ArubaOS 6.4.0.2

Release Notes

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software fro Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by an Aruba warranty. For more information, refer to the ArubaCare service and support terms and conditions.

ArubaOS 6.4.0.2 is a software patch release that introduces fixes to the issues identified in the previous releases. For more information on the features described in the following sections, see the *ArubaOS 6.4 User Guide*, *ArubaOS 6.4 CLI Reference Guide*, and *ArubaOS 6.4 MIB Reference Guide*.

NOTE

See the Upgrade Procedures on page 87 for instructions on how to upgrade your controller to this release.

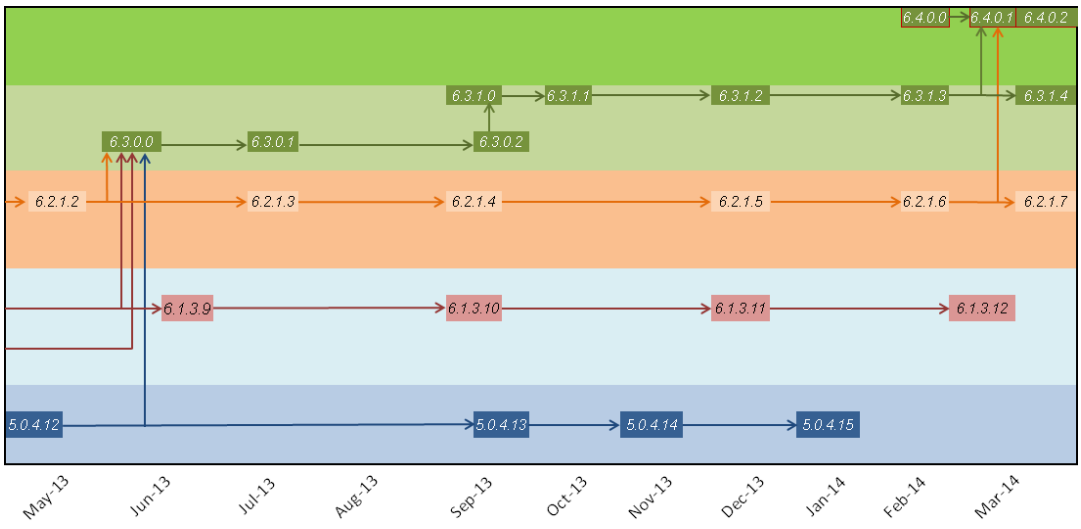
Chapter Overview

- What's New in this Release on page 13 describes the new fixes, known issues, and enhancements introduced in this release.
- Features Added in Previous Releases on page 25 describes features and enhancements added in previous ArubaOS 6.4.x release versions.
- Issues Resolved in Previous Releases on page 41 describes issues resolved in previous ArubaOS 6.4.x release versions.
- Known Issues and Limitations in Previous Releases on page 75 describes known and outstanding issues identified in previous ArubaOS 6.4.x release versions.
- Upgrade Procedures on page 87 covers the procedures for upgrading a controller to ArubaOS 6.4.0.2.

Release Mapping

The following illustration shows the patch and maintenance releases that are included in their entirety in ArubaOS 6.4.0.2:

Figure 1 *ArubaOS Releases and Code Stream Integration*



Supported Browsers

The following browsers are officially supported for use with ArubaOS 6.4.0.2 WebUI:

- Microsoft Internet Explorer 10.x, and 11 on Windows XP, Windows Vista, Windows 7, and Windows 8
- Mozilla Firefox 23 or higher on Windows XP, Windows Vista, Windows 7, and MacOS
- Apple Safari 5.1.7 or higher on MacOS

Contacting Support

Table 1: *Contact Information*

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

This chapter describes new features, regulatory changes, and bugs fixed in . In addition, it also lists the bugs that are not resolved yet, and bugs currently under investigation.

ArubaOS-AirWave Cross-Site Request Forgery Mitigation

To defend against Cross-Site Request Forgery (CSRF) attacks, an enhancement is added to use randomly generated session-ID in HTTP transactions with the ArubaOS WebUI. As a consequence, AirWave must be upgraded to AirWave 7.7.10 so that it includes the session-ID in its requests.

Upgrade Recommendations

- Upgrade to AirWave 7.7.10 to maintain full functionality.
- Upgrade controllers to ArubaOS 6.4.0.2 to mitigate CSRF. Controllers that are not upgraded would continue to work with the upgraded AirWave 7.7.10 as controllers with older ArubaOS software image ignore the session-ID in the request.

Fixed Software Versions

- ArubaOS 6.4.0.2
- AirWave 7.7.10

Frequently Asked Questions

Q. What happens if I upgrade ArubaOS but not AirWave?

A. If the controller is upgraded to ArubaOS 6.4.0.2, AirWave must also be upgraded to version 7.7.10 to maintain full functionality. If AirWave 7.7.10 patch is not applied, client monitoring, AppRF information, and push certificate will not work on the controller with ArubaOS 6.4.0.2 software image.

Q. What happens if I upgrade to AirWave 7.7.10 but not all controllers to ArubaOS 6.4.0.2?

A. If you upgrade to AirWave 7.7.10, controllers that are not upgraded to ArubaOS 6.4.0.2 will continue to work with the upgraded AirWave 7.7.10, but will ignore the session-ID in the request.

Q. Where can I find more information on CSRF?

A. http://en.wikipedia.org/wiki/Cross-site_request_forgery

EAP-MD5 Support

The controller does not support EAP-MD5 authentication for wireless clients. In ArubaOS 6.3.x and ArubaOS 6.4, EAP-MD5 authentication for wired clients failed. This issue is fixed in ArubaOS 6.4.0.2.

Regulatory Updates

The following table describes regulatory enhancements introduced in ArubaOS 6.4.0.2.

Contact your local Aruba sales representative on device availability and support for the countries listed in the following table.

Table 2: *Regulatory Domain Updates*

Regulatory Domain	Change
India	Added support for AP-175DC access point.
Senegal	Added support for AP-134 and AP-135 access points.

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 and issue the command **show ap allowed-channels country-code <country-code> ap-type <ap-model>**.

The following example shows indoor, outdoor and DFS channels supported by an AP-105 in the **United States** domain.

```
(host) #show ap allowed-channels country-code us ap-type 105
Allowed Channels for AP Type 105 Country Code "US" Country "United States"
-------------------------------------------------------------------------
PHY Type                 Allowed Channels
--------                 ----------------
802.11g (indoor)         1 2 3 4 5 6 7 8 9 10 11
802.11a (indoor)         36 40 44 48 52 56 60 64 100 104 108 112 116 132 136 140 149 153 157
161 165
802.11g (outdoor)        1 2 3 4 5 6 7 8 9 10 11
802.11a (outdoor)        52 56 60 64 100 104 108 112 116 132 136 140 149 153 157 161 165
802.11g 40MHz (indoor)   1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (indoor)   36-40 44-48 52-56 60-64 100-104 108-112 132-136 149-153 157-161
802.11g 40MHz (outdoor)  1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (outdoor)  52-56 60-64 100-104 108-112 132-136 149-153 157-161
802.11a (DFS)            52 56 60 64 100 104 108 112 116 132 136 140
```

Resolved Issues

The following issues are resolved in ArubaOS 6.4.0.2:

AirGroup

Table 3: *AirGroup Fixed Issues*

Bug ID	Description
96675	**Symptom:** Local controllers handling multicast Domain Name System (mDNS) process crashed. To resolve this issue, the cache entries and memory used for the device that sends an mDNS response packet with a time-to-live (TTL) value as zero are cleared. **Scenario:** This issue was observed when the controller received mDNS response packets, and the value of TTL was set to zero. This issue was observed in ArubaOS 6.3, but was not specific to any controller model.

Application Monitoring (AMON)

Table 4: *AMON Fixed Issues*

Bug ID	Description
94570	**Symptom:** Incorrect roles were displayed in the WebUI dashboard for the clients connected to RAPs in split-tunnel mode. This issue was resolved by resetting the flag that populates the client role value in the dashboard. **Scenario:** This issue was not limited to any specific controller model or release version.

AP-Platform

Table 5: *AP-Platform Fixed Issues*

Bug ID	Description
95893	**Symptom:** When an AP sent a DHCP request, it received an IP address 0.0.0.0 from the Preboot Execution Environment (PXE) server. Though the AP accepted this IP address, the AP could not communicate further and rebooted. The fix ensures that the PXE acknowledgment is ignored and the AP receives a valid IP address. **Scenario:** This issue was observed in deployment scenarios that have a DHCP server and multiple PXE servers. This issue was observed in APs running ArubaOS 6.3 or earlier.
96051 96754 98008	**Symptom:** AP-115 access points rebooted unexpectedly. This issue is resolved by adding a device queue status check before sending data to an ethernet driver. **Scenario:** A crash occurred when the throughput was high on ethernet connected to a 100/10M switch. This issue was observed in AP-114 and AP-115 access points running ArubaOS 6.3.x and later versions.
96239 95472	**Symptom:** When an AP was configured with a static IP address, the Link Aggregation Control Protocol (LACP) on AP-220 Series access points was not functional. This issue is resolved by initiating a LACP negotiation when an AP with a static IP is identified. **Scenario:** This issue was observed in AP-220 Series access points running ArubaOS 6.3.1.3 and 6.4.0.1 when configured with a static IP.
96913	**Symptom:** When a controller was upgraded from ArubaOS 3.4.4.3 and above, or ArubaOS 5.0.x (5.0.3.1 or later), or ArubaOS 6.0.x (6.0.1.0 or later) to ArubaOS 6.4.0.1, APs failed to upgrade to ArubaOS 6.4.0.1. A defensive check is made in affected API so that PAPI messages which are smaller than PAPI header size are handled properly in ArubaOS 6.0.x compared to ArubaOS 5.0.x. **Scenario:** This issue was observed in APs running ArubaOS 3.x, orArubaOS 5.0.x (5.0.3.1 or later) or ArubaOS 6.0.x (6.0.1.0 or later). APs running ArubaOS 6.1 and later versions are not impacted.
97544	**Symptom:**RAP-109 could not be used on un-restricted controllers that do not have Japan country code. This issue is resolved by mapping the country code in AP regulatory domain profile to the AP regulatory domain enforcement. **Scenario:** This issue was observed when the Instant AP with Japan Stock-Keeping Unit (SKU) was converted to Remote AP running ArubaOS 6.3.1.3.

AP-Regulatory

Table 6: *AP-Regulatory Fixed Issues*

Bug ID	Description
95759	**Symptom:** RADAR detection and channel change events were observed in APs on Russia country code. The issue is fixed by correcting the country domain code for Russia. **Scenario:** This issue was not limited to any specific AP model or ArubaOS release version.

AP-Wireless

Table 7: *AP-Wireless Fixed Issues*

Bug ID	Description
86184	**Symptom:** Wireless clients were unable to associate to an access point on the 5 GHz radio. This issue is resolved by making code level changes to ensure that an APs channel is changed after radar detection. **Scenario:** This issue was observed when a channel change in an access point failed after a Dynamic Frequency Selection (DFS) radar signature detection. This issue was observed in AP-125 running ArubaOS 6.1.x, 6.2.x, 6.3.x.
96751	**Symptom:** An AP continuously crashed and rebooted due to out of memory. Disabling wireless and rogue AP containment features in the **Intrusion Detection System (IDS**) profile resolved this issue. **Scenario:** This issue occurred when wireless and rogue AP containment features were enabled on the IDS profile. This issue was observed on AP-220 Series running ArubaOS 6.3.1.2 version.
97818	**Symptom:** Zebra® QL 420 Plus mobile printer did not associate with AP-220 Series access points. Improvements in the wireless driver of the AP in ArubaOS 6.4.0.2 resolved the issue. **Scenario:** This issue was observed in AP-220 Series access points running ArubaOS 6.3.1.2 or later versions.

Authentication

Table 8: *Authentication Fixed Issues*

Bug ID	Description
96285	**Symptom:** The user was not assigned with the correct role when the XML API changed the user role. This issue is resolved by sending a notification to the Campus AP (CAP) in the bridge mode during External Captive Portal (ECP) event of role change. **Scenario:** This issue was observed when the client was connected to the CAP in the bridge mode. This issue was not limited to any specific controller model and occurred on ArubaOS running 6.3.1.2.

Base OS Security

Table 9: *Base OS Security Fixed Issues*

Bug ID	Description
93537	**Symptom:** Wireless clients did not get a Dynamic Host Configuration (DHCP) IP. This issue is resolved by enabling both IP Mobility and MAC authentication, so that user gets an IP address even if the MAC authentication fails due to configuration error or connectivity issues. **Scenario**: This issue was observed when L3 mobility was configured on the controller and MAC authentication failed for the client, which caused mobile IP to drop packets from the client. This issue was not limited to any specific controller model or release version.
96458	**Symptom:** A controller rebooted with the reboot cause **Nanny rebooted machine - low on free memory**. This issue is resolved by freeing the memory that was leaking in the authentication module. **Scenario:** This issue was observed for VPN users when the **cert-cn-lookup** parameter was disabled under **aaa authentication vpn** profile. This issue was not limited to a specific controller model or release version.
96755	**Symptom:** Wired 802.1X using EAP-MD5 authentication failed. This issue is resolved by the modifying the authentication code to allow the wired-clients that perform authentication using EAP-MD5 authentication framework. **Scenario:** This Issue was observed when wired clients connected directly either to the controller or to the Ethernet port of a Campus AP or Remote AP. This issue was not limited to a specific controller model or release version.

Captive Portal

Table 10: *Captive Portal Fixed Issues*

Bug ID	Description
92927 94414 97765	**Symptom:** When Apple® iOS 7 clients tried to connect through the Captive Portal profile, the users were not redirected to the next page even after a successful authentication. A change in the redirect URL has fixed this issue. **Scenario:** This issue was observed only in clients using Apple iOS 7 devices.

Controller-Datapath

Table 11: *Controller-Datapath Fixed Issues*

Bug ID	Description
92657	**Symptom:** Although the **prohibit-arp-spoofing** parameter was disabled in firewall, clients were getting blacklisted with reason **ARP spoofing**. Controlling the action on ARP-spoofing only by the **prohibit-arp-spoof** parameter and on ip-spoofing only by the firewall **prohibit-ip-spoof** parameter fixed the issue. **Scenario:** This issue was not limited to a specific controller model or release version.
93582	**Symptom:** A 7210 controller crashed. The logs for the event listed the reason for the crash as **datapath timeout**. Ensuring that the destination UDP port of the packet is PAPI port while processing Application Level Gateway (ALG) module resolved this issue. **Scenario:** This issue was observed in 7210 controllers running ArubaOS 6.3.1.0.
95939 96156	**Symptom**: The local controller crashed as buffer allocation requests were queued to a single processor that resulted in high CPU utilization. This issue is resolved by distributing allocation requests to different CPUs to balance the load across all processors. **Scenario**: This issue was observed in 7200 Series controllers running ArubaOS 6.3.

Controller-Platform

Table 12: *Controller-Platform Fixed Issues*

Bug ID	Description
96420 88234 91172 93465 93913 94754 95664 97384 97761	**Symptom:** A local controller rebooted unexpectedly. The log files for the event listed the reason for the reboot as **Kernel Panic**. This issue is resolved by making code level changes to handle chained buffer punts to the CPU. **Scenario:** This issue was observed when the local controller received an Aggregate MAC Service Data Unit (AMSDU) packet sent by the clients as fragmented multiple packets which triggered internal conditions. This issue was observed in 3600controllers running ArubaOS 6.3.1.2.

IPSec

Table 13: *IPSec Fixed Issues*

Bug ID	Description
95634 97749	**Symptom:** Site-to-Site IPsec VPN tunnels randomly lost connectivity on a 7210 controller. This issue is resolved by making code level changes to ensure that the key length matches. **Scenario:** This issue was observed when there were 500 or more remote sites terminating IPsec VPN tunnels on a 7210 controller running ArubaOS 6.3.1.2.

