work when upgrading ArubaOS. This issue is resolved by deleting the AP-image/ancillary files to free the space on the controller partition where the ArubaOS image is loaded. **Scenario:** This issue was observed in 600 Series controllers running ArubaOS 6.4.2.8. **Platform:** 600 Series controllers. **Reported Version:** ArubaOS 6.4.2.8.
94286 119559	**Symptom:** A 650 controller failed to upgrade to ArubaOS 6.4.2.6-FIPS because of insufficient memory. The fix ensures that there is enough memory before upgrading to ArubaOS 6.4.2.6-FIPS. **Scenario:** This issue was observed in 650 controllers running ArubaOS 6.4.2.5-FIPS. **Platform:** 650 controllers. **Reported Version:** ArubaOS 6.4.2.5-FIPS.
122773 123921 124070 124130 124204 124322	**Symptom:** A master controller rebooted unexpectedly. The log files for the event listed the reason as **kernel panic**. This issue is resolved by displaying a warning message during an invalid Direct Memory Access (DMA) type error. **Scenario:** To transfer a packet from the control plane to the datapath, a message was sent to the DMA to copy the packet to the SOS. To confirm the transfer, DMA sent a message and checked the descriptor for the packet buffer pointer, which was NULL. This resulted in a kernel crash with a NULL pointer exception. This issue was observed in 7000 Series and 7205 controllers running ArubaOS 6.4.3.2. **Platform:** 7000 Series and 7205 controllers. **Reported Version:** ArubaOS 6.4.3.2.

DHCP

Table 14: *DHCP Fixed Issues*

Bug ID	Description
108349	**Symptom:** When a client connected to a Wi-Fi network, there was a delay in getting an IP address from the DHCP server. The delay in obtaining the IP address was due to the delay introduced by the Process Application Programming Interface (PAPI) protocol to communicate the station information from authentication to DHCP relay agent process. The fix addresses this delay by using Global Shared Memory (GSM) to retrieve the station information instead of the PAPI protocol. **Scenario:** When an **ip helper-address** was configured on a VLAN interface together with **option-82 essid** or **option-82 ap-name**, the DHCP process dropped the first DHCP packet from the client while it waited for the authentication manager to respond. This issue was observed in controllers running ArubaOS 6.1.3.x, ArubaOS 6.3.x, or ArubaOS 6.4.x. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.7.

Hardware Management

Table 15: *Hardware Management Fixed Issues*

Bug ID	Description
112912	**Symptom:** When the **show inventory** command was executed, the **System Serial#** value was displayed as **Unknown**. This issue is resolved by increasing the **nvram lock retry** count to 30. **Scenario:** This issue was observed because of the limited number of attempts to acquire the nvram lock. This issue was observed in controllers running ArubaOS 6.4.0.2. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.0.2.

IPsec

Table 16: *IPsec Fixed Issues*

Bug ID	Description
115565	**Symptom:** Missed heartbeats were observed between an AP and controller. This is issue is resolved by disabling the Digital Pre-Distortion (DPD) trigger for PSK based RAPs. **Scenario:** This issue was observed in RAPs deployed in the PSK mode running ArubaOS 6.4.0.3. **Platform:** Access points deployed as PSK RAPs. **Reported Version:** ArubaOS 6.4.0.3.
121339	**Symptom:** The strength of IKE, based on the length of the symmetric cipher key, was lower than the strength of ESP, which was a violation of Common Criteria requirements. This issue is resolved by changing the strength of IKE to be equal to or greater than the strength of ESP. This change applies only to ArubaOS FIPS versions. **Scenario:** This issue was not specific to any controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.4.0.
121559	**Symptom:** A controller sent NO_PROPOSAL_CHOSEN response instead of INVALID_KE_PAYLOAD response to IKE_SA_INIT message after finding a matching policy but with different a DH group. This issue is resolved by sending INVALID_KE_PAYLOAD response proposing the acceptable DH group to IKE_SA_INIT message after finding a matching policy but with different a DH group. **Scenario:** This issue was observed when all ISAKMP policies with DH group 2 were disabled and a new policy similar to RAP default policy was created but with DH group 14 instead of DH group 2 and the RAP failed to start because it proposed only DH group 2 in loops. This issue was not specific to any controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.3.