Mobility

Table 14: *Mobility Fixed Issues*

Bug ID	Description
96207 96214 96222 96555	**Symptom:** The client did not receive an IP address through DHCP, and could not pass traffic when L3 mobility was enabled on the controller. This issue is resolved by clearing the state machine of the affected client. **Scenario:** This issue was observed when the client roamed from a Virtual AP (VAP) in which the **mobile-ip** parameter was enabled to a VAP in which the **mobile-ip** parameter was disabled. This issue was observed in ArubaOS 6.3 and later versions, but was not limited to a specific controller model.

RADIUS

Table 15: *RADIUS Fixed Issues*

Bug ID	Description
96038	**Symptom:** Sometimes, the user name was missing in the RADIUS accounting **STOP** messages sent from the controller. The fix ensures that a check is added for user entries with multiple IP addresses before revoking authentication. **Scenario:** This issue was observed when the controller revoked authentication for user entries with multiple IP addresses. This issue was not limited to any specific controller model or release version.

Remote AP

Table 16: *Remote AP Fixed Issues*

Bug ID	Description
97009	**Symptom:** A RAP failed to establish a PPPoE connection when the RAP's up-link port was VLAN tagged. The fix ensures that the RAP can establish a PPPoE connection with VLAN tag. **Scenario:** This issue was observed in RAPs running ArubaOS 6.3.1.3.

Station Management

Table 17: *Station Management Fixed Issues*

Bug ID	Description
86620 88646	**Symptom**: The **show ap association client-mac** command showed client MAC addresses for clients that aged out beyond the idle timeout value. This issue is resolved by making code level changes to station table in the STM module. **Scenario**: This issue was not limited to a specific controller or ArubaOS release version.

Voice

Table 18: *Voice Fixed Issues*

Bug ID	Description
94038 94600	**Symptom:** The **show voice call-cdrs** and **show voice client-status** commands displayed incorrect state transitions for consulted, transfer, and speaker announced call scenarios. The fix ensures the state transitions for New Office Environment (NOE) application layer gateway. **Scenario:** This issue was observed in an NOE deployed voice environment with controllers running ArubaOS 6.1 or later versions.

WebUI

Table 19: *WebUI Fixed Issues*

Bug ID	Description
68464 94529 94961	**Symptom:** The user was forced out of a WebUI session with the **Session is invalid** message. This issue is resolved by fixing the timing issue for the exact session ID from cookies in the https request. **Scenario:** This issue was observed when a web page of the parent domain name was accessed previously from the same browser. This issue was not limited to any specific controller model or release version.
96465	**Symptom:** Some cipher suites were not working when the operations were offloaded to hardware. This issue was resolved by disabling the cipher suites which were not working with the hardware engine. **Symptom:** This issue was observed during any crypto operation that uses DH key exchange**.**
94818	**Symptom: AP Group** name did not support special characters. With this fix, you can create an **AP Group** name with the following special characters: **" / > < : } { + _) (* & ^ % $ # @ ! [ ] ; , . /**. **Scenario:** This issue was seen when you create an **AP Group** from the **Configuration > WIRELESS > AP Configuration** page of the controller's WebUI. This issue was not limited to any specific controller or release version.

Known Issues and Limitations

The following known issues and limitations are observed in ArubaOS 6.4.0.2. Bug IDs and applicable workarounds are included.

AP-Wireless

Table 20: *AP-Wireless Known Issues*

Bug ID	Description
88940	**Symptom:** A crash is observed on APs when the status of the channel is set inappropriately by the process handling the AP management. **Scenario:** This issue is observed when a standard RAP or CAP is configured at the Dynamic Frequency Selection (DFS) channel. This issue is observed in AP-70 connected to controllers running ArubaOS 6.3.1.2. **Workaround:** Set the AP channel to No DFS before rebooting the AP.
97333	**Symptom:** All clients associated with an AP disassociates when more than 48 users start FTP downloads. **Scenario:** This issue is observed on controllers running ArubaOS 6.4.0.1. **Workaround:** None.

Base OS Security

Table 21: *Base OS Security Known Issues*

Bug ID	Description
93550	**Symptom:** Running the **aaa test-server** command for a TACACS authentication server displays **AAA server timeout** in spite of successful authentication. **Scenario:** This issue is not limited to a specific controller model or release version. **Workaround:** Issue the **aaa test-server** command twice.
95479	**Symptom:** A controller stops responding and reboots. The log files for the event listed the reason as **Nanny rebooted machine - sshd process died**. **Scenario:** This issue is observed in 7200 Series controller running ArubaOS 6.3.1.2. **Workaround:** None.

Captive Portal

Table 22: *Captive Portal Known Issues*

Bug ID	Description
95922	**Symptom:** Captive portal log out does not work. **Scenario:** This issue is observed when you configure a captive portal profile with an external log in page and custom captive portal certificate. This issue is not limited to any specific controller model or release version. **Workaround:** None.

Controller-Datapath

Table 23: *Controller-Datapath Known Issues*

Bug ID	Description
88629	**Symptom:** ACL enforcement for Microsoft® Skype doesn't work consistently. **Scenario:** This issue occurs on 7200 Series controllers running ArubaOS 6.4 when Deep Packet Inspection (DPI) is enabled on the controller. **Workaround:** None.
89722	**Symptom:** Facebook® application traffic is not getting classified correctly. **Scenario:** This issue occurs on 7200 Series controllers running ArubaOS 6.4 when DPI is enabled on the controller. **Workaround:** None.
91085	**Symptom:** Google® hangout sessions are classified as Google. **Scenario:** This issue occurs on 7200 Series controllers running ArubaOS 6.4 when AppRF is enabled on the controller. **Workaround:** None.

Table 23: *Controller-Datapath Known Issues*

Bug ID	Description
92955	**Symptom:** When sending small sized data packets at high speed data rate through IPSec tunnel, the controller crashes due to **datapath timeout**. **Scenario:** This issue is observed when the controller sends IPsec traffic at 400 Mbps with 64 bytes packet size. This causes the controller's ingress queue run out of buffer. This issue is not limited to any specific controller model or software release version. **Workaround:** None.
93327	**Symptom:** World of Warcraft® online game sessions are not getting classified correctly. **Scenario**: This issue occurs on 7200 Series controllers running ArubaOS 6.4 when AppRF is enabled on the controller. **Workaround:** None

Controller-Platform

Table 24: *Controller-Platform Known Issues*

Bug ID	Description
94615	**Symptom:** The controller may get into an **OutOfMemory** or **kernel panic** state during an ArubaOS image upgrade. **Scenario:** This issue is seen when you issue the **tar logs tech-support** command repetitively on the controller. This depletes the kernel **LowFree** memory. This issue is observed in 600 Series controller running ArubaOS 6.4 or later versions. **Workaround:** Do not issue the **tar logs tech-support** command repetitively before upgrading an ArubaOS software image.
97789 98763	**Symptom:** Controllers running ArubaOS 6.4 fail to copy an ArubaOS image using TFTP. **Scenario:** This issue is seen when you copy an ArubaOS image onto the non-boot partition of the controller using TFTP. The following error message is displayed: • In CLI: **Error determining image version** • In WebUI: **Error determining new default boot partition version** This issue is not limited to any specific controller model and observed in controllers running ArubaOS 6.4. **Workaround:** Use FTP or SCP to copy an ArubaOS image onto the non-boot partition.

LLDP

Table 25: *LLDP Known Issues*

Bug ID	Description
94302	**Symptom:** In rare cases, issuing some of the LLDP show commands display the **<ERRS> |lldp| Invalid Physical Port 0 passed at Function: li_get_handle** error message in the log. This issue does not impact any functionality. **Scenario:** This issue is not specific to any controller model and occurs on ArubaOS running 6.4. **Workaround:** None.
94647	**Symptom:** In rare cases, a **lldp GSM PORT_INFO Lookup failed at Function: sm_handle_lldp_info_events** error message appears in the log. **Scenario:** This issue occurs when the script to shut or open the interface is executed multiple times. This issue is not limited to any specific controller model and occurs on ArubaOS running 6.4. **Workaround:** None.

PhoneHome

Table 26: *PhoneHome Known Issues*

Bug ID	Description
96219	**Symptom:** Issuing the **no phonehome smtp** command removes SMTP as the transport protocol but does not rollback to the default HTTPS mode. **Scenario:** This issue is seen when you delete SMTP as the transport protocol. This issue is observed in controllers running ArubaOS 6.4 or later versions. **Workaround:** To roll back to the default HTTPS mode, issue the **phonehome https <email address>** command.

Startup Wizard

Table 27: *Startup Wizard Known Issues*

Bug ID	Description
98110	**Symptom:** Mobility Controller **Setup Wizard** page gets stuck with Java script error when you click **Next** on the **VLANs and IP Interfaces** tab of the controller's WebUI. **Scenario:** This issue is not limited to any specific controller model and is observed in ArubaOS 6.4.0.2. **Workaround:** Use Mozilla® Firefox browser to access the **VLANs and IP Interfaces** tab of the **Setup Wizard** page.
98159	**Symptom: Campus WLAN Wizard** page gets stuck in **Role Assignment** step when you click **Next** on the **Authentication Server** step of the controller's WebUI using Microsoft® Internet Explorer 10 or Internet Explorer 11. **Scenario:** This issue is not limited to any specific controller model and is observed in ArubaOS 6.4.0.2. **Workaround:** Use any browser other than Internet Explorer 10 and Internet Explorer 11 to access the **Role Assignment** tab under the **Setup Wizard** page.

Voice

Table 28: *Voice Known Issues*

Bug ID	Description
87316	**Symptom:** The Call Detailed Record (CDR) for a VoIP client goes into **ABORTED** state due to session age out. **Scenario:** This issue is observed in an L3 mobility deployment when the Real-time Transport Protocol (RTP) packets do not get tunneled to the Home Agent (HA), when a client that has roamed to the Foreign agent (FA) initiates a Lync call. This issue is observed in controllers running ArubaOS 6.3 or later versions. **Workaround:** None.

Issues Under Investigation

The following issues have been reported in ArubaOS 6.4.0.2 and are being investigated.

802.1X

Table 29: *802.1X Issues Under Investigation*

Bug ID	Description
93878	**Symptom:** Wireless clients connecting to an 802.1X based SSID observe slow network speed. However, the same set of clients when connect to an open or PSK-based SSID get good network speed. This issue is observed in 3200 controllers running ArubaOS 6.3.0.1.

Controller-Datapath

Table 30: *Controller-Datapath Issues Under Investigation*

Bug ID	Description
94143	**Symptom:** A 3200 controller running ArubaOS 6.3.1.1 stopped responding and rebooted. The log files for the event listed the reason as **datapath timeout**.
95532	**Symptom:** A 7210 controller running ArubaOS 6.3.1.1 stopped responding and rebooted. The log files for the event listed the reason as **datapath timeout**.

Controller-Platform

Table 31: *Controller-Platform Issues Under Investigation*

Bug ID	Description
95125	**Symptom:** A controller unexpectedly reboots when upgrading to ArubaOS 6.3.0.2.

Features Introduced in ArubaOS 6.4.0.1

This section describes the new features introduced in ArubaOS 6.4.0.1.

For additional information on these features, see the *ArubaOS 6.4 User Guide*.

PhoneHome Reporting Enhancements

The PhoneHome feature can be enabled by selecting the **Enable** option under **Maintenance** > **File > Aruba TAC Server** section of the WebUI. When Auto PhoneHome is enabled, the first report occurs 7 days after the feature has been enabled. The Auto PhoneHome Report is disabled by default.

The PhoneHome feature does not report any user information including client MAC address or user names.

The PhoneHome feature, allows a controller to proactively report events such as hardware failures, software malfunctions and other critical events. When PhoneHome is enabled on a controller, the customer support portal will provide a summary of deployed APs and licenses that are linked to a specific controller. To view this information, you must enter a valid email address with a domain name associated with your controller in the **Maintenance > File > Aruba TAC Server** section of the controller WebUI. Access to this information also requires an active support contract and login access to the customer portal.

Previously, PhoneHome required reports to be sent over SMTP. However, starting with ArubaOS 6.4, controllers have the option to send PhoneHome reports over HTTPS to the Aruba Activate server.

If your controller is behind the proxy server and does not have direct access to the Internet, you can configure PhoneHome to send reports using an SMTP server. PhoneHome integration with Activate offers following benefits:

- **Simpler configuration**. Phonehome only requires you to configure the email ID of the network administrator managing the device, as Activate already has information to accurately identify your controller. This email address appears in the output of the command.
- **Smaller bandwidth requirements**. When the PhoneHome feature sends the report to the Activate server, the PhoneHome report is zipped into a smaller package, then divided into smaller 1 MB pieces before being sent to the server using secure HTTPS. Only reports sent to Activate are zipped before they are sent, so reports sent to Activate use less bandwidth than a report sent to a SMTP server.
- **Enhanced error management**. If any individual portion of the report is not successfully received by the Activate server, PhoneHome makes up to three attempts to resend just that portion of the file, rather than resending the entire report. Reports sent via SMTP must be resent in their entirety if any portion is not received by the SMTP server.
- **Automatic removal of old reports**. Once the entire report has been sent to the Activate server, Activate sends an acknowledgment to the controller, prompting the controller to delete its local copy of the report
- The PhoneHome feature can be enabled or disabled using the **Maintenance** > **File > Aruba TAC Server** option in the WebUI. The same can also be done through **phonehome [enable | disable]** option in the CLI.

Features Introduced in ArubaOS 6.4

This section lists the major features introduced in ArubaOS 6.4.

AP-Platform

Support for the AP-270 Series

The Aruba AP-274 and AP-275 are environmentally hardened, outdoor rated, dual-radio IEEE 802.11ac wireless access points. These access points use MIMO (Multiple-in, Multiple-out) technology and other high-throughput mode techniques to deliver high-performance, 802.11ac 2.4 GHz and 5 GHz functionality while simultaneously supporting existing 802.11a/b/g/n wireless services.

Support for the AP-103

The Aruba AP-103 wireless access point supports the IEEE 802.11n standard for high-performance WLAN. This access point uses MIMO (Multiple-in, Multiple-out) technology and other high-throughput mode techniques to deliver high performance, 802.11n 2.4 GHz or 5 GHz functionality while simultaneously supporting existing 802.11a/b/g wireless services.

Hotspot 2.0

Hotspot 2.0 is a Wi-Fi Alliance Passpoint specification based upon the 802.11u protocol that provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users the ability to roam between partner networks without additional authentication.

ArubaOS 6.4 supports Hotspot 2.0 with enhanced network discovery and selection. Clients can receive general information about the network identity, venue and type via management frames from the Aruba AP. Clients can also query APs for information about the network's available IP address type (IPv4 or IPv6), roaming partners, and supported authentication methods, and receive that information in Information Elements from the AP.

ArubaOS 6.4 supports several ANQP and H2QP profile types for defining Hotspot data. The following table describes the profiles in the Hotspot profile set.

Table 32: *ANQP and H2QP Profiles referenced by an Advertisement Profile*

Profile	Description
Hotspot Advertisement profile	An advertisement profile defines a collection of ANQP and H2QP profiles. Each hotspot 2.0 profile is associated with one advertisement profile, which in turn references one of each type of ANQP and H2QP profile.
ANQP 3GPP Cellular Network profile	Use this profile to define priority information for a 3rd Generation Partnership Project (3GPP) Cellular Network used by hotspots that have roaming relationships with cellular operators.
ANQP Domain Name profile	Use this profile to specify the hotspot operator domain name.
ANQP IP Address Availability profile	Use this profile to specify the types of IPv4 and IPv6 IP addresses available in the hotspot network.
ANQP NAI Realm profile	An AP's NAI Realm profile identifies and describes a Network Access Identifier (NAI) realm accessible using the AP, and the method that this NAI realm uses for authentication.
ANQP Network Authentication profile	Use the ANQP Network Authentication profile to define the authentication type used by the hotspot network.

Table 32: *ANQP and H2QP Profiles referenced by an Advertisement Profile*

Profile	Description
ANQP Roaming Consortium profile	Name of the ANQP Roaming Consortium profile to be associated with this WLAN advertisement profile.
ANQP Venue Name profile	Use this profile to specify the venue group and venue type information be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.
H2QP Connection Capability profile	Use this profile to specify hotspot protocol and port capabilities.
H2QP Operating Class Indication profile	Use this profile to specify the channels on which the hotspot is capable of operating.
H2QP Operator Friendly Name profile	Use this profile to define the operator-friendly name sent by devices using this profile.
H2QP WAN Metrics profile	Use this profile to specify the WAN status and link metrics for your hotspot.

AP-220 Series Enhancements

The following enhancements have been made to the AP-220 Series access point:

- DTIM per VAP support
- CAC and TSPEC handling
- Multi-client performance tuning

AP-130 Series Functionality Improvements when Powered Over 802.3af (POE)

Starting with ArubaOS 6.4, all features and both Ethernet ports of the AP-130 Series are supported when the AP is powered by 802.3af POE.

Franklin Wireless U770 4G Modem Support

ArubaOS 6.4 introduces support of the Franklin Wireless U770 4G USB cellular modem for the Sprint LTE service on the RAP-155.

Huawei E3276 LTE Modem Support

ArubaOS 6.4 introduces support of the Huawei E3276 LTE USD cellular modem on the RAP-3WN, RAP-108, RAP-109, and RAP-155.

Authentication

Authentication Server Limits

Starting with ArubaOS 6.4, a maximum of 128 LDAP, RADIUS, and TACACS servers, each can be configured on the controller.

EAP-MD5 Support

The controller does not support EAP-MD5 authentication for wireless clients. In ArubaOS 6.3.x and ArubaOS 6.4, EAP-MD5 authentication for wired clients fail. This issue is under investigation and expected to be fixed in the upcoming ArubaOS 6.3.x and ArubaOS 6.4.x patch releases.

Controller-Platform

AirGroup

Default Behavior Changes

Starting from ArubaOS 6.4, AirGroup is disabled by default. If you upgrade from an existing non-AirGroup version to AirGroup 6.4 or perform the fresh installation of ArubaOS 6.4, the AirGroup is disabled by default. If you run an earlier version of ArubaOS with the AirGroup enabled and upgrade to ArubaOS 6.4, the AirGroup feature is enabled.

The following AirGroup features are introduced in ArubaOS 6.4:

AirGroup DLNA UPnP Support

ArubaOS 6.4 introduces the support for DLNA (Digital Living Network Alliance), a network standard that is derived from UPnP (Universal Plug and Play) in addition to the existing mDNS protocol. DLNA uses the Simple Service Discovery Protocol (SSDP) for service discovery on the network. DLNA provides the ability to share digital media between multimedia devices like Windows and Android, similar to how mDNS supports Zero Configuration Networking to Apple® devices and services.

ArubaOS 6.4 ensures that DLNA seamlessly works with the current mDNS implementation. All the features and policies that are applicable to mDNS are extended to DLNA. This ensures full interoperability between compliant devices.

AirGroup mDNS Static Records

AirGroup processes mDNS packets advertised by servers and creates the relevant cache entries. When a query comes from a user, AirGroup responds with the appropriate cache entries with the relevant policies applied. Starting from ArubaOS 6.4, AirGroup provides the ability for an administrator to add the mDNS static records to the cache.

Group Based Device Sharing

ArubaOS 6.4 AirGroup supports the sharing of AirGroup devices such as AppleTV, or Printers to a **User Group** using CPPM. This is an enhancement to features that support device sharing based upon the user's username, user-role, and location.

AirGroup-WebUI Monitoring Dashboard Enhancements

This release of ArubaOS provides the following enhancements to the AirGroup WebUI:

- **Usage** – You can view the following enhancements in the **Usage** page of the WebUI:
  - The AirGroup service names in the **AirGroup** row are now clickable. If you click a service, you are redirected to the **Dashboard** > **AirGroup** page that displays a list of AirGroup servers filtered by Service Name.
- **Clients** – You can view the following enhancements in the **Clients** page of the WebUI:
  - Under **Dashboard** > **Clients**, a new **AirGroup** column is added to display the devices that are listed as mDNS, DLNA, or both. If a device does not support both **mDNS** and **DLNA**, this field is blank.
- **AirGroup** - You can view the following enhancements in the **AirGroup** page of the WebUI:
  - A new **AirGroup type** column is added and this column specifies if the type of the AirGroup device is mDNS, DLNA or both.
  - The MAC address of each AirGroup user and server is now clickable. If you click MAC link, you are redirected to the **Dashboard** > **Clients** > **Summary page** > **AirGroup** tab. If an AirGroup user or AirGroup server is a wired trusted client, the MAC address is not clickable.

AirGroup-Limitations

The AirGroup feature has the following limitations in ArubaOS 6.4:

- AirGroup's DLNA discovery works across VLANs, however, media streaming from Windows Media Server does not work across VLANs. This limitation is a result of Digital Rights Management (DRM) support in Windows Media Server, which restricts media sharing across VLANs. Media streaming works only when both client and server are connected to the same VLAN.
- Android devices cannot discover media server while using the native music and video player applications and when they are connected across VLANs. For example, Samsung Tab 3 cannot discover the media server on Samsung Galaxy S4 while using the native music and video player applications. Android devices can discover media server when they are connected in the same VLAN. This restriction is caused by Samsung devices.
- Xbox cannot be added as an extender to the Windows clients using the Windows Media Center application with the AirGroup feature enabled. You need to disable the AirGroup feature before adding Xbox as an extender.

Passwords Secured During FTP Copy

Password are masked when using FTP to copy a file to a remote system. In previous releases, the password was entered in clear text at the end of the copy command. Starting with ArubaOS 6.4.0.0, the password is masked, and must be entered in a separate line. If you use scripts to copy files from controllers, scripts used on controllers running previous releases of ArubaOS must be modified to support the new ArubaOS 6.4 password behavior.

Old syntax:

```
(host) # copy running-config ftp: <ftphost> <user> <password> <filename>
```

New syntax:

```
(host) # copy running-config ftp:  <ftphost> <user> <filename>
Password: <ftp-password>
```

In the following example, the password is entered on the second line, and is displayed in masked text.

```
(host)  # copy running-config ftp: 192.168.1.2 adminuser runconfig
Password: ********
```

AppRF 2.0

The AppRF 2.0 feature improves application visibility and control by allowing you to configure and view access control list (ACL), bandwidth application, and application category-specific data. AppRF 2.0 supports a Deep Packet Inspection (DPI) engine for application detection for over a thousand applications. All wired and wireless traffic that traverses the controller can now be categorized and controlled by application and application category.

AppRF 2.0 provides the ability to:

- permit or deny an application or application category for a specific role. For example, you can block bandwidth monopolizing applications on a guest role within an enterprise.
- rate limit an application or application category, such as video streaming applications, for a specific role.
- mark different L2/L3 Quality of Service (QoS) for an application or application category for a user role. For example, you can mark video and voice sessions that originate from wireless users with different priorities so that traffic is prioritized accordingly in your network.

Policy Configuration

Access control lists now contain new application and application category options that let you permit or deny an application /application category on a given role.

Global Session ACL

A new session ACL has been added named "global-sacl." This session, by default, is in position one for every user role configured on the controller. The global-sacl session ACL has the following properties:

- It cannot be deleted.
- It always remains at position one in every role and its position cannot be modified.
- It contains only application rules.
- It can be modified in the WebUI and dashboard on a master controller.
- Any modifications to it results in the regeneration of ACE's of all roles.

Role Default Session ACL

You can configure role-specific application configuration using the WebUI and dashboard. For example, you can deny the facebook application on the guest role using the dashboard without having to change the firewall configuration.

A new role session ACL named apprf-"role-name"-sacl has been added. This session, by default, is in position one for every user role configured on the controller.

The string "apprf" is added to the beginning and "sacl" to the end of a role's name to form a unique name for role default session ACL. This session ACL is in position 2 of the given user role after the global session ACL and takes the next higher priority after global policy rules.

The predefined role session ACL has the following properties:

- It cannot be deleted through the WebUI or CLI. It it is only deleted automatically when the corresponding role is deleted.
- It always remains at position 2 in every role and its position cannot be modified.
- It contains only application rules.
- It can be modified using the WebUI or dashboard on a master controller, however any modification results in the regeneration of ACE's for that role.
- It cannot be applied to any other role.

Bandwidth Contract Configuration

Bandwidth contract configuration lets you configure bandwidth contracts for both the global or application-specific levels.

Global Bandwidth Contract Configuration

You can configure bandwidth contracts to limit application and application categories on an application or global level.

Role-Specific Bandwidth Contracts

Application-specific bandwidth contracts (unlike "generic" bandwidth-contracts) allow you to control or reserve rates for specific applications only on a per-role basis. An optional exclude list is provided that allows you to exclude applications or application categories on which a generic user/role bandwidth-contract is not applied. The exclude list enables you to give specific enterprise applications priority over other user traffic.

Important points regarding bandwidth contracts include:

- Application bandwidth contracts are per-role by default.
- When an application bandwidth-contract is configured for both a category and an application within the category, always apply the most specific bandwidth contract.

AppRF Dashboard Application Visibility

The AppRF Dashboard Application Visibility feature allows you to configure both application and application category policies within a given user role.

The **AppRF** page on the **Dashboard** tab displays the PEF summary of all the sessions in the controller aggregated by users, devices, destinations, applications, WLANs, and roles.The elements are now represented in box charts instead of pie charts.

Applications and Application Categories containers are only displayed on 7200 Series controllers. The remaining controller platforms will retain ArubaOS 6.3.x.x Firewall charts (i.e. without new application classification box chart).

Branch

Centralized BID Allocation

In Master-Local controller set-up, the Master controller runs the BID allocation algorithm and allocates BID to the branches terminating on it and to the Local controllers. The Master controller saves the BIDs in it's memory IAP database to avoid the collision of BID (per subnet) whereas the Local controller saves the BIDs only in it's in memory data structures. The IAP manager in Local controller forwards only the new register request (branch coming for the first time with BIDs as -1) message to the Master controller. For existing branch's register request, the Local controller tries to honor the requested BIDs first. The master and local communication is within the existing IPSec tunnel. The Master controller gets the register request and allocates BIDs using the BID allocation algorithm. Finally, the Master controller sends back the allocated BIDs to the Local controller and the Local controller updates its data structure and sends the response to the IAP.

General guidelines for upgrading from existing IAP-VPN release to ArubaOS 6.4:

1. Ensure that all the branches are upgraded to Instant 4.0.
2. Upgrade the data-center to ArubaOS 6.4.

If you have a Master-Local setup; upgrade the Master controller first and then the Local controller.

3. Ensure that always the IAP-VPN branches are configured using authorized tools like AirWave/Athena, else you must trust all branches or the required branch using the following command,

   ```
   iap trusted-branch-db allow-all
   ```

   or

   ```
   iap trusted-branch-db add mac-address<mac-address>
   ```

Instant version earlier than 4.0 also need the previous command to be executed for the controller to come up with ArubaOS 6.4.

Controller LLDP Support

ArubaOS 6.4 provides support for Link Layer Discovery Protocol (LLDP) on controllers to advertise identity information and capabilities to other nodes on the network, and store the information discovered about the neighbors.

High Availability

This section describes High Availability features added or modified in ArubaOS 6.4.

High Availability Configuration Using the WebUI

The high availability profiles introduced in ArubaOS 6.3 can now be configured using the **Configuration > Advanced Services Redundancy** window of the ArubaOS 6.4 WebUI. In previous releases, high availability

profiles were configured in the **HA** section of the **Configuration > Advanced Services > All Profile Management** window. This section of the WebUI is removed in ArubaOS 6.4.

Client State Synchronization

State synchronization improves failover performance by synchronizing client authentication state information from the active controller to the standby controller, allowing clients to authenticate on the standby controller without repeating the complete 802.1X authentication process.This feature requires you to configure the high availability group profile with a pre-shared key. The controllers use this key to establish the IPsec tunnels through which they send state synchronization information.

The state synchronization feature limits each high availability group to one IPv4 standby controller and one IPv6 standby controller, or one pair of dual-mode IPv4 and IPv6 controllers. Therefore, this feature can only be enabled in high-availability deployments that use the following topologies for each IPv4 or IPv6 controller pair.

- **Active/Active Model**: In this model, two controllers are deployed in dual mode. Controller one acts as a standby for the APs served by controller two, and vice-versa. Each controller in this deployment model supports approximately 50% of its total AP capacity, so if one controller fails, all the APs served by that controller would fail over to the other controller, thereby providing high availability redundancy to all APs in the cluster.
- **Active/Standby Model**: In this model, the active controller supports up to 100% of its rated capacity of APs, while the other controller in standby mode is idle. If the active controller fails, all APs served by the active controller would failover to the standby controller.

High Availability Inter-controller Heartbeats

The high availability inter-controller heartbeat feature allows for faster AP failover from an active controller to a standby controller, especially in situations where the active controller reboots or loses connectivity to the network.

The inter-controller heartbeat feature works independently from the AP mechanism that sends heartbeats from the AP to the controller. If enabled, the inter-controller heartbeat feature supersedes the AP's heartbeat to its controller. As a result, if a standby controller detects missed inter-controller heartbeats from the active controller, it triggers its standby APs to failover to the standby controller, even if those APs have not detected any missed heartbeats between the APs and their active controller. Use this feature with caution in deployments where the active and standby controllers are separated over high-latency WAN links.

When this feature is enabled, the standby controller starts sending regular heartbeats to an AP's active controller as soon as the AP has an UP status on the standby controller. The standby controller initially flags the active controller as *unreachable*, but changes its status to *reachable* as soon as the active controller sends a heartbeat response. If the active controller later becomes unreachable for the number of heartbeats defined by the heartbeat threshold (by default, 5 missed heartbeats), the standby controller immediately detects this error, and informs the APs using the standby controller to fail over from the active controller to the standby controller. If, however, the standby controller never receives an initial heartbeat response from the active controller, and therefore never marks the active controller as initially reachable, the standby controller will not initiate a failover.

Extended Standby Controller Capacity

The standby controller oversubscription feature allows a standby controller to support connections to standby APs beyond the controller's original rated AP capacity. This feature is an enhancement from the high availability feature introduced in ArubaOS 6.3, which requires the standby controller have a AP capacity equal to or greater than the total AP capacity of all the active controllers it supports.

Starting with ArubaOS 6.4, a 7200 Series controller acting as a standby controller can oversubscribe to standby APs by up to four times that controller's rated AP capacity, and a standby M3 controller module or

3600 controller can oversubscribe by up to two times its rated AP capacity, as long as the tunnels consuming the standby APs do not exceed the maximum tunnel capacity for that standby controller.

3200XM, 3400, and 600 Series controllers do not support this feature.

Feature Support on 600 Series Controllers

The 600 Series controller platforms do not support the following features in ArubaOS 6.4.

- AirGroup
- AppRF 1.0/Firewall Visibility
- IF-MAP
- AP Image Preload
- Centralized Image Upgrade
- IAP-VPN

Control Plane Bandwidth Contracts Values

Beginning with ArubaOS 6.4, control plane bandwidth contracts are configured in packets per second (pps) instead of bits per second (bps). This makes performance more predictable. The bandwidth contract range is now 1 to 65536 pps. Additionally, show commands related to control plane bandwidth contracts display pps. The formula used to convert bps to pps is **pps=bps/(256 x 8)**.

Automatic GRE from IAP

ArubaOS 6.4 introduces automatic GRE tunnel formation between the controller and Instant access points. Manual configuration of GRE is no longer required on the controller. This feature uses the existing IPSec connection with the controller to send control information to set up the GRE tunnel. Since the GRE control information is exchanged through a secure tunnel, security and authentication is addressed.

DHCP Lease Limit

The following table provides the maximum number of DHCP leases supported per controller platform.