Master-Local

Table 17: *Master-Local Fixed Issues*

Bug ID	Description
121996	**Symptom:** DNS server IP longer than 10 characters failed bulk edit resulting in DNS field set to 0.0.0.0. The fix ensures that a controller sets the DNS server IP correctly. **Scenario:** When you bulk edit a DNS server IP lesser than 10 characters long (example: x.x.x.x), the controller sets the IP correctly. But for DNS server IP longer than 10 characters (example: xx.xx.xx.xx), the controller sets the IP to 0.0.0.0. This issue was observed in controllers running ArubaOS 6.4.x but was not limited to any specific controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.0.0.

Mobility

Table 18: *Mobility Fixed Issues*

Bug ID	Description
123985	**Symptom:** When the **no ip mobile proxy auth-sta-roam-only** command was executed, an incorrect warning message, **With this command, removed mobility will be supported for only static IPv4 clients and not supported for pure IPv6/Dual Stack/Dynamic IPv4 clients**. **Please refer the User Guide for more info was displayed.** This issue is resolved by displaying the correct warning message, **With this command removed mobility will be supported for only IPv4 clients and not supported for pure IPv6/Dual Stack clients Please refer the UserGuide for more info**. **Scenario:** The incorrect message was displayed because the mobility support for IPv4 DHCP clients for ip mobile proxy was added. This issue was observed in controller running ArubaOS 6.4.3. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.0.0.

Radius

Table 19: *Radius Fixed Issues*

Bug ID	Description
115370	**Symptom:** Though the user entered correct credentials the first time, subsequent authentication failed if the user entered incorrect credentials the previous time. This issue is resolved by clearing the entries in the last server when there is an authentication failure. **Scenario:** This issue was observed when subsequent authentication requests were sent to the last server in the server-group. This issue was observed in 3600 controllers running ArubaOS 6.4.2.5. **Platform:** 3600 controllers. **Reported Version:** ArubaOS 6.4.2.5.

Remote AP

Table 20: *Remote AP Fixed Issues*

Bug ID	Description
115691	**Symptom:** When a Remote Access Point (RAP) failed back from the backup License Management System (LMS) to the primary LMS after the expiry of LMS hold timer, the wired clients obtained IP addresses but did not have connectivity. This issue is resolved by changing how the RAPs calculate the last modified time when switching from the backup LMS to the primary LMS. **Scenario:** This issue was observed in 3200 controllers running ArubaOS 6.3.1.15 in a master-master topology. **Platform:** 3200 controllers. **Reported Version:** ArubaOS 6.3.1.15.
116102	**Symptom:** Customers were not able to access uplink devices as the route-cache on the uplink of the Access Point (AP) never expired. Hence, devices were not able to send Gratuitous Address Resolution Protocol (GARP) packets. The fix ensures that the AP validates for stale ARP and then notifies the route-cache to delete the entry. **Scenario:** This issue was observed when the uplink device used the static IP address and did not send the GARP packets. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.6.

SNMP

Table 21: *SNMP Fixed Issues*

Bug ID	Description
112973	**Symptom:** The **ifSpeed** MIB entry for the 10G port was incorrect. This issue is resolved by adding the **ifSpeed** MIB for the 10G port. **Scenario:** This issue was observed in 7200 Series controllers running ArubaOS 6.3 or later. **Platform:** 7200 Series controllers. **Reported Version:** ArubaOS 6.3.1.13

Station Management

Table 22: *Station Management Fixed Issues*

Bug ID	Description
121643 121642	**Symptom:** A controller crashed and the log files were flooded with **handle_ap_message_response: BSS <MAC> nothing outstanding** warning messages. This issue is resolved by making changes to handle the expected response from GSM channel properly instead of error logging. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.3.2. This issue was observed when the Station Management (STM) process handled the responses from the BSS GSM channel incorrectly. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.2.