Table 33: *DHCP Lease Limit*

Platform	DHCP Lease Limit
620	256
650/651	512
3200XM	512
3400	512
3600, M3	512
7210	5000
7220	10000
7240	15000

IPv6

This section describes IPv6 features added or modified in ArubaOS 6.4.

Multicast Listener Discovery (MLDv2) Snooping

This release of ArubaOS supports Source Specific Multicast (SSM) and Dynamic Multicast Optimization (DMO) as part of the IPv6 MLDv2 feature.

Source Specific Multicast

The Source Specific Multicast (SSM) supports delivery of multicast packets that originate only from a specific source address requested by the receiver. You can forward multicast streams to the clients if the source and group match the client subscribed source group pairs (S,G).

The controller supports the following IPv6 multicast source filtering modes:

- Include - In Include mode, the reception of packets sent to a specified multicast address is enabled only from the source addresses listed in the source list. The default IPv6 SSM address range is FF3X::4000:1 – FF3X::FFFF:FFFF, and the hosts subscribing to SSM groups can only be in the Include mode.
- Exclude - In Exclude mode, the reception of packets sent to a specific multicast address is enabled from all source addresses. If there is a client in the Exclude mode, the subscription is treated as an MLDv1 join.

Dynamic Multicast Optimization

When multiple clients are associated to an AP, and when one client is subscribed for a multicast stream, all the clients associated to the AP receive the stream, as the packets are directed to the multicast MAC address. To restrict the multicast stream to only the subscribed clients, DMO sends the stream to the unicast MAC address of the subscribed clients. DMO is currently supported for both IPv4 and IPv6.

Understanding MLDv2 Limitations

The following are the MLDv2 limitations:

- Controller cannot route multicast packets.
- For mobility clients mld proxy should be used.
- VLAN pool scenario stream is forwarded to clients in both the VLANs even if the client from one of the VLANs is subscribed.
- Dynamic Multicast Optimization is not applicable for wired clients in controllers.

Static IPv6 GRE Tunnel Support

Static IPv6 L2/L3 GRE tunnels can be established between Aruba devices and other devices that support IPv6 GRE tunnel. IPv4 and IPv6 L2 GRE tunnels carry both IPv6 and IPv4 traffic. The IPv6 traffic can also be redirected over the IPv4 L3 GRE tunnel.

The following options for directing traffic into the tunnel are introduced for IPv6:

- Static route, redirects traffic to the IP address of the tunnel.
- Firewall policy (session-based ACL), redirects traffic to the specified tunnel ID.

If a VLAN interface has multiple IPv6 addresses configured, one of them is used as the tunnel source IPv6 address. If the selected IPv6 address is deleted from the VLAN interface, then the tunnel source IP is re-configured with the next available IPv6 address.

Important Points to Remember

- By default a GRE Tunnel Interface is in IPv4 L3 mode.
- IPv6 configurations are allowed on an IPv4 Tunnel only if the tunnel mode is set to IPv6. Similarly, IPv4 configurations are allowed on an IPv6 Tunnel only if the tunnel mode is set to IP.

Understanding Static IPv6 GRE Tunnel Limitations

ArubaOS does not support the following functions for Static IPv6 GRE Tunnels:

- IPv6 Auto configuration and IPv6 Neighbor Discovery mechanisms do not apply to IPv6 tunnels.
- No support for Tunnel encapsulation limit and MTU discovery options on the IPv6 tunnels.
- You cannot use IPv6 GRE for a master-local setup as IPSec is not supported in this release..

IGMPv3 Support

ArubaOS 6.4 supports IGMPv3 functionality that makes Arubacontrollers aware of the Source Specific Multicast (SSM) and optimizes network bandwidth. The SSM functionality is an extension of IP multicast where the datagram traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. By default, the multicast group range of 232.0.0.0 through 232.255.255.255 (232/8) is reserved for SSM by IANA (Internet Assigned Numbers Authority).

IPv6 Enhancements

This release of ArubaOS provides the following IPv6 enhancements on the AP:

- DNS based ipv6 controller discovery
- FTP support for image upgrade in an IPv6 network
- DHCPv6 client support

VRRPv3 Support on Controllers

Virtual Router Redundancy Protocol (VRRP) eliminates a single point of failure by providing an election mechanism, among the controllers, to elect a master controller. The master controller owns the configured virtual IPv6 address for the VRRP instance. When the master controller becomes unavailable, a backup controller steps in as the master and takes ownership of the virtual IPv6 address.

VRRPv2 support over IPv4 is already present on the Aruba Mobility Controllers. VRRPv3 support over IPv6 is introduced in the current version of ArubaOS.

Depending on your redundancy solution, you can configure the VRRP parameters on your master and local controllers. The following parameters are added in this release.

- IP version - Select IPv4 \ IPv6 from the drop-down list.
- IP \ IPv6 Address - Based on the selection made in the IP version field, either IP Address \ IPv6 Address is displayed. This is the virtual IP address that is owned by the elected VRRP master. Ensure that the same IP address and VRRP ID is used on each member of the redundant pair. Note: The IP address must be unique and cannot be the loopback address of the controller. Only one global IPv6 address can be configured on a VRRP instance.

Understanding VRRP Limitations

- It is not recommended to enable preemption on the master redundancy model. If preemption is disabled and if there is a failover, the new primary controller remains the primary controller even when the original master is active again. The new primary controller does not revert to it's original state unless forced by the administrator. Disabling preemption prevents the master from “flapping” between two controllers and allows the administrator to investigate the cause of the outage.
- VRRP version 2 over IPv4 supports the master-master redundancy model. However, this support is not available in VRRP version 3 over IPv6. This model will be supported once support for IPsec over IPv6 is added. Currently only master-local and local-local redundancy are supported.

Security

Palo Alto Networks Firewall Integration

User-Identification (User-ID) feature of the Palo Alto Networks (PAN) firewall allows network administrators to configure and enforce firewall policies based on user and user groups. User-ID identifies the user on the network

based on the IP address of the device which the user is logged into. Additionally, firewall policy can be applied based on the type of device the user is using to connect to the network. Since the Arubacontroller maintains the network and user information of the clients on the network, it is the best source to provide the information for the User-ID feature on the PAN firewall.

Application Single Sign-On Using L2 Network Information

This feature allows single sign-on (SSO) for different web-based applications using Layer 2 authentication information. Single sign-on for web-based application uses Security Assertion Markup Language (SAML), which happens between the web service provider and an identity provider (IDP) that the web server trusts. A request made from the client to a web server is redirected to the IDP for authentication. If the user has already been authenticated using L2 credentials, the IDP server already knows the authentication details and returns a SAML response, redirecting the client browser to the web-based application. The user enters the web-based application without needing to enter the credentials again.

Enabling application SSO using L2 network information requires configuration on the controller and on the IDP server. The Aruba ClearPass Policy Manager (CPPM) is the only IDP supported.

802.11w Support

ArubaOSsupports the IEEE 802.11w standard, also known as Management Frame Protection (MFP). MFP makes it difficult for an attacker to deny service by spoofing Deauth and Disassoc management frames.

MFP is configured on a virtual AP (VAP) as part of the **wlan ssid-profile**. There are two parameters that can be configured, **mfp-capable** and **mfp-required**. Both are disabled by default.

Ability to Disable Factory-Default IKE/IPsec Profiles

This feature enables you to delete default IKE policies and default IPsec dynamic maps. You can do this by using the **crypto isakmp policy** and **crypto dynamic-map** CLI commands. Or, use the WebUI and navigate to **Advanced Services > VPN Services > IPSEC**.

AOS/ClearPass Guest Login URL Hash

This feature enhances the security for the ClearPass Guest login URL. A new parameter called **url_hash_key** (disabled by default) has been added to the Captive Portal profile so that ClearPass can trust and ensure that the client MAC address in the redirect URL has not been tampered with by anyone.

Authentication Server Load Balancing

Load balancing of authentication servers ensures that the authentication load is split across multiple authentication servers, thus avoiding any one particular authentication server from being overloaded. Authentication Server Load Balancing functionality enables the Aruba Mobility Controller to perform load balancing of authentication requests destined to external authentication servers (Radius/LDAP etc). This prevents any one authentication server from having to handle the full load during heavy authentication periods, such as at the start of the business day.

Enhancements in the User Authentication Failure Traps

The output of the **show snmp trap-queue** command has been enhanced to support the information such as Server IP address, user MAC, AP name, authentication failure details, authentication request time out, authentication server down, and up traps messages that are sent to the host.

RADIUS Accounting on Multiple Servers

ArubaOS 6.4 provides support for the controllers to send RADIUS accounting to multiple RADIUS servers. The controller notifies all the RADIUS servers to track the status of authenticated users. Accounting messages are sent to all the servers configured in the server group in a sequential order.

RADIUS Accounting for VIA and VPN Users

RADIUS Accounting is now supported for VIA and VPN users. A knob has been added under the **AAA Authentication VIA Auth profile** and the **AAA Authentication VPN profile** to enable this feature.

Spectrum Analysis

AP Platform Support for Spectrum Analysis

Starting with ArubaOS 6.3.1.0 and ArubaOS 6.4, AP-120 Series access points do not support the spectrum analysis feature, and cannot be configured as a spectrum monitor or hybrid AP.

Voice and Video

Unified Communication and Collaboration

This section describes the Unified Communication and Collaboration (UCC) feature introduced in ArubaOS 6.4. The Unified Communications Manager (UCM) is the core solution component of this feature. UCC addresses the onslaught of mobile devices that use voice, video, and collaboration applications. This reduces the cost of voice infrastructure for communication and collaboration needs.

UCC continues to support all existing functionality provided by ArubaOS 6.3.x. Following are the new sub-features introduced in ArubaOS 6.4.

- UCC Dashboard in the WebUI
- UCC **show** commands
- UCC— AirWave Integration
- Changes to Call Admission Control
- Per User Role Lync Call Prioritization
- Dynamically Open Firewall for UCC Clients using STUN
- UCC Call Quality Metrics

AP Support

ArubaOS 6.4.x.x is will be the last release to support the AP-120 Series. ArubaOS 6.3.x.x will be the last release to support the a/b/g only APs as well as the RAP-5. ArubaOS 6.3 will be supported at least through October 31st 2018. Individual AP support dates will vary based on their end of sale date. Please see the Aruba end of support page http://www.arubanetworks.com/support-services/end-of-life-products/ for additional details.

Table 34: *AP Support*

AP Model	End of Sale Dates (Standard Variants)	Last ArubaOS Version Supported
AP-60, AP-61, AP-65, AP-65WB, AP-70 (All Variants)	31-May-2011	ArubaOS 6.3
AP-85 (All Variants)	30-Apr-2013	ArubaOS 6.3
AP-120, AP-121 (802.11a/b/g)	31-Jan-2012	ArubaOS 6.3
AP-120, AP-121 (802.11a/n or b/g/n)	31-Jan-2012	TBD

AP Model	End of Sale Dates (Standard Variants)	Last ArubaOS Version Supported
AP-124, AP-125 (802.11a/b/g)	1-Aug-2013	ArubaOS 6.3
AP-124, AP-125 (802.11a/n or b/g/n)	1-Aug-2013	TBD
RAP-2WG	31-Oct-2013	ArubaOS 6.3
RAP-5WN	31-Oct-2013	ArubaOS 6.3
RAP-5	31-Jan-2012	ArubaOS 6.3

MIB and Trap Enhancements

Modified Traps

The following traps are modified in ArubaOS 6.4:

- wlsxMgmtUserAuthenticationFailed
- wlsxNUserAuthenticationFailed
- wlsxNAuthServerReqTimeOut
- wlsxNAuthServerTimeOut
- wlsNAuthServerIsDown
- wlsNAuthServerUp

Regulatory Updates

The following table describes regulatory enhancements introduced in ArubaOS 6.4.

Table 35: *Regulatory Domain Updates*

Regulatory Domain	Change
Argentina, Uruguay, and Vietnam	Support for AP-92 and AP-93 access points.
Uruguay	Support for AP-104 and AP-105 access points.
Argentina, Chile, Israel, and Taiwan	Support for RAP-108 and RAP-109 access points.
Thailand, Indonesia	Support for the RAP-109 remote access point.
Australia, Argentina, Brazil, Chile, China, Colombia, Egypt, Hong Kong, India, Indonesia, Israel, Malaysia, Mexico, New Zealand, Qatar, Russia, Saudi Arabia, Singapore, South Korea, South Africa, Taiwan, Thailand, Trinidad and Tobago, UAE, and Ukraine	Support for AP-110 Series access points.

Regulatory Domain	Change
Australia, Chile, China, Egypt, Hong Kong, India, Indonesia, Israel, Japan, Malaysia, Mexico, New Zealand, Qatar, Russia, Saudi Arabia, Singapore, South Africa, Taiwan, Thailand, and Ukraine	Support for RAP-155 and RAP-155P access points
Costa Rica	Support for AP-130 Series access points.
Indonesia	Support for AP-175 access points
Nigeria	Support for AP-105 access points
Argentina, Brazil, Chile, India, Indonesia, Israel, Mexico, Phillipines, Russia, Taiwan, Trinidad and Tobago, and Ukraine	Support for AP-220 Series access points.
China	Support for the AP-224 access point.
Argentina, Chile, and Israel	Support for the RAP-3WN and RAP-3WNP access points.
Serbia and Montenegro	In addition to the **CS** country code used for both Serbia and Montenegro combined, ArubaOS now supports the **RS** country code for Serbia and the **ME** country code for Montenegro.

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 and issue the command **show ap allowed-channels country-code <country-code> ap-type <ap-model>**.

The following example shows indoor, outdoor and DFS channels supported by an AP-105 in the **United States** domain.

```
(host) #show ap allowed-channels country-code us ap-type 105
Allowed Channels for AP Type 105 Country Code "US" Country "United States"
-------------------------------------------------------------------------
PHY Type                 Allowed Channels
--------                 ----------------
802.11g (indoor)         1 2 3 4 5 6 7 8 9 10 11
802.11a (indoor)         36 40 44 48 52 56 60 64 100 104 108 112 116 132 136 140 149 153 157
161 165
802.11g (outdoor)        1 2 3 4 5 6 7 8 9 10 11
802.11a (outdoor)        52 56 60 64 100 104 108 112 116 132 136 140 149 153 157 161 165
802.11g 40MHz (indoor)   1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (indoor)   36-40 44-48 52-56 60-64 100-104 108-112 132-136 149-153 157-161
802.11g 40MHz (outdoor)  1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (outdoor)  52-56 60-64 100-104 108-112 132-136 149-153 157-161
802.11a (DFS)            52 56 60 64 100 104 108 112 116 132 136 140
```

This chapter describes issues resolved in previous ArubaOS 6.4.x release version.

Resolved Issues in ArubaOS 6.4.0.1

The following issues are resolved in ArubaOS 6.4.0.1:

PhoneHome

Table 36: *PhoneHome Fixed Issues*

Bug ID	Description
96789	**Symptom**: Starting with ArubaOS 6.4.0.1, PhoneHome automatic reporting is disabled by default. This is a change in behavior from ArubaOS 6.4.0.0, as this feature was automatically enabled when the controller upgraded to ArubaOS 6.4.0.0. **Scenario**: This change in behavior impacts controllers upgrading to ArubaOS 6.4.0.1.

Resolved Issues in ArubaOS 6.4

The following issues were resolved in ArubaOS 6.4 release.

802.1X

Table 37: *802.1X Fixed Issues*

Bug ID	Description
89106	**Symptom**: A configured CLASS attribute was missing from the accounting messages sent from the RADIUS server to clients when previously idle clients reconnected to the network. **Scenario**: This issue occurred in a deployment using RADIUS accounting, where the RADIUS server pushed CLASS attributes in the access-accept messages for 802.1X authentication. When an idle user timed out from the network, ArubaOS deleted the CLASS attribute for the user along with rest of the user data. This issue is resolved with the introduction of the **delete-keycache** parameter in the 802.1X authentication profile, which, when enabled, deletes the user keycache when the client's user entries get deleted. This forces the client to complete a full 802.1X authentication process when the client reconnects after an idle timeout, so the CLASS attributes are again be sent by the RADIUS servers.
92564	**Symptom**: Clients experienced authentication failure when they used 802.1 x authentication. This issue is resolved by increasing the stack size. **Scenario**: The issue occurred due to stack overflow, which caused memory corruption. This issue was observed in 600 Series controllers and 3000 Series controllers running ArubaOS 6.1 and 6.2.