Unified Communication

Table 23: *Unified Communication Fixed Issues*

Bug ID	Description
114962	**Symptom:** An **unknown** error message was displayed in the **Dashboard> UCC> QoS Correction** page of the controller WebUI even though the controller modified the DSCP value. This issue is resolved by adding support for original L2 and L3 priority value displayed on the controller for RAP. **Scenario:** This issue was observed in all controllers with RAP topology. **Platform:** All RAPs. **Reported Version:** ArubaOS 6.4.2.2.
115679	**Symptom:** Session Initiation Protocol (SIP) SIP Application Layer Gateway (ALG) was unable to detect and prioritize voice calls made from Cisco Jabber client running on Android devices. This issue is resolved by fixing the Session Description Protocol (SDP) parsing issue in the SIP ALG. **Scenario:** This issue occurred due to incorrect parsing of SDP contents and was observed in controllers running ArubaOS 6.4.2.4. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4.
117456	**Symptom:** UCC dashboard and show commands, **show ucc call-info cdrs** and **show ucc statistics counter call client**, displayed the Lync call statistics for other peer-to-peer conversations even though client was not part of the Lync conversation. This issue is resolved by changing how the XML message of the external clients are handled. **Scenario:** This issue was observed when a controller received XML message for audio call, where both the client IP addresses are external to controller and one of the client's call was on-going. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.5.

Table 23: *Unified Communication Fixed Issues*

Bug ID	Description
121964	**Symptom:** The Station Management (STM) process that handles AP management and client association stopped responding and rebooted the controller. This issue is resolved by applying defensive checks in the STM process to handle errors from Process Application Programming Interface (PAPI) messages. **Scenario:** This issue was observed when the STM process stopped responding due to a datapath timeout. This issue was observed in 7220 controllers running ArubaOS 6.4.2.5. **Platform:** 7220 controllers. **Reported Version:** ArubaOS 6.4.2.5.

Webserver

Table 24: *Webserver Fixed Issues*

Bug ID	Description
121400	**Symptom:** A user is directed to the secure login page and not the default home page after captive portal authentication was completed. This issue was resolved by making internal code changes to remove the landing page from the query argument. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.1.15, ArubaOS 6.4.2.5, ArubaOS 6.4.3.0, and later versions. This issue occured when the redirect URL was not configured in captive portal profile and the original URL contained a cgi name value pair. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.5.
115304	**Symptom:** During SSL handshake for HTTPS connection establishment, a controller sent **Unrecognized name** alert to clients. Any HTTPS client or Web browser that treated this warning as a fatal error, terminated the SSL handshake and did not establish the HTTPS connection with the controller. This issue is resolved by correcting an incorrect HTTPS server configuration. **Scenario:** This issue was observed only when a custom certificate was used for Web server and Captive Portal. This issue did not affect the widely used Web browsers like, Chrome, Firefox, or Internet Explorer. However, custom applications that used .net were affected. This issue was observed in controllers running ArubaOS 6.3.x or later and was not limited to any specific controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.2.

WebUI

Table 25: *WebUI Fixed Issues*

Bug ID	Description
109986	**Symptom:** The WebUI did not list the APs to add as spectrum monitor (SM) when the AP count in SM mode was large. This issue was resolved by adding pagination support that displays up to 50 SMs per page in the WebUI. **Scenario:** This issue was observed because of missing pagination in the WebUI. This issue was observed in controllers running ArubaOS 6.3.1.13. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.13.
113679	**Symptom:** A new guest account created from GPP was assigned an incorrect lifetime value. This issue is resolved by implementing internal code changes. **Scenario:** When the date on the controller clock was set to Jan 29, 30, and 31 of 2015, and a new guest account was created from GPP, this account was assigned a lifetime value of 3 days 8 hours instead of 8 hours, the default value. This issue was observed in controllers running ArubaOS 6.4.2.4 or later. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4.
115991	**Symptom:** A user was not able to move an Access Control List (ACL) through the WebUI if it contained the **&** symbol. This issue is resolved by adding support for special characters in the ACL. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.2.4 but was not limited to any specific controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4.
117454 119171	**Symptom:** The WebUI did not display the list of connected clients. This issue is resolved by using an updated command to incrementally retrieve and display the list of connected clients in the WebUI. **Scenario:** This issue was observed because of a miscalculated index in the command that incrementally retrieved and displayed the list of connected clients. This issue was observed in controllers running ArubaOS 6.4.3.1. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.1.
117491	**Symptom:** A **JavaScript** error is displayed when a user clicked on **View Commands** option in the **Security > Authentication > Servers> Radius Server > click on radius server instance > Server Group** of the controller WEBUI page. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in all controllers running ArubaOS 6.4.3.1 or later versions. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.1.

Table 25: *WebUI Fixed Issues*

Bug ID	Description
120008	**Symptom:** A Virtual Access Point (VAP) was not deleted when the user selected **--NONE--** from the **Virtual AP** drop-down list, in **ADVANCED SERVICES > All Profiles > Wireless LAN > Virtual AP > Show Reference** page of the WebUI. An internal JavaScript code fix ensures that the VAP profile is deleted when the user selects **--NONE--** from the **Virtual AP** drop-down menu. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.3.2 but was not limited to any specific controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.2.
121622	**Symptom:** When a user attempted to delete smart configuration from the master controller through the WebUI, the error message **Config group is being used. Remove reference in whitelist before deleting** was displayed. This issue is resolved by allowing a user to delete smart configuration. **Scenario:** This issue was observed when a user had multiple config-groups with similar names and the user attempted to delete smart configuration from a master controller. This issue was observed in 7240 controllers running ArubaOS 6.4.3.2. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.2.
121653	**Symptom:** A user was not able to modify the port-channel configuration for specific gigabitethernet <slot>/<module>/<port> through smart configuration. This issue is resolved by removing a delete/add command for the port-channel configuration for specified gigabitethernet <slot>/<module>/<port> when a add/delete command for the same configuration is received. **Scenario:** This issue was observed because of the simultaneous co-existence of both add and delete commands for the port-channel configuration of a specific gigabitethernet <slot>/<module>/<port>. This issue was observed in controllers running ArubaOS 6.4.3.2 but was not limited to any specific controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.2.

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

If there is any specific bug that is not documented in this section, contact Aruba Technical Support with your case number.

802.1X

Table 26: *802.1X Known Issues*

Bug ID	Description
122266	**Symptom:** Wireless clients randomly perform full authentication while roaming to other AP. **Scenario:** This issues is seen although the Opportunistic Key Caching (OKC) setting is enabled on the WLAN SSID profile. This issue is observed in controllers running ArubaOS 6.4.2.x. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** None.

Air Management-IDS

Table 27: *Air Management-IDS Known Issues*

Bug ID	Description
118444	**Symptom:** Some access points detect other access points as spoofing access points. **Scenario:** This issue is observed in AP-225 access points connected to 7210 controllers running ArubaOS 6.4.2.6. **Platform:** AP-225 access points. **Reported Version:** ArubaOS 6.4.2.6. **Workaround:** None.
118659	**Symptom:** Users observe frequent **Block ACK DoS Attack** messages in the security log of the controller. **Scenario:** This issue is observed in AP-200 Series access points connected to 7030 controllers running ArubaOS 6.4.1.0. This issue is observed after the user upgrades to ArubaOS 6.4.2.7. **Platform:** AP-200 Series access points. **Reported Version:** ArubaOS 6.4.3.2. **Workaround:** None.

AP-Platform

Table 28: *AP-Platform Known Issues*

Bug ID	Description
119458	**Symptom:** AP reboots due to an internal system error. **Scenario:** This issue is observed in AP-125 access points connected to an M3 controller running ArubaOS 6.3.1.9. **Platform:** AP-125 access points. **Reported Version:** ArubaOS 6.3.1.9. **Workaround:** None.
123748	**Symptom:** AP-225 access points reboot continuously after a maintenance window. **Scenario:** This issue is observed because of corrupted EEPROM in the radio. This issue is observed in AP-225 access points connected to controllers running ArubaOS 6.4.2.5 **Platform:** AP-225 access points. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** None.

AP-Wireless

Table 29: *AP-Wireless Known Issues*

Bug ID	Description
116969	**Symptom:** The basic and beacon rates configuration for the Virtual Access Points (VAPs) of AP-325 access points are not specific to each SSID. **Scenario:** The rates configuration tied to the primary VAP overrides the rates configuration that is specific to other VAPs. The primary VAP (VAP0) is the VAP that comes up as aruba000 for the VAP beaconing on 5 GHz band and aruba100 for the VAP beaconing on 2.4 GHz band. The other VAPs which correspond to aruba001, aruba002, and so on on the A radio inherit the configuration from VAP0. Aruba101, aruba102, and so on are interfaces corresponding to the VAPs on the G radio which inherit the configuration from aruba100. This issue is observed in AP-325 access points connected to controllers running ArubaOS 6.4.4.0. **Platform:** AP-325 access points. **Reported Version:** ArubaOS 6.4.4.0. **Workaround:** None.
117675	**Symptom:** When a client associates with a Virtual Access Point (VAP) in tunnel mode with dynamic-wep encryption, it cannot send/receive traffic. **Scenario:** This issue is observed in AP-320 Series access points connected to controllers running ArubaOS 6.4.4.0. **Platform:** AP-320 Series access points. **Reported Version:** ArubaOS 6.4.4.0. **Workaround:** None.
117815	**Symptom:** A user cannot change the max retries setting of an access point. **Scenario:** This issue is observed in AP-320 Series access points connected to controllers running ArubaOS 6.4.4.0. **Platform:** AP-320 Series access points. **Reported Version:** ArubaOS 6.4.4.0. **Workaround:** If dynamic-wep is required, use d-tunnel mode.