AirGroup

Table 38: *AirGroup Fixed Issues*

Bug ID	Description
88522 92368	**Symptom:** The multicast Domain Name System (mDNS) process of AirGroup crashed and restarted on a controller. This issue is resolved by blocking the memory leak to ensure that the controller is not crashing when the maximum number of servers and users supported on each platform is exceeded. **Scenario:** This issue was triggered when the number of AirGroup users exceeded the limit specified on a platform. This issue was observed in the controllers except 600 Series controllers running earlier versions of ArubaOS 6.4.

Air Management-IDS

Table 39: *Air Management-IDS Fixed Issues*

Bug ID	Description
84148	**Symptom:** The **show wms client** command took a long time to return output. This issue is fixed by retrieving wms client information from the in-memory data structures, instead of sending queries to the database. **Scenario:** This issue occurred when the **show wms client** command was executed. This issue was not limited to any specific controller model or release version.
90330	**Symptom:** An adhoc AP was classified as an AP to be manually contained, but it would not be contained unless the **protect from adhoc** feature was also enabled. This issue is resolved by changes that ensure an adhoc AP marked for containment is correctly contained. **Scenario:** This issue was observed in controllers running ArubaOS 6.2 or later.
92070	**Symptom:** The age field in the RTLS station report sent by an AP was sometimes reset although the station was no longer being heard by the AP. **Scenario:** This issue occured when the detecting AP can no longer hear frames from the station, but it can still hear frames sent by other APs to the station. This issue could occur on a controller running ArubaOS6.1 or later.
93912	**Symptom:** Issuing the **show wms client probe** command did not return any output and instead it displayed the **WMS module busy** message after a timeout period. Executing the command with the MAC address of the client fixed this issue. **Scenario:** This issue is observed when there was a large number of entries in the WLAN Management System (WMS) table. This issue is not limited to any specific controller model or ArubaOS version.

AP-Datapath

Table 40: *AP-Datapath Fixed Issues*

Bug ID	Description
90645	**Symptom:** The **show datapath session ap-name command** output did not display **ap-name** option. The command output is now displayed correctly even if the **ap-name** parameter is used. **Scenario:** This issue was observed in controllers running ArubaOS 6.2.1.3 and was not limited to any specific controller model.
94067	**Symptom:** The VLAN in the wired AP is different from the AP's native VLAN. **Scenario:** This issue occurred on the AP-93H device connected to controllers running any ArubaOS version. This issue occurred because the wired driver did not support the extra two bytes used by the internal switch chip.

AP-Platform

Table 41: *AP-Platform Fixed Issues*

Bug ID	Description
86096	**Symptom:** When multiple DNS servers were configured in a local RAP DHCP pool, only the first server in the DNS server list was available to the DHCP client. **Scenario**: This issue was observed in RAPs that were configured to use a local DHCP server and were running ArubaOS 6.2 or 6.3. This issue occurred due to incorrect handling of the DNS servers configured by SAPD.
86112	**Symptom**: The APs went to an inactive state. Changes in the internal code fixed this issue. **Scenario:** This issue was observed when the **named-vlan** parameter was configured in **wlan virtual-ap <name>** command and when all the VLAN IDs were greater than 4064. This issue was not limited to any specific controller model or ArubaOS version.
87775	**Symptom:** A Remote AP (RAP) crashed due to incorrect watchdog feeding. The issue is resolved by ensuring that the hardware watchdog feeding is done periodically. **Scenario:** This issue was observed in RAP-5WN and AP-120 Series access points running ArubaOS 6.3 or earlier versions when there was a high traffic flow in the network.
87857	**Symptom**: Fragmented configuration packets sent from the controller to the AP can cause the AP to come up with the “D:” (dirty) flag. Improvements to how ArubaOS handles out-of-order packets resolve this issue. **Scenario**: This issue is triggered by network congestion or breaks in the connection between the controller and AP.
88288 88568 89040 89135 89137 89252 89254 89255 90021 90028 90495 90604 91016 91392 91393 91755 92585 93336	**Symptom**: 802.11n-capable APs unexpectedly stopped responding and rebooted. Log files for the event listed the reason for the crash as **kernel panic** or **kernel page fault**. This issue was resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario**: This issue occurred on AP-125, AP-135, and AP-105 access points running ArubaOS 6.3.0.1.
88389 89882 90175 90332	**Symptom:** 802.11n-capable access points unexpectedly rebooted. The log files for the event listed the reason for the reboot as **kernel page fault**. Improvements in the wireless driver of the AP resolved this issue. **Scenario:** This issue was observed when an 802.11n-capable campus AP was in bridge forwarding mode and there was a connectivity issue between the AP and the controller. This issue was observed in 802.11n-capable access points running any version of ArubaOS.
88504 92678	**Symptom:** No output was displayed when the **show ap config ap-group <ap-group>** command was executed. Increasing the buffer size of SAPM (an AP management module in STM) resolved this issue. **Scenario:** This issue was observed on controllers running ArubaOS 6.3.x.x.
88813 89594	**Symptom:** The **show ap allowed-max-EIRP** command displayed incorrect information for AP-220 Series access points. This display issue is resolved by increasing the buffer size that stores Effective Isotropic Radiated Power (EIRP) information.

Table 41: *AP-Platform Fixed Issues*

Bug ID	Description
	Scenario: This issue was observed in 3200 Series controllers and 3400 Series controllers running ArubaOS 6.3.x.
89016	**Symptom**: The SNMP OID **wlanStaAccessPointESSID** had no value when a client roamed from a down AP to an active AP. Improvements to internal processes that manage layer-2 roaming resolve this issue. **Scenario**: This issue was observed when clients roamed between APs running ArubaOS 6.2.
89041	**Symptom:** A 802.11n-capable access point unexpectedly rebooted or failed to respond. This issue is resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario**: This issue was observed when a client disconnected from the network. The issue occurred on 802.11n access points running ArubaOS 6.3.0.1.
89042	**Symptom**: An access point crashed and rebooted frequently. The log files for the event listed the reason for the crash as **kernel panic**. This issue is resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario**: This issue was observed in 802.11n access points running ArubaOS 6.3.0.1.
89043 89054 89045	**Symptom**: 802.11n- capable access points unexpectedly rebooted or failed to respond. This issue is resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario**: This issue was observed on 802.11n-capable access points running ArubaOS 6.3.0.1.
89514 92163 93504	**Symptom:** AP-220 Series access point rebooted repeatedly when connected to a Power over Ethernet (PoE) switch without storing a reboot reason code in the flash memory of the AP. Design changes to the AP-220 Series access point code resolve the issue. **Scenario:** This issue was observed on AP-220 Series access points running ArubaOS 6.3.x or later versions.
89691 94047	**Symptom**: APs stopped responding and rebooted. The log files for the event listed the reason for the crash as **kernel page fault**. A change in the route cache has fixed this issue. **Scenario**: This issue occurred when the deletion of the route cache was interrupted. This issue was not limited to any specific controller model or release version.
90854	**Symptom:** On multiport APs (such the AP-93H), the APs bridge priority was configured as 8000 by default. This caused the AP to become a root bridge, when connected to a switch, and the AP became slow. **Scenario:** Starting in ArubaOS 6.4, the default value has been set to 61440 (0xF000), which avoids this issue.
91803	**Symptom:** An AP-120 Series controller failed unexpectedly. **Scenario:** This issue occured on an AP-120 Series controller running on ArubaOS 6.3.10. It was due to the AP's memory is low due to heavy traffic or many clients.
88793 91804 92194 92195 92700 92749 93080 93140 93695 93798 93845 93997	**Symptom:** APs stopped responding and crashed due to a higher utilization of memory caused by the client traffic. A change in the AP memory management resolved this issue. **Scenario:** This issue was observed in ArubaOS 6.2 and later versions, but was not limited to a specific controller model.

Table 41: *AP-Platform Fixed Issues*

Bug ID	Description
91820	**Symptom:** An AP crashed and rebooted frequently and the log file for the event listed the reason for the reboot as **Kernel Panic**. Updates to the wireless driver fixed this issue. **Scenario:** This issue occurred while receiving and freeing the buffer memory. This issue was observed in AP-135 access points running ArubaOS 6.3.1.0.
91937	**Symptom:** AP-92 and AP-93 access points were unable to come up with ArubaOS 6.3.x.x-FIPS. ArubaOS 6.3.x.x-FIPS now supports AP-92 and AP-93 access points. **Scenario:** When upgrading to ArubaOS 6.3.x.x.-FIPS, the image size was too big to fit into AP-92's or AP-93's 8 MB flash, and hence was rejecting these access points to come up although these access points required to be supported with 16 MB flash. **NOTE:** Due to the infrastructure limitation, to support 16 MB flash, the code block for 8 MB flash had to be removed as well. So, AP-92 and AP-93 access points with 8 MB flash will also come up with ArubaOS 6.3.x.x-FIPS but it is not supported. Only the AP-92 and AP-93 access points with 16 MB flash are supported with ArubaOS 6.3.x.x-FIPS.
91963	**Symptom:** An AP rebootstrapped with the **Wrong cookie in request** error after a failover from one controller to another. This issue is fixed by enhancements to drop the error message if an AP detected a cookie mismatch when the error message came from a different controller than current the LMS. **Scenario:** This issue occurred after a failover of an AP from one controller to another, and when the AP received the messages from old controller and incorrectly identified as a cookie mismatch. This issue was observed in controllers in a master-local topology with an LMS and a backup LMS configured.
92245	**Symptom:** An AP did not respond with "**aruba_valid_rx_sig: Freed packet on list at ath_rx_ tasklet+0x138/0x2880……**" message and needed a manual power cycle to restore the normal status. This issue is resolved by improvements to the wireless drivers in ArubaOS 6.4. **Scenario:** This issue occurred when the buffer was corrupted in wireless driver. This issue was observed in AP-125 model access points associated to controllers running ArubaOS 6.3.1.
92348	**Symptom:** Upstream traffic flow was interrupted and caused IP connectivity issues on MAC OS clients. This issue is fixed by setting the maximum number of MAC service data units (MSDUs) in one aggregate-MSDU (A-MSDU) to 2 and disabling the de-aggregation of AMSDU for tunnel mode VAP. **Scenario:** This issue occurred when the maximum number of MSDUs in one A-MSDU was set to 3, which was not supported in Broadcom driver. This issue was observed in MacBook Air clients associated with AP-225 access points running ArubaOS 6.3.1.0.
92572	**Symptom:** APs stopped responding and crashed due to a higher utilization of memory caused by the client traffic. A change in the AP memory management has resolved this issue. **Scenario:** This issue was observed in ArubaOS 6.2 and later versions, but is not specific to any controller model.
93012 95172	**Symptom:** Sometimes, a low voice call quality was observed on the clients. This issue is resolved by suspending any off-channel AP operation and ensuring that the voice calls are given higher priority. **Scenario:** This issue was observed in AP-225 connected to controllers running ArubaOS 6.3.1.0 and earlier versions.
93067	**Symptom:** The authorization for users was unexpectedly revoked and the **show ap client trail-info** CLI command displayed the reason as **Ptk Challenge Failed**. Sending the Extensible Authentication Protocol over LAN (EAPoL) packets as best effort traffic instead of voice traffic resolved this issue. **Scenario:** This issue was observed in AP-220 Series access points running ArubaOS 6.3.1.1 when the virtual AP is configured with WPA-802.1X-AES encryption.
93715 93380 93494	**Symptom:** An unexpected reboot of an AP-220 Series AP occurred due to a kernel panic. Internal software changes resolved this issue. **Scenario:** This reboot was triggered by VAP deletion and can occur upon mode change when all VAPs are deleted. The crash was caused because the PCI device is put to sleep when all the VAPs are deleted but ArubaOS accessed the PCI device before it woke up. This issue was limited to AP-220 Series APs running any version of ArubaOS.

Table 41: *AP-Platform Fixed Issues*

Bug ID	Description
93687 93744 93780 93904 94068 94102 94124 94146 94166 94192 94193 94196 94258 94371 94373 94422 94455 94540 94564 94763 94843 94864 94893 94917 94918 94927 94937 94956 94988 95010 95011 95144 95189 95259 95293 95619	
94189	**Symptom:** The enet1 interface of AP-135 did not power up when connected to a data switch. Starting with ArubaOS 6.4, the AP-130 Series supports full functionality when powered by an 802.3af Power over Ethernet (PoE) power source. **Scenario:** The issue was observed when the AP was connected to an 802.3af PoE power source. This issue was observed in AP-135 access points, but is not specific to any version of ArubaOS.
94279 94720	**Symptom:** A regulatory mismatch was observed on non-US controllers after an IAP was converted to a controller based AP. This issue is resolved by adding a new rule to verify the RW domain and accept RW APs on non-US controllers. **Scenario:** This issue was observed in IAP-224, IAP-225-RW, IAP-114, and IAP-115-RW.
94456	**Symptom:** Users observed AP reboot issues with two source mac addresses from the same port. This issue is fixed by not allowing ICMPv6 packets before Ethernet 1 is bonded even when it is UP. **Scenario:** This issue occurred when Ethernet 1 acted as uplink on an AP and the first ICMPv6 packet was sent with source MAC address of Ethernet 1. However, the successive ICMPv6 packets were sent with the source MAC of Ethernet 0 and caused AP reboot. This issue was not limited to any AP, controller models, and ArubaOS release version.

AP Regulatory

Table 42: *AP Regulatory Fixed Issues*

Bug ID	Description
86764	**Symptom:** The output of the **show ap allowed channels** command incorrectly displayed that 5 GHZ channels were supported on AP-68 and AP-68P. This issue is resolved by modifying the allowed channel list for AP-68 and AP-68P. **Scenario:** This issue was observed in AP-68 and AP-68P running ArubaOS versions 6.1.x, 6.2.x, or 6.3.
90995	**Symptom:** The Effective Isotropic Radiated Power (EIRP) was inconsistent and in some instances greater than the MaxEIRP, for HT20 and W52. This issue is resolved by updating the algorithm to consider the maximum EIRP for all modulation schemes. **Scenario:** This issue was observed in M3 controllers running ArubaOS 6.1.3.6.

AP-Wireless

Table 43: *AP-Wireless Fixed Issues*

Bug ID	Description
67847 69062 69346 71530 74352 74687 74792 75212 75792 75944 76142 76217 76715 77273 77275 78118 80735 82147 83242 83243 83244 83624 83833 84170 84339 84511 85015 85054 85086 85367 85959 88515 89136 89253 89256 89816 90603 91084 92871 92877 92878 92879 93923	**Symptom:** APs unexpectedly rebooted and the log files listed the reason for reboot as **Data BUS error**. A change in the exception handling module has fixed this issue. **Scenario:** This issue was observed in AP-120 Series and AP-68P devices connected to controllers running ArubaOS 6.3.1.2.
69424 71334 74646 75248 75874 78978 78981 79891 80054 85753 87250	**Symptom:** When upgraded to ArubaOS 6.2, AP-125 crashed and rebooted. Reallocating the ArubaOS loading address in memory fixed the issue. **Scenario:** This issue was observed when upgrading to ArubaOS 6.2 from ArubaOS 6.1.3.2 and later in any deployment with an AP-125.