Table 29: *AP-Wireless Known Issues*

Bug ID	Description
119884	**Symptom:** The client is unable to pass traffic even though it associates to an AP. **Scenario:** In the AP driver **debug client-table**, the AP association is displayed as present. However, running the **show ap remote debug association**, **show ap remote debug mgmt-frames**, and **show ap association** commands display either stale information or no information for AP association in the Station Management (STM) table. This issue is observed in AP-200 Series access points running ArubaOS 6.4.2.6. **Platform:** AP-200 Series access points. **Reported Version:** ArubaOS 6.4.2.6. **Workaround:** None.
124001	**Symptom:** AP-224 access points reboot with reason **out of memory** and clients cannot associate with the access points or send traffic. **Scenario:** This issue is observed when ARM is enabled with scanning. This issue is observed in AP-224 access points connected to controllers running ArubaOS 6.4.2.7. **Platform:** AP-224 access points. **Reported Version:** ArubaOS 6.4.2.7. **Workaround:** None.
125316	**Symptom:** On disabling an AP radio, unknown Wi-Fi packets were observed on channel 1. **Scenario:** This issue is seen when an AP radio is disabled in either 2.4 GHz or 5 GHz. This issue is observed in AP-320 Series access points running ArubaOS 6.4.4.0. **Platform:** AP-320 Series access points. **Reported Version:** ArubaOS 6.4.4.0. **Workaround:** Enable and disable the Virtual AP profile on an AP where the radio is disabled.

Controller-Datapath

Table 30: *Controller-Datapath Known Issues*

Bug ID	Description
122147	**Symptom:** The controller interface displays an incorrect MAC address of the CPPM server. **Scenario:** This issue occurs in a controller-L2 switch-CPPM served topology. The **show arp table** command displays the correct MAC address of the CPPM server whereas the **show mac-address table** command displays an incorrect CPPM MAC address. This issue is observed in controllers running ArubaOS 6.4.x. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.2. **Workaround:** None.

Controller-Platform

Table 31: *Controller-Platform Known Issues*

Bug ID	Description
119827	**Symptom:** 3600 controller does not send traffic and reboots unexpectedly even when connected directly to a PC. **Scenario:** This issue is observed in 3600 controllers running ArubaOS 6.3.1.5. **Platform:** 3600 controllers. **Reported Version:** ArubaOS 6.3.1.5 **Workaround:** None.

Monitoring

Table 32: *Monitoring Known Issues*

Bug ID	Description
119350	**Symptom:** The WLAN count for APs in the **Dashboard > Access Points** page is incorrect when the Virtual AP is configured using **AP Name** specific configuration. **Scenario:** An increment in WLAN count is observed when an AP for which the Virtual AP is configured using **AP Name** specific configuration is rebooted. This issue is observed in controllers running ArubaOS 6.4 and prior versions. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.8. **Workaround:** None.

Station Management

Table 33: *Station Management Known Issues*

Bug ID	Description
119408	**Symptom:** The controller fails to blacklist a client permanently using the WebUI. **Scenario:** Blacklisting the client shows the blacklisted timer is sometimes set to lifetime of default 1 hour instead of permanent even though the blacklist timer is set to 0 globally in CLI as well as in the Virtual AP profile. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.8. **Workaround:** None.
124275	**Symptom:** The even VLAN pool assignment pools the users in only one particular VLAN although CPPM pushes different VLANs as vendor specific VLANs. **Scenario:** This issue is observed because of a mismatch in the current VLAN usage counts between the Station Management (STM) and authentication modules. This issue is observed in controllers running ArubaOS 6.4.2.6. **Platform:** All platforms. **Reported Version:**ArubaOS 6.4.2.6. **Workaround:** None.