Table 43: *AP-Wireless Fixed Issues*

Bug ID	Description
87360 88619 88620 88989 89537 91689 92641 92975 93079 93455 93811 91689	
86398	**Symptom**: The output of the **show ap debug system-status** command showed an unexpectedly large increase in the buffers in use for queue 8. Changes in how unfinished frames are queued prevents an error that allowed this counter to increment more than once per frame. **Scenario**: This occurred in AP-135 and AP-115 access points running ArubaOS 6.3.x.x, and managing multicast traffic without Dynamic Multicast Optimization (DMO).
86456	**Symptom**: A controller running ArubaOS 6.3 with an AP-125 running as a RAP rebooted unexpectedly. This was caused when the AP received a BC/MC auth frame and failed. **Scenario**: This issue occurred on an AP-125 access point running ArubaOS 6.3.
86584	**Symptom:** The AP-225 did not support prioritization for multicast traffic. **Scenario:** This issue was observed on theAP-220 Series running ArubaOS 6.3.x.
88282	**Symptom**: AP-220 Series access points running ArubaOS 6.3.0.1 stopped responding and rebooted. The log files for the event listed the reason for the crash as **kernel panic: Fatal exception**. ArubaOS memory improvements resolve this issue. **Scenario**: This issue occurred in a master-local 7200 Series controller topology where the AP-220 Series AP terminated on both the controllers in campus mode.
88328	**Symptom:** Wireless clients experienced packet loss when connecting to remote AP that was in bridge mode. The fix ensures that some buffer is reserved for transmitting unicast traffic. **Scenario:** This issue was observed in AP-105 running ArubaOS 6.1.3.8 when there was a huge multicast or broadcast traffic in the network.
88385 94033	**Symptom**: Bridge mode users (802.1x and PSK) are randomly unable to associate to a RAP. Adding reference count for messages between authentication and Station management processes to avoid incorrect order of messages resolved this issue. **Scenario**:This issue occurred because of the incorrect order of messages between authentication and station management processes. This issue was observed in controllers running ArubaOS 6.3.0.1 or later.
88741	**Symptom:** Throughput degradation was observed on the AP-225. **Scenario:** This issue was caused by an internal ArubaOS malfunction and was observed only in AP-225.
88771 88772 91086	**Symptom:** 802.11n capable access points stopped responding and rebooted. The log files for the event listed the reason for the crash as kernel page fault. This issue was resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario:** This issue was observed only in 802.11n capable access points running ArubaOS 6.3.0.1.
88827 93771	Symptom: An AP stopped responding and reset. Log files listed the reason for the event as **ath_bstuck_ tasklet: Radio 1 stuck beacon;resetting**. Changes in the ArubaOS 6.4 channel change and radio reset routines prevent this error.

Table 43: *AP-Wireless Fixed Issues*

Bug ID	Description
	Scenario: This issue occurred in an AP-125 running ArubaOS 6.2.1.3, and was not associated with any controller model.
89442 93804	**Symptom:** The AP-220 Series controllers crashed frequently. Log files listed the reason for the event as **Kernel Panic: Unable to handle kernel paging request**. **Scenario:** This issue occurred when the radio mode was altered between Monitor and Infrastructure. This issue was observed only in AP-220 Series controllers running ArubaOS 6.3.1.2.
88631 88044 88569 88843 89044 89046 89053 89058 89325 89326 89811 89901 90890 92076 92336 92786 93335	**Symptom:** An access point stopped responding and continuously rebooted. Improvements in the wireless driver of the AP fixed this issue. **Scenario:** This issue was observed in AP-220 Series running ArubaOS 6.3.0.1 when clients disconnected from the network.
89460	**Symptom:** When APs used adjacent DFS channels, the AP-135 falsely detected RADAR and exhausted all DFS channels. If no non-DFS were enabled, the AP stopped responding to clients. **Scenario:** This issue was observed in an AP-135 running ArubaOS 6.3.x and 6.2.x. It was caused when APs used adjacent DFS channels.
89735 89970 90572 91140 91560 91620 92017 92428 93373	**Symptom:** The Ethernet interface of an 802.11ac capable AP restarted frequently. Changes in the internal code fixed this issue. **Scenario:** This issue was observed in AP-220 Series access points running ArubaOS 6.3.1.0 and later versions.
90960	**Symptom**: Microsoft® Surface Pro and Surface RT clients were unable to acquire an IP address or correctly populate the ARP table with a MAC address when connecting to an AP using 20 MHz channels on 2.4 GHz or 5 GHz radios. This issue is resolved by channel scanning improvements to APs in 20 Mhz mode. **Scenario**: This issue was triggered when Microsoft Surface clients running Windows 8 or Windows 8.1 connected to 20 MHz APs running ArubaOS 6.1.3.8.
91192	**Symptom**: Poor performance was observed in clients connecting to an AP due to non-WiFi interference. Implementing the Cell-Size-Reduction feature in AP-220 Series along with deauthorizing clients when they are about to go out of the desired cell range resolved this issue. **Scenario**: This issue was observed in AP-220 Series connected to controllers running ArubaOS 6.3.1.1 or earlier.
91373	**Symptom:** MacBook clients were unable to pass traffic on the network. This issue was resolved by changes to ArubaOS that require APs to send data frames to all connected clients.

Table 43: *AP-Wireless Fixed Issues*

Bug ID	Description
	Scenario: This issue was observed in AP-220 Series access points that were upgraded to ArubaOS 6.3.1.0, and was triggered by virtual APs being enabled or disabled, either manually (by network administrators) or automatically, as a part of the regular AP startup process.
91374	**Symptom**: Latency issues occur when clients are connected to a single AP. **Scenario:** This issue occurred on an AP-225 access point on a controller running ArubaOS 6.3.1 and later. This occurred when clients go into PS mode.
91379 91449 91454 91480 94171 94238 94413	**Symptom:** An AP-220 Series device unexpectedly crashed. Using the correct structure to fill the information in the outgoing response frame resolved this issue. **Scenario:** The 802.11k enabled client that sent a Neighbor Report Request frame caused the AP-220 Series device to crash when the packet was freed. This issue was observed in controllers running ArubaOS 6.3.x or later.
91856	**Symptom:** Certain 802.11b clients did not communicate with 802.11n-capable access points. Improvements in the wireless driver of 802.11n-capable access points resolved this issue. **Scenario:** This issue was observed when Denso® 802.11b handy terminals communicated with 802.11n-capable access points on channel 7. This issue was not limited to a specific controller model or release version.
91770 91802 91805 91946 92052 92102 92260 92550 92552 92554 92555 92557 92559 92561 92562 92736 92788 92790 92873 92976 92977 93756 93757 93963	**Symptom:** AP-135 stopped responding and rebooted. Improvements to the wireless driver in ArubaOS 6.1.3.2 resolved the issue. **Scenario:** This issue occurred when the buffer was corrupted in the wireless driver. This issue was observed in AP-135 running ArubaOS 6.3.1.0.
92346	**Symptom**: When the 80MHz option is enabled in the RF arm-profile, HT Capabilities in beacon only show 20MHz support. **Scenario:** This issue occurred on controllers with AP-225 access points running ArubaOS6.3.1 and later.
92626	**Symptom:** An AP crashed and the log files for the event listed the reason for the crash as **kernel panic**. This issue is fixed by referencing the valid memory. **Scenario:** This issue occurred when an invalid memory was referenced. This issue occurred in AP-225 access points running ArubaOS 6.3.1.1.

Table 43: *AP-Wireless Fixed Issues*

Bug ID	Description
92775 96408	**Symptom:** Wireless clients received Automatic Private IP Address (APIPA) when associated to AP-225. Improvements in the wireless driver of the AP fixed the issue. **Scenario:** This issue was seen when wireless clients associated to encryption-enabled tunnel-mode Virtual AP (VAP) on the AP-225 and there was one or more bridge or decrypt-tunnel VAPs configured with encryption mode set to **static-wep**.
93113	**Symptom:** Windows 7 clients using Intel 4965 NIC intermittently stopped passing traffic when connected to AP-225. Changes in the internal code resolved this issue. **Scenario:** This issue occurred on AP-225 running ArubaOS 6.3.1.1.
93288	**Symptom:** Some clients with low signal strength had trouble sending packets to an AP. Implementing the Cell-Size-Reduction feature on AP-220 Series along with deauthorizing clients when they are about to go out of the desired cell range resolved this issue. **Scenario:** This issue was observed in AP-220 Series connected to controllers running ArubaOS 6.3.1.1 or earlier.
93476	**Symptom:** Sporadic input/output control errors were seen in the logs of many APs. Changes in the internal code resolved this issue. **Scenario:** This issue was observed when the authentication manager tries to set the keys for previous association, then station sends deauthentication, or the AP disconnects the station.
93710 94370	**Symptom:** Vocera clients associated to an AP were unable to communicate with the Vocera server. This issue was resolved by limiting the multicast transmission rate so that the unicast transmission is not affected. **Scenario:** This issue occurred when multicast traffic blocked hardware and software queues resulting in unicast packets being dropped. This issue is observed in AP-225 connected to controllers running ArubaOS 6.3.1.1.
93996	**Symptom:** An AP-120 Series access point rebooted unexpectedly. This issue is resolved by making changes to the internal code to avoid a potential condition that causes an infinite loop and NMI watchdog condition which causes the AP to reboot. **Scenario:** This issue occurred on AP-120 Series devices connected to controllers running ArubaOS 6.3.1.0.
94059 94520 95057 95106 95107	**Symptom:** An AP rebooted due to unhandled kernel unaligned access. **Scenario:** This issue was observed in AP-120 Series access points when the controllers were upgraded from ArubaOS 6.1.3.7 to 6.1.3.9, but is not limited to any specific controller model.
94117	**Symptom**: Clients are unable to connect to a SSID when the **Local Probe Request Threshold** setting in the SSID profile (which defines the SNR threshold below which incoming probe requests are ignored) is set to a value of 25 dB. This issue is resolved by changes that allow the AP to respond to probe requests with the same dB value as the local probe request threshold. **Scenario**: This issue was triggered in ArubaOS 6.3.1.x because when the Local Probe Request Threshold setting had a value of 25 dB in this setting, the AP did not respond to probe requests with SNR higher than 35 dB. As a result, APs did not respond to authentication requests from the clients, preventing them from associating to the AP.
94155 94249	**Symptom:** An AP-225 device rebooted unexpectedly when connected to a PoE. This issue is resolved by making code level changes in the index table. **Scenario:** This issue occurred due to the drastic peak in power when AP-225 is connected to 3af PoE (Power over Ethernet) and operates in low-power mode. This issue was observed in AP-225 connected to controllers running ArubaOS.

Table 43: *AP-Wireless Fixed Issues*

Bug ID	Description
94164 94534	**Symptom:** Wireless clients were unable to connect to an AP through the G band when the WPA2 authentication scheme was used. This issue is resolved by changing the initial value of VHT (Very High Throughput) to **0**. **Scenario:** This issue was observed in AP-225 connected to controllers running ArubaOS 6.3.1.1.
94198	**Symptom:** An AP rebooted unexpectedly with the log error message out of memory. **Scenario:** This issue occurred on the AP-120 Series running ArubaOS 6.3.1.0.
95006	**Symptom:** IOS devices faced connectivity issues after upgrading from 6.1.3.8 to 6.3.1.2.This issue is resolved by revising the received signal strength indication (RSSI) threshold value that triggers the handoff assist. **Scenario:** This issue was observed in controllers running ArubaOS 6.2 and 6.3 when the RSSI dropped below the defined threshold value.

ARM

Table 44: *ARM Fixed Issues*

Bug ID	Description
93312	**Symptom:** When location server was configured on the controller, a connected Air Monitor (AM) mode AP did not generate a probe report unless the location-feed flag was manually set through the AP console. **Scenario:** This issue occurred could occur on any model of AP operating in AM mode running ArubaOS 6.3.x.x.

Authentication

Table 45: *Authentication Fixed Issues*

Bug ID	Description
94629	**Symptom:** The clients connected to RAPs lost connectivity when the process handling the AP management and user association crashed. This fix ensures that the AP management and user association process does not crash. **Scenario:** This issue was observed in controllers running ArubaOS 6.3 and 6.4.
94964	**Symptom:** Captive Portal users were forced to re-authenticate every 5-10 minutes as users were not sending the IPv6 traffic. This issue is resolved by making code level changes in the authentication module. **Scenario:** This issue was observed when wired users connected to an AP and IPv6 was enabled on the controller. This issue was limited only to release versions that supported IPv6 features.

Base OS Security

Table 46: *Base OS Security Fixed Issues*

Bug ID	Description
86141 93351 93726	**Symptom:** Issuing the **show global-user-table list** command displayed duplicate client information. Ignoring the master controller IP query in Local Management Switch (LMS) list fixed the issue. **Scenario:** This issue was observed in a VRRP or master-local deployment where the master controller queried itself and the LMS list resulted in duplicate client information. This issue was observed in controllers running ArubaOS 6.3.X.0.
86867	**Symptom:** When a user-role and the ACL that have the same name and were configured as the ip access-group on the interface for APs/RAPs, the AP/RAP traffic was hitting the user-role ACL instead of the ip access-group ACL. **Scenario:** This issue was observed on controllers running ArubaOS 6.2.1.2.
87405	**Symptom:** Firewall policies were not enforced on certain client traffic when the clients were connected to a RAP in wired mode and configured with a static IP. This issue is resolved by ensuring that the sessions established with untrusted users are deleted and recreated to apply the firewall policies correctly. **Scenario:** This issue was observed when the traffic was initiated by a device or server connected to the controller with an idle client. This issue was not limited to any specific controller model or release version.
87742	**Symptom:** AP group information was not present in the RADIUS packet when the radio was disabled on the AP. The fix ensures that the AP group information is correctly populated in the RADIUS packet even when the radio is disabled. **Scenario:** This issue occurred when the wired clients were connected to the AP where BSSIDs were unavailable due to a disabled radio. This issue was not limited to any specific controller model or release version.
88271	**Symptom**: It was not possible to configure a **deny any any protocol** access control list (ACL) that overrode a statically configured **permit any any protocol** ACL. This issue is resolved by improvements that allow a user-defined ACL to take precedence over a static ACL entry. **Scenario**: This issue was observed on a controller running ArubaOS 6.3.0.1.
89453	**Symptom**: The **show rights** command did not display all the user roles configured in the controller. The output of this command now displays all the user roles configured in the controller. **Scenario** This issue was observed when more than 50 user roles were configured on a controller running ArubaOS 6.2.1.3.
90180	**Symptom**: Re-authentication of the management users was not triggered upon password change. The users are now getting **Password changed, please re-authenticate** message on the console, forcing the user to login again with the new password. **Scenario**: The issue was observed when users were already connected, and the password for these users was changed. The re-authentication message for these users was not shown. This issue was not limited to any specific controller model or ArubaOS version.
90209	**Symptom:** A controller rebooted unexpectedly. The log files for the event listed the reason as **datapath timeout**. **Scenario:** The timeout occurred due to a VIA client sending an SSL fallback packet, where the third SSL record encapsulating the IPSec packet had an invalid IP header. This issue was not limited to a specific controller model and was observed in ArubaOS 6.2.1.2.
90233	**Symptom:** Clients with a logon user role did not age out from the user-table after the logonlifetime AAA timer expired. Users are mpw aged out with the logon user role if the User Derivation Rule (UDR) is configured in the AAA profile. **Scenario**: This issue was observed when UDR was configured in the AAA profile with the logon defined as the default user role. This issue was observed on controllers running ArubaOS 6.2.1.x.