Webserver

Table 34: *Webserver Known Issues*

Bug ID	Description
122500	**Symptom:** When a WebUI session times out after exceeding the absolute session timeout, the WebUI login screen intermittently displays the reason as **Session is invalid** or **Session timed out** instead of **Absolute Session timed out**. **Scenario:** This issue is seen when you configure the **Absolute Session Timeout** setting from the **Configuration > Management > General > WebUI Session Timer** page of the WebUI. This issue is observed in controllers running ArubaOS 6.4.4.0. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.4.0 **Workaround:** None.

Maximum Number of NAT Pools

A controller supports a maximum of 60 NAT pools.

This chapter details software upgrade procedures. Aruba best practices recommend that you schedule a maintenance window for upgrading your controllers.

Read all the information in this chapter before upgrading your controller.

Topics in this chapter include:

Upgrade Caveats

Before upgrading to this version of ArubaOS, take note of these known upgrade caveats.

- AP LLDP profile is not supported on AP-120 Series in ArubaOS 6.4.x.
- Starting from ArubaOS 6.3.1.0, the local file upgrade option in the 620 and 650 controller WebUIs have been disabled.
- ArubaOS 6.4.x does not allow you to create redundant firewall rules in a single ACL. ArubaOS will consider a rule redundant if the primary keys are the same. The primary key is made up of the following variables:
  - source IP/alias
  - destination IP/alias
  - proto-port/service

  If you are upgrading from ArubaOS 6.1 or earlier and your configuration contains an ACL with redundant firewall rules, upon upgrading, only the last rule will remain.

  For example, in the below ACL, both ACE entries could not be configured in ArubaOS 6.4.x. When the second ACE is added, it overwrites the first.

```
(host) (config) #ip access-list session allowall-laptop
(host) (config-sess-allowall-laptop)# any any any  permit time-range test_range
(host) (config-sess-allowall-laptop)# any any any  deny
(host) (config-sess-allowall-laptop)#end
(host) #show ip access-list allowall-laptop

ip access-list session allowall-laptop
allowall-laptop
---------------
Priority  Source  Destination  Service  Action  TimeRange
--------  ------  -----------  -------  ------  ---------
1         any     any          any      deny
```

- ArubaOS 6.4.x supports only the newer MIPS controllers (7200 Series, 7000 Series, M3, 3200XM, 3400, 3600, and 600 Series). Legacy PPC controllers (200, 800, 2400, SC1/SC2) and 3200 controllers are not supported. Do not upgrade to ArubaOS 6.4.x if your deployment contains a mix of MIPS and PPC controllers in a master-local setup.
- When upgrading the software in a multicontroller network (one that uses two or more Aruba controllers), special care must be taken to upgrade all the controllers in the network and to upgrade them in the proper sequence. (See Upgrading in a Multicontroller Network on page 44.)

GRE Tunnel-Type Requirements

This section describes the important points to remember when configuring an L2 GRE tunnel with respect to tunnel-type:

- ArubaOS 6.4.4.0 continues to support L2 GRE tunnel type zero, but it is recommended to use a non-zero tunnel type.
- If both L2 and L3 tunnels are configured between end point devices, you must use a non-zero tunnel type for L2 GRE tunnels.

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 controller? Verify this information by navigating to the **Monitoring > NETWORK > All 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 controller (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS is currently on the controller?
  - Are all controllers in a master-local cluster running the same version of software?
  - Which services are used on the controllers (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 controller. 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, refer to the "Software Licenses" chapter in the *ArubaOS 6.4.x User Guide*.

Memory Requirements

All Aruba controllers store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the controller. 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 controller. After the controller 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 controller 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 controller logs, crash data, or flash backups should be copied to a location off the controller, then deleted from the controller to free up flash space. You can delete the following files from the controller 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 42 to copy the **crash.tar** file to an external server, and then execute the **tar clean crash** command to delete the file from the controller.
- **Flash Backups:** Use the procedures described in Backing up Critical Data on page 42 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 controller.
- **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 42 to copy the **logs.tar** file to an external server, and then execute the **tar clean logs** command to delete the file from the controller.