Table 46: *Base OS Security Fixed Issues*

Bug ID	Description
90454	**Symptom**: A remote AP unexpectedly rebooted because it failed to receive heartbeat responses from the controller. Changes to the order in which new IPsec SAs are added and older IPsec SAs are removed resolved this issue. **Scenario**: This issue occurred after a random IPsec rekey, and was triggered when the outbound IPsec SA was deleted before the inbound IPsec SA was added. This removed the route cache for the inner IP, causing the session entry to incorrectly point to the default gateway, and preventing heartbeat responses from reaching the AP.
90904 92079	**Symptom:** In the ArubaOS Dashboard, under **Clients > IP address**, the IP addresses, Role Names, and names of clients connected to a RAP in split tunnel mode were not displayed. **Scenario:** The client information was not being sent correctly to through the controller and, therefore, not being displayed in the dashboard.
91548	**Symptom**: The error message "User licensed count error" appeared in the error log. However, the system functionality was not affected. **Scenario:**This issue occurred on controllers running ArubaOS 6.2.1.3 and later. This occured when the VIA client connected to a RAP in split-tunnel or bridge-mode and the RAP was connected to the same controller from behind NAT.
92674	**Symptom:** Class attribute was missing in the Accounting STOP packet. This issue is resolved by not resetting the counters when an IPv6 user entry is deleted. **Scenario:** This issue occurred when the counters were reset during an IPv6 user entry aged out. This issue was not limited to any specific controller or ArubaOS version.
92817	**Symptom:** Wireless clients were blacklisted even when the rate of the IP Session did not exceed the threshold value set. This issue is resolved by increasing the storage of the threshold to 16 bits. **Scenario:** This issue was observed if the threshold of the IP Session rate was set to a value greater than 255. This issue was observed in controllers running ArubaOS 6.x.
93066 93868	**Symptom:** The MAPC module on the controller crashed unexpectedly. The log files for the event listed the reason for the crash as **mapc segmentation fault**. Internal code changes in the MAPC module of the controller fixed this issue. **Scenario:** This issue was observed when IF-MAP was configured on the controller to communicate with ClearPass Policy Manager (CPPM). This issue was observed on 7200 Series controllers running ArubaOS 6.3 or later versions.
93130	**Symptom:** A controller reboots unexpectedly. The log files for the event listed the reason for the reboot as **datapath exception**. This issue is resolved by adding SSL implementation to validate a packet before processing it. **Scenario**: This issue was observed when VIA was used to establish a tunnel with the controller, using SSL fallback. This issue was not limited to any specific controller model or ArubaOS version.
93237	**Symptom:** An internal module (Authentication) crashed on the controller. Ignoring the usage of the **equivalentToMe** attribute, which was not used by the master controller resolved this issue. **Scenario**: This issue was observed when the Novell Directory System (NDS) pushed the bulk of user data as the value for the attribute to the master controller. This issue was not limited to any specific controller model or ArubaOS version.
95367	**Symptom:** Issuing **show rules <role-name>** command from the command-line interface of a controller resulted in an internal module (Authentication) crash. Ensuring that Access Control Lists (ACLs) are not configured with spaces in the code resolved the issue. **Scenario:** This issue was observed when a large number of ACL was configured with spaces in their names. This was not limited to any specific controller model or ArubaOS version.

Configuration

Table 47: *Configuration Fixed Issues*

Bug ID	Description
73459 85136 86427 90081	**Symptom:** The output of the **show acl hits** CLI command and the **Firewall Hits** information on the **UI Monitoring** page of the controller WebUI showed inconsistent information.This issue is resolved by displaying consistent information. **Scenario:** This issue occurred because the formatting of the XML response from the controller to the WebUI was incorrect, when the output was beyond the specified limit. This issue was not limited to a specific controller model or release version.
88120	**Symptom**: The **Configuration > Wireless > AP Installation > AP provisioning > Status** tab of the controller WebUI and the output of the commands **show ap database long status up start 0 sort-by status sort-direction ascending** and **show ap database long status up start 0 sort-by status sort-direction descending** do not correctly sort the AP entries in ascending or descending order by up time. Improvements to how the controller sorts APs by status and up time resolve this issue. **Scenario**: This issue was identified in controllers running ArubaOS 6.2.1.2
91903 93462 93631	**Symptom:**The controller's fpcli process crashed when executing the command **show ap tech-support ap-name <ap name>** with a non-existing or incorrect AP name. Now, when this command is executed with a non-existent AP, the CLI returns AP with name "X" not found. **Scenario:** This issue was observed on an M3 controller running ArubaOS 6.1.3.10 but was not limited to a specific controller model.

Captive Portal

Table 48: *Captive Portal Fixed Issues*

Bug ID	Description
87294 87589 92575	**Symptom:** Captive Portal (CP) whitelist that was mapped to the user-role did not get synchronized with the standby controller. Checks in the CP whitelist database fixed this issue. **Scenario:** This issue was observed when a net-destination was created and added to the CP profile whitelist that mapped to the user-role in the master controller. This issue was observed in ArubaOS 6.2.1.2 and was not limited to any specific controller model.
88001	**Symptom:** The domain name whitelist could not be configured using wild card characters in the Captive Portal profile. The fix ensures that the wild card characters are supported while configuring the domain name whitelist. **Scenario:** This issue was not limited to any specific controller model or release version.
88116	**Symptom:** Captive Portal user was incorrectly redirected to the **User Authenticated** page even when the user provided a wrong username or password. The user now gets an **Invalid username or password** error message when providing wrong credentials. **Scenario:** This issue was observed if MSCHAPv2 was used for Captive Portal authentication. This issue was not limited to a specific controller model or release version.
88283	**Symptom:** The captive portal profile used https by default. For authentication, the user was redirected to the https://securelogin.example.com. But if this URL was manually changed to http://securelogin.example.com, then connection remained insecure from that point onwards. The controller now sends a redirect URL using the protocol configured on the controller. **Scenario:** This issue was observed when there was a mismatch between the protocol configured on the AAA profile and the protocol from the browser, This issue was not limited to a specific controller model or release version.
88405	**Symptom**: After successfully authenticating a client using Captive Portal, the browser did not automatically redirect the client to the original URL. **Scenario**: This issue was observed in the 7200 Series controller running ArubaOS 6.3.0.0.

Table 48: *Captive Portal Fixed Issues*

Bug ID	Description
91442	**Symptom:** In the master controller's command line interface **Login** page, the question mark symbol was neither getting pushed nor getting added to the local controller. This issue is resolved by ensuring that the master controller's command line interface accepts the question mark symbol. **Scenario:** This issue was observed while synchronizing the configuration from the master controller to the local controller.
92170	**Symptom:** In Captive Portal, a custom welcome page did not redirect to the original Web page after successful client authentication. Changes in the Captive Portal code to send "url" cookie to the Web browser fixed this issue. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.0.0 or later versions.
93674	**Symptom**: Clients were unable to access an external captive portal page after the controller reset. Changes in how ArubaOS manages captive portal authentication profiles resolved this issue. **Scenario**: This issue occurred in ArubaOS 6.1.3.x when the controller failed to use the correct ACL entry for a pre-authentication captive portal role.
94167	**Symptom:** When client traffic was moving through an L3 GRE tunnel between a switch and a controller, the controller did not provide the captive portal page to the client. **Scenario:** This issue was observed after an M3 was upgraded to ArubaOS 6.1.3.10. This issue was caused because the controller was unable to find the correct role for the client traffic and, therefore, did to provide the captive portal page.

Controller-Datapath

Table 49: *Controller-Datapath Fixed Issues*

Bug ID	Description
82770	**Symptom:** Using ADP, access points did not discover the master controller after enabling Broadcast/Multicast (BC/MC) rate optimization. With this new fix, enabling BC/MC rate optimization does not block ADP packets. **Scenario:** When BC/MC rate optimization was enabled on the VLAN, the controller dropped ADP packets from access points. This issue was not limited to a specific controller model or release version.
82824	**Symptom**: In some cases, when there was a large number of users on the network (more than 16k), and the **Enforce DHCP** parameter was enabled in the AP group's AAA profile, a user was flagged as an IP spoofed user. Changes to how ArubaOS manages route cache entries with the 'DHCP snooped' flag resolves this issue. **Scenario**: This issue was observed in controllers running ArubaOS 6.3.
83422 85600 87794 88311 88360 88505 88683 88740 88833 88985 89004 89303 89910 90450 90457	**Symptom:** A 7200 Series controller unexpectedly rebooted. The controller log files listed the reason for the event as a **datapath timeout**. Improvements in creating tunnels in the internal controller datapath resolved this issue. **Scenario:** This issue was observed in 7200 Series controllers running ArubaOS 6.2.1.x.

Table 49: *Controller-Datapath Fixed Issues*

Bug ID	Description
90482 90609 90836 91170 91363 91695 92161 92177 92811 93064 93572 93985 94025 94514	
85398 85627	**Symptom:** A controller responded to the Domain Name System (DNS) queries even when the IP domain lookup was disabled. This issue is resolved by ensuring that the DNS service is completely stopped if the IP domain lookup is disabled. **Scenario:** This issue occurred when the controller responded to DNS requests with its own IP. This issue was observed in controllers running ArubaOS 6.1.3.6.
85685 85543 87406	**Symptom:** An M3 controller running ArubaOS 6.1.3.8 stopped responding and rebooted. The log files for the event listed the reason for the crash as **fpapps: Segmentation fault**. Changes to the process that handles the VLAN interfaces fixed the issue. **Scenario:** This issue was observed when the VLAN interface on the controller constantly switched between an UP and DOWN state, resulting in VRRP status change. This issue was not limited to a specific controller model or ArubaOS release version.
85796 88233 88731 90350 91310 93153 93183	**Symptom:** A controller crash was observed due to a session table entry corruption. This issue is resolved by modifying the method by which the IGMP query is handled over a port channel. **Scenario:** This issue occurred when an IGMP query was triggered on the port channel. This issue was observed in 3000 Series controllers, 7200 Series controllers, and M3 controllers running ArubaOS 6.2.x.
85843	**Symptom**: A controller unexpectedly rebooted. Log files for the event listed the reason for the reboot as **datapath exception**. Memory improvements resolve this issue in ArubaOS 6.4. **Scenario**: This issue was observed in a 7200 Series controller running ArubaOS 6.2.1.1.
87295	**Symptom:** A crash was observed in a controller when it received certain types of DNS packets. This issue is fixed by modifying the internal code to handle the DNS packets correctly. **Scenario:** This issue was observed when the **firewall-visibility** feature was enabled on a controller running ArubaOS 6.2 or later.
88325	**Symptom**: Enabling support for jumbo frames on an uplink interface caused pings larger than 1472 bytes to fail. This issue is resolved by changes that ensure ArubaOS uses the correct default MTU size when jumbo frames are disabled globally, while still enabled on a port. **Scenario**: This issue was observed in ArubaOS 6.3.1.0, on a controller with jumbo frames disabled globally, but enabled on a port.
88469 90779	**Symptom:** A controller denied any FTP download that used Extended Passive mode over IPv4. Modifying the FTP ALG to handle Extended Passive mode correctly resolved this issue. **Scenario:** This issue was observed when an IPv4 FTP client used Extended Passive mode. In such a case, the FTP ALG on the controller detected it as a Bounce Attack and denied the session. This issue was not limited to a specific controller model or release version.

Table 49: *Controller-Datapath Fixed Issues*

Bug ID	Description
87417 87846 87949 88039 88226 88445 89433 89539 89641 90024 90458 90469 90746 90896 91853 92284 92464 92466 92827 92828 92829 92830 92832 94007 95012	**Symptom:** A master controller rebooted unexpectedly. The log files for the event listed the reason for the reboot as **datapath exception**. Enhancements to the Broadcom driver of the access point fixed this issue. **Scenario:** This issue was observed in 7240 controller running ArubaOS 6.3.1.1 in a master-local topology.
87949 88039 88226 88445 89433 89539 89641 90024 90458 90469 90746 90896 91853 92294 92464 92466 92827 92828 92829 92830 92832 92988 93555	**Symptom:** A controller stopped responding to network traffic and rebooted. The log file for the event listed the reason for the reboot as **datapath timeout**. This fix ensures that the CPU livelock does not recur. **Scenario:** This issue occurred on 7200 Series controllers running ArubaOS 6.3.0.1 and 6.2.x.x.
89906 92248 93423 94010 94682	**Symptom:** A controller unexpectedly rebooted and the log file listed the reason for the reboot as **datapath timeout**. This issue is fixed by increasing the stack memory size in the data plane. **Scenario:** This issue was observed when clients using SSL VPN connected to RAP and the controller tried to decompress these packets. This issue is not limited to any specific controller model or ArubaOS release version.

Table 49: *Controller-Datapath Fixed Issues*

Bug ID	Description
94989 95215 95958	
93874	**Symptom:** With Multiple TID Traffic to Temptrak device with AES Encryption, the device drops packets from AP. **Scenario:** This issue was observed on ArubaOS 6.3.1.1 and is specific to 7200 Series controllers. This issue occurred because the controller was using multiple replay counters, which the device did not support.
93466	**Symptom**: The 7200 Series controllers rebooted and the log files for the event displayed the reason for the reboot as **datapath timeout**. This issue is fixed by not forwarding the mirrored packets to monitor port when the monitor port status is down. **Scenario**: This issue was observed when the port monitor was enabled on the controller and then a Small Form-factor Pluggable (SFP) was plugged in the monitor port. This issue was observed in 7200 Series controllers and was not limited to a specific ArubaOS version.
95927	**Symptom:** Winphone devices were unable to pass traffic as the ARP requests from the devices were considered as ARP spoofs . This issue is resolved by using DHCP binding to verify if the IP address acquired by the device was already used by an old user in the controller and avoid incorrect determination of a valid ARP request as spoof. **Scenario:** This issue was observed when the devices acquired an IP address that was used by an old user earlier on the controller. This issue is not limited to any specific controller model or release version.
95588	**Symptom:** GRE tunnel groups sessions initiated by remote clients failed. This issue is resolved by redirecting the traffic initiated only by local clients. **Scenario:** This issue was observed when traffic from remote clients was redirected. This issue was observed in controllers running ArubaOS 6.3 or later.

Controller-Platform

Table 50: *Controller-Platform Fixed Issues*

Bug ID	Description
70068 85684 87008	**Symptom**: An internal controller module stops responding when a user attempts to add or delete a large number of VRRP instances. This issue is resolved by internal work flow enhancements that prevent this issue from occurring. **Scenario**: This error can be triggered by a VRRP state change, enabling or disabling an interface, or adding or deleting a tunnel.
82402 84212 86636 87552 89437 90466 91280 93591 94721 94727 95074 95624 95643 95644	**Symptom:** A controller unexpectedly stopped responding and rebooted. The log files for the event listed the reason for the crash as **httpd_wrap process died**. Verifying the Process Application Programming Interface (PAPI) packet before processing it resolved the issue. **Scenario:** This issue was observed when the PAPI library used by all applications did not filter the broadcast traffic correctly prior to PAPI inspection that caused the applications to crash. This issue occurred in 3400 controllers running ArubaOS 6.2.1.0.
82736 82875 83329 83762 84022 85355 85370 85628 86005 86029 86031 86572 86589 87410 87505 87587 88005 88332 88351 88434 88921 89636 89818 90909 91269 91308 91370 91517 92823 93294 93770 95946	**Symptom:** A controller rebooted unexpectedly. Changes in the watchdog implementation on the controller resolved the issue. **Scenario:** Log files for the event indicated the reasons for the reboot were **soft watchdog reset** or user pushed reset. This issue was identified in ArubaOS 6.1.x.x, and is not limited to any specific controller model.

Table 50: *Controller-Platform Fixed Issues*

Bug ID	Description
83502 83762 85355 85370 86029 86031 88005 89636 92823	**Symptom**: A controller rebooted unexpectedly. Changes in the watchdog implementation on the controller resolved the issue. **Scenario**: Log files for the event indicated the reason for the reboot as **user pushed reset** This issue was identified in ArubaOS 6.1.3.x, and is not limited to a specific controller model.
85685 92814	**Symptom:** An M3 controller stopped responding and rebooted due to an internal memory leak. Internal code changes fixed the memory leak. **Scenario:** This issue occurred after the **show running-config** or **write memory** command was executed on the controller on which the static or default routes were not configured. This issue was observed in M3 controllers running ArubaOS version 6.2.1.3 or later.
86107 93279	**Symptom**: The controller stopped processing radius packets every three hours and then resumed after one minute. This issue was resolved by setting **aaa profile <aaa-profile-name>** to **no devtype-classification** for all aaa profiles in use. Then execute the **clear aaa device-id-cache all** command. **Scenario:** An internal process took a backup of the database every three hours, and during this time authentication tried to access information from the database and waited there until backup was complete. Authentication resumed after that. This issue was observed on controllers running ArubaOS 6.2 or earlier.
86216 85566 87090 87635 88321 88387 88699 89436 89727 89839 89911 90162 90338 90481 91193 91387 91941 92139 92187 92516 92808 93630 93693 93931 94308	**Symptom:** During a kernel panic or crash, the panic dump generated by the controller was empty. New infrastructure has been added to improve the collection of crash dumps. **Scenario:** This issue impacts 3000 Series, 600 Series, and M3 controllers and was observed on ArubaOS 6.1.3.7.
86266	**Symptom**: In rare cases, issuing commands through a telnet shell caused an internal controller process to stop responding, triggering an unexpected controller reboot. This issue is resolved by changes that prevent ArubaOS from referencing null pointers within the software. **Scenario**: This issue was triggered by varying sequences of commands issued via the telnet shell, and is not specific to a controller model or release version.
87498	**Symptom**: An internal process (FPAPPS) failed unexpectedly.