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
- Controller Logs

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 controller:

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 controller's command line:

1. Make sure you are in the **enable** mode in the controller 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 in a Multicontroller Network

In a multicontroller network (a network with two or more Aruba controllers), special care must be taken to upgrade all controllers based on the controller type (master or local). Be sure to back up all controllers being upgraded, as described in Backing up Critical Data on page 42.

NOTE

For proper operation, all controllers in the network must be upgraded with the same version of ArubaOS software. For redundant (VRRP) environments, the controllers should be of the same model.

To upgrade an existing multicontroller system to this version of ArubaOS:

1. Load the software image onto all controllers (including redundant master controllers).
2. If all the controllers cannot be upgraded with the same software image and rebooted simultaneously, use the following guidelines:
   a. Upgrade the software image on all the controllers. Reboot the master controller. After the master controller completes rebooting, you can reboot the local controllers simultaneously.
   b. Verify that the master and all local controllers are upgraded properly.

Upgrading to ArubaOS 6.4.4.0

The following sections provide the procedures for upgrading the controller to ArubaOS 6.4.4.0 by using the WebUI or CLI.

Install Using the WebUI

CAUTION

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 42.

NOTE

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

Upgrading From an Older Version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your controller. If you are running one of the following versions of ArubaOS, you must download and upgrade to an interim version of ArubaOS before upgrading to ArubaOS 6.4.4.0.

- For controllers running ArubaOS 3.x.versions earlier than ArubaOS 3.4.4.1, download the latest version of ArubaOS 3.4.5.x.
- For controllers running ArubaOS 3.x or those running ArubaOS 5.0.x versions earlier than ArubaOS 5.0.3.1, download and install the latest version of ArubaOS 5.0.4.x.
- For controllers running ArubaOS 6.0.0.0 or 6.0.0.1 versions, download and install the latest version of ArubaOS 6.0.1.x.

Follow step 2 to step 11 of the procedure described in Upgrading From a Recent Version of ArubaOS on page 44 to install the interim version of ArubaOS, and then repeat steps 1 through 11 of the procedure to download and install ArubaOS 6.4.4.0.

Upgrading From a Recent Version of ArubaOS

The following steps describe the procedure to upgrade from one of these recent versions of ArubaOS:

- 3.4.4.1 or later
- 5.0.3.1 or latest version of 5.0.x
- 6.0.1.0 or later 6.x

Install the ArubaOS software image from a PC or workstation using the WebUI on the controller. You can also install the software image from a TFTP or FTP server using the same WebUI page.

1. Download ArubaOS 6.4.4.0 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 on the controller at the factory. Therefore, even if you do not manually verify the SHA hash of a software image, the controller 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. Choose the nonboot partition from the **Partition to Upgrade** radio button.
8. Choose **Yes** in the **Reboot Controller After Upgrade** radio button to automatically reboot after upgrading. Choose **No**, if you do not want the controller to reboot immediately.

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

9. Choose **Yes** in the **Save Current Configuration Before Reboot** radio button.
10. Click **Upgrade**.

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

    If you chose to automatically reboot the controller 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 42 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. The RAP-5/RAP-5WN reboots to complete the provisioning image upgrade.

Install Using 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 42.

Upgrading From an Older Version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your controller. For more information, see Upgrading From an Older Version of ArubaOS on page 44.

Follow steps 2 through 7 of the procedure described in Upgrading From a Recent Version of ArubaOS on page 46 to install the interim version of ArubaOS, and then repeat steps 1 through 7 of the procedure to download and install ArubaOS 6.4.4.0.

Upgrading From a Recent Version of ArubaOS

The following steps describe the procedure to upgrade from one of these recent versions of ArubaOS:

- 3.4.4.1 or later
- 5.0.3.1 or latest version of 5.0.x
- 6.0.1.0 or later 6.x

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

1. Download ArubaOS 6.4.4.0 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.

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

   or

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

   or

   ```
   (hostname)# 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**.

   ```
   (hostname) #show image version
   ---------------------------------
   Partition               : 0:0 (/dev/ha1)
   Software Version        : ArubaOS 6.1.1.0 (Digitally Signed - Production Build)
   Build number            : 28288
   Label                   : 28288
   Built on                : Thu Apr 21 12:09:15 PDT 2012
   ---------------------------------
   Partition               : 0:1 (/dev/hda2) **Default boot**
   ```

```
Label                  : 38319
Built on               : Fri June 07 00:03:14 2013
```

5. Execute the **copy** command to load the new image onto the nonboot partition.

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

or

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

or

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

or

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

The USB option is available on the 7010, 7030, and 7200 Series controllers.

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

```
(hostname)# show image version

-----------------------------------
Partition              : 0:0 (/dev/hda1) **Default boot**
Software Version       : ArubaOS 6.4.4.0 (Digitally Signed - Production Build)
Build number           : 51745
Label                  : 51745
Built on               : Fri Sep 18 02:28:34 PDT 2015
-----------------------------------
Partition              : 0:1 (/dev/hda2)
Software Version       : ArubaOS 6.4.3.0 (Digitally Signed - Production Build)
Build number           : 49296
Label                  : 49296
Built on               : Sun Mar 15 01:15:24 PDT 2015
```

7. Reboot the controller.

```
(hostname)# reload
```

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

```
(hostname)# 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 42 for information on creating a backup.

Installing the FIPS Version of ArubaOS 6.4.4.0

Download the FIPS version of the software from https://support.arubanetworks.com.

Instructions on Installing FIPS Software

Follow the steps below to install the FIPS software that is currently running a non-FIPS version of the software:

1. Install the FIPS version of the software on the controller.
2. Execute the **write erase** command to reset the configuration to the factory default; otherwise, you cannot log in to the controller using the CLI or WebUI.
3. Reboot the controller by executing the **reload** command.

This is the only supported method of moving from non-FIPS software to FIPS software.

Downgrading

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

If you upgraded from ArubaOS 3.3.x to ArubaOS 5.0, the upgrade script encrypts the internal database. New entries created in ArubaOS 6.4.4.0 are lost after the downgrade (this warning does not apply to upgrades from ArubaOS 3.4.x to ArubaOS 6.1).

If you downgrade to a pre-6.1 configuration that was not previously saved, some parts of your deployment may not work as they previously did. For example, when downgrading from ArubaOS 6.4.4.0 to 5.0.3.2, changes made to WIPS in ArubaOS 6.x prevent the new predefined IDS profile assigned to an AP group from being recognized by the older version of ArubaOS. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error.

These new IDS profiles begin with *ids-transitional* while older IDS profiles do not include *transitional*. If you have encountered this issue, execute the **show profile-errors** and **show ap-group** commands to view the IDS profile associated with the AP group.

When reverting the controller software, whenever possible, use the previous version of software known to be used on the system. Loading a release not previously confirmed to operate in your environment could result in an improper configuration.

Before You Begin

Before you reboot the controller with the preupgrade software version, you must perform the following steps:

1. Back up your controller. For details, see Backing up Critical Data on page 42.
2. Verify that the control plane security is disabled.
3. Set the controller to boot with the previously saved pre-ArubaOS 6.4.4.0 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 6.4.4.0 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.4.4.0 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 6.4.4.0, the changes do not appear in RF Plan in the downgraded ArubaOS version.
   - If you installed any certificates while running ArubaOS 6.4.4.0, 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 preupgrade 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 preupgrade 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 preupgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the saved preupgrade 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 preupgrade 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 preupgrade 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 preupgrade 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).

   In the following example, partition 1, the backup system partition, contains the backup release ArubaOS 6.1.3.2. Partition 0, the default boot partition, contains the ArubaOS 6.4.4.0 image.

   ```
   #show image version
   ---------------------------------
   Partition               : 0:0 (/dev/hda1) **Default boot**
   Software Version        : ArubaOS 6.4.4.0 (Digitally Signed - Production Build)
   Build number            : 51745
   Label                   : 51745
   ```

```
Built on                : Fri Sep 18 02:28:34 PDT 2015
----------------------------------
Partition               : 0:1 (/dev/hda2)
Software Version        : ArubaOS 6.1.3.2 (Digitally Signed - Production Build)
Build number            : 38319
Label                   : 38319
Built on                : Fri June 07 00:03:14 2013
```

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 controller 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 controller 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 of the controller 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 logs from the controller.
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 controller) or any recent changes to your controller 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 recreate the problem.
8. Provide any wired or wireless sniffer traces taken during the time of the problem.
9. Provide the controller site access information, if possible.