Table 50: *Controller-Platform Fixed Issues*

Bug ID	Description
	Scenario: This issue occurred on a 3200 controller running ArubaOS 6.3.0.1 when the PPOE/PPP connection was established.
89155	**Symptom**: 600 Series controllers experienced high levels of CPU usage while booting, triggering the warning messages **Resource 'Controlpath CPU' has exceeded 30% threshold.** This issue is resolved by changes to internal CPU thresholds that better reflect expected CPU usage levels. **Scenario**: This issue was observed in controllers running ArubaOS 6.1.2.3.
90751 90633 90863 91154 91138 91474 91656	**Symptom:** Controllers continuously stopped responding and rebooted. Enhancements to memory allocation resolved this issue. **Scenario:** The issue occurred when an internal module (FPCLI) crashed due to memory corruption. This issue was observed in M3 controllers and is not limited to a specific ArubaOS version.
90619 92250	**Symptom:** The controller WebUI stopped responding indefinitely. The fix ensures that the AirWave query fails if there is no firewall visibility. **Scenario:** This issue occurred when AirWave queried for firewall visibility details from a controller on which the firewall visibility feature was disabled. This issue was observed in controllers running ArubaOS 6.2 or later.
91383	**Symptom:** Executing a **show** command causes the controller command-line interface to display an error: **Module Configuration Manager is busy. Please try later.** Improvements to how the controller manages HTTP session keys resolved this issue. **Scenario:** This issue occurred when issuing **show** commands from the command-line interface of a 3000 Series standby controller, and is triggered when the database synchronization process attempts to simultaneously replace and add an HTTP session key in the user database.
91778	**Symptom**: A controller unexpectedly reboots, displaying the error message **Mobility Processor update**. **Scenario**: This issue was observed in a local M3 controller module running ArubaOS 6.3.x.x in a master-local topology.
93990	**Symptom:** A few **Not Found** error messages appeared in the controller's console while performing initial configuration while booting. Modifying the make subsystem, and packaging the binary resolved this issue. **Scenario:** A certain binary was not built correctly due to changes in make or packaging script. This issue was observed in 600 Series controllers running ArubaOS 6.1.x.x or later.
91541 94013 94045 95079	**Symptom:** A controller rebooted due to low memory. Changes in the internal code of the controller software fixed this issue. **Scenario:** This issue occurred when there was continuous high traffic terminating on the control plane. This resulted in an internal component of the ArubaOS software to take up high memory. This issue was observed in 600 Series, 3000 Series, and M3 controllers running ArubaOS 6.1 or later versions.
95044	**Symptom:** All access points went down when the controller to which they were connected rebooted and an error was displayed - **Ancillary image stored on flash is not for this release**. This issue is resolved by writing the boot partition information to the secondary bank of the NVRAM. **Scenario:** This issue occurred when the controller rebooted due to a watchdog reset. This issue is observed only in 7200 Series controllers.

Control Plane Security

Table 51: *Control Plane Security Fixed Issues*

Bug ID	Description
85402	**Symptom:** When sending the RAP whitelist information to CPPM, ArubaOS did not fill the Calling-Station-Id correctly. **Scenario:** The controller returned a Calling-Station-Id value of 000000000000 instead of the actual value. This issue was caused by a malfunction in an internal controller process (auth) and was observed on a controller running ArubaOS 6.3.0.

DHCP

Table 52: *DHCP Fixed Issues*

Bug ID	Description
90611	**Symptom:** The Dynamic Host Configuration Protocol (DHCP) module crashed on a controller and users were not able to perform a new DHCP configuration. The updates to the DHCP wrapper fixed this issue in ArubaOS 6.4. **Scenario:** This issue was triggered by a race condition that caused the DHCP wrapper process to crash with continuous restarts. This issue was not limited to a specific controller model or release version.
92438	**Symptom:** Dynamic Host Configuration Protocol (DHCP) logs were displayed even when the DHCP debug logs were not configured. The fix ensures that the DHCP logs are printed only when the debug log is configured. This issue is resolved by changing the DHCP debug log configuration. **Scenario:** This issue was observed on controllers running ArubaOS 6.2 or later.

Generic Routing Encapsulation

Table 53: *Generic Routing Encapsulation Fixed Issues*

Bug ID	Description
89832	**Symptom:** Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel between L2 connected controllers dropped because of keepalive failures. This issue is fixed by bridging the packets before routing in the forwarding pipeline. **Scenario:** This issue occurred when the GRE tunnel keep alive was enabled and the **Configuration > Network > IP > IP Interface > Edit VLAN (1) > Enable Inter-VLAN Routing** option was disabled. This issue was observed in controllers running ArubaOS 6.3 configured with L2 GRE tunnel between L2 connected switches.

GSM

Table 54: *GSM Fixed Issues*

Bug ID	Description
91870	**Symptom:** The output of the **show ap database** command indicated that a RAP-5 was inactive and that the RAP-5 would not come up. This issue is resolved by increasing the allocation for AP wired ports to 16x. **Scenario:** This issue was observed with RAP-5 APs when all four wired AP ports were enabled in ArubaOS 6.3. ArubaOS 6.3 introduced GSM where space was pre-allocated for the AP wired ports based on the maximum number of APs times the maximum number of wired ports, because RAP-5 has four wired ports and the controller allowed four times the campus APs. As a result, the number of GSM slots was insufficient.

Guest Provisioning

Table 55: *Guest Provisioning Fixed Issues*

Bug ID	Description
87091	**Symptom:** The **Guest Provisioning** page of the WebUI showed incorrect alignment when it was printed from the Internet Explorer 8 or the Internet Explorer 9 Web browser. Improvements in the HTML styles resolved this issue. **Scenario:** This issue was first identified in ArubaOS 5.0.4.0. This issue was not observed when users viewed the controller WebUI using older versions of Internet Explorer (version 6 and 7).

HA-Lite

Table 56: *HA-Lite Fixed Issues*

Bug ID	Description
80206	**Symptom:** The high availability: fast failover feature introduced in ArubaOS 6.3 did not support VRRP-based LMS redundancy in a deployment with master-master redundancy. This topology is supported inArubaOS 6.4. **Scenario:** This issue occurred because the high availability: fast failover feature does not allow the APs to form standby tunnels to the standby master controller.

Hardware Management

Table 57: *Hardware Management Fixed Issues*

Bug ID	Description
87481	**Symptom:** 7200 Series controller returned an invalid value when an SNMP query was performed on the internal temperature details (OID .1.3.6.1.4.1.14823.2.2.1.2.1.10). The fix ensures that the SNMP attribute is set correctly for the temperature details. **Scenario:** This issue was limited to 7200 Series controllers running ArubaOS 6.3 or later versions.

IGMP Snooping

Table 58: *IGMP Snooping Fixed Issues*

Bug ID	Description
93737	**Symptom:** The **ERROR: IGMP configuration failed** error message was displayed when the **IGMP** proxy was configured using the WebUI. This issue is resolved by ensuring that only one of the following radio buttons - **Enable IGMP**, **Snooping**, or **Proxy** under the **Configuration** > **Network** > **IP** > **IP Interface** > **Edit VLAN** page of the WebUI is enabled. **Scenario:** This issue was not limited to any specific controller model or ArubaOS version.

IPv6

Table 59: *IPv6 Fixed Issues*

Bug ID	Description
88814	**Symptom:** When clients connected to a controller, they received IPV6 router advertisements from VLANs with which they were not associated. This issue is resolved by updating the datapath with the router advertisements conversion flag, so that datapath converts multicast router advertisements to unicast. **Scenario:** This issue was observed in IPv6 networks with derived VLANs and was not limited to a specific controller model or release version.

Licensing

Table 60: *Licensing Fixed Issues*

Bug ID	Description
87424	**Symptom:** The licenses were lost on a standby master controller due to which the configuration on the local controller was also lost. Caching the master controller's license limits on the standby controller for a maximum of 30 days resolved this issue. **Scenario:** This issue occurred when the standby comes up before the master after a reboot. This occurred in all master scenarios when running ArubaOS 6.3 or later.
89294	**Symptom:** RAPs were unable to come up on a standby controller if the AP licenses were installed only on the master controller. **Scenario:** This issue occurred when centralized licensing was enabled and all AP licenses were installed on the master controller and the RAP feature was disabled on the standby controller. This issue was observed in controllers running ArubaOS 6.3.

Local Database

Table 61: *Local Database Fixed Issues*

Bug ID	Description
88019	**Symptom:** A warning message **WARNING: This controller has RAP whitelist data stored in pre-6.3 format, which is consuming .....running the command 'local-userdb-ap del all** appeared when a user logged into the controller. This issue is fixed by deleting the warning file when all the old entries are deleted. **Scenario:** This issue occurred when a controller was upgraded from a previous version of ArubaOS to 6.3 or later version. This issue was not limited to any specific controller model or release version.

Master-Redundancy

Table 62: *Master-Redundancy Fixed Issues*

Bug ID	Description
80041 87032 87946 88067	**Symptom:** The show **database synchronize** command displayed a FAILED message and the standby controller was out of sync with the Master. Additionally, if there is a switchover at this time, the system is in an inconsistent state. This issue is resolved by ignoring any aborted database's synchronization sequence number on the master controller, so that the subsequent database synchronization can proceed without waiting for a response from the standby controller for previous aborted database synchronization. **Scenario:** This issue occurred when a controller was upgraded from a previous version of ArubaOS to 6.3 or later version. This issue was not limited to any specific controller model or release version.

Mesh

Table 63: *Mesh Fixed Issues*

Bug ID	Description
89458 91343 92614	**Symptom:** A Mesh Point rebooted frequently as it could not connect to a Mesh Portal. This issue is resolved by allowing Mesh Point to use the configured power for transmitting probe requests instead of reduced power. **Scenario:** This issue occurred when the transmission power on the Mesh Point was very low compared to the configured power. This issue was observed in AP-105 and AP-175 with controllers running ArubaOS 6.1.x and later versions.

Mobility

Table 64: *Mobility Fixed Issues*

Bug ID	Description
88281	**Symptom:** IP mobility entries were not cleared even when the client leaves the controller and user entries aged out. Additionally, the command **clear ip mobile host <mac-address>** did not clear the stale entry. **Scenario:** This issue was caused by a message loss between the controller's Mobile IP and authentication internal processes. Due to the message loss, the affected clients were blocked. This issue was observed in controllers running ArubaOS 6.3.x, 6.2.x, and 6.1.x.

PPPoE

Table 65: *PPPoE Fixed Issues*

Bug ID	Description
86681	**Symptom**: A controller was not able to connect to the Internet. This issue is fixed by modifying the way Point-to-Point Protocol over Ethernet (PPPoE) handles user name that contains special characters. **Scenario:** The PPPoE connection was not established with an internet service provider (ISP) server when a PPPoE user name contained special characters (for example: #0001@t-online.de). This issue was observed on controllers running ArubaOS 6.1.3.7 or later.
94356	**Symptom:** PPPoE connection did not work with 'ip nat inside' configuration. Changes to the logic that prevented NAT to occur in datapath fixed this issue. **Scenario:** This issue was observed on controllers with uplink as a PPPoE interface, and the client VLAN has 'ip nat inside' enabled.

Remote AP

Table 66: *Remote AP Fixed Issues*

Bug ID	Description
82015	**Symptom:** An AP associated with a controller did not age out as expected when you changed the heartbeat threshold and interval parameters. Changes in the internal code fixed this issue. **Scenario:** This issue occurred when you changed the heartbeat threshold and interval parameters in the AP's system profile while the AP's status is UP in the controller. This issue was not limited to any specific controller, AP model, or ArubaOS release version.
85249	**Symptom:** A degradation of Transmission Control Protocol (TCP) throughput by 9 to 11 Mbps was observed on a RAP. This issue is resolved by optimizing driver code. **Scenario:** This issue occurred in RAPs with any forwarding mode and not specific to any AP model.
85970	**Symptom:** RAPs were rebooting or crashing with a reboot reason as **Kernel page fault at virtual address**. This issue is resolved by adding a check while processing packets with no session entry. **Scenario:** This issue was observed when the RAPs received some packets with no session entries from the IPSec tunnel. This issue was observed only in RAPs running ArubaOS 6.2.x.
86650	**Symptom**: A controller sent continuous RADIUS requests for the clients connected behind the wired port of a remote AP (RAP). This issue is resolved by ArubaOS enhancements that prevent memory corruption. **Scenario**: This issue was observed when a RAP used a PPPoE uplink and operated as a wired AP in split-tunnel or bridge mode. This issue occurred on ArubaOS running 6.1.3.6, and was not limited to any specific controller model.
86934	**Symptom:** The AP failed during boot up when the Huawei® modem E1371 was used. Clearing an empty device descriptor of the modem fixed the issue. **Scenario:** This issue was caused by an internal code error when using this modem. This issue was observed in RAP-108 and RAP-109 running ArubaOS 6.3.
88193	**Symptom:** BOSE WiFi products were not able to acquire an IP address through the internal built-in DHCP server in a RAP-5WN. **Scenario:** This issue occurred on controllers running ArubaOS 6.1.3.9 and later. The DHCP client did not receive an DHCP offer or acknowledgment from the DHCP server.
90355	**Symptom:** AP-70 and RAP-108 access points connecting to the network using a cellular uplink were not able to achieve a 3G connection. This issue is resolved by improvements to the AP boot process, and changes that allow cellular modems to support multiple ports on the AP. **Scenario:** This issue was observed in 6.3.x.x nd 6.2.x.x, when AP-70 and RAP-108 access points connected to a Huawei® E220 Modem.
91106	**Symptom:** When a Remote Access Point (RAP) was rebooted from the controller using the **apboot** command, the system did not generate a log message. Changes to the internal code for handling log messages fix this issue. **Scenario:** This issue was observed in Remote Access Points running ArubaOS 6.1.x.x.
91292	**Symptom:** A Remote AP (RAP) failed over from backup LMS to primary and did not shutdown wired port. This issue is fixed by ensuring that the wired port is shut down initially when a failover occurs from backup LMS to primary LMS and then reconnects to primary LMS. This ensures that the wired port is enabled and the DHCP process is initiated. **Scenario:** This issue occurred when wired clients retained the old IP address retrieved from backup LMS and connected to primary LMS with LMS pre-emption enabled. This issue was observed in RAPs running ArubaOS 6.3.1.0.

Table 66: *Remote AP Fixed Issues*

Bug ID	Description
93707	**Symptom:** The RAP rebootstraps every 6 minutes if the RAP's local gateway IP is 192.168.11.1. **Scenario:** This issue occurred on controllers running ArubaOS6.2.1.4 and 6.3.1.1. It was caused by the DHCP server net assignment conflicting with the RAP's local networks.
94140	**Symptom:** IAP whitelist database on the controller did not allow multiple APs in same branch to share a common remote IP. **Scenario:** Starting with ArubaOS 6.4, this option is now supported. This issue was caused by a typecasting error that prevented smaller IP addresses from being allowed.
94703	**Symptom:** IAP-VPN connection disconnected intermittently. This issue is resolved by not allowing IAP database to store more than six subnets per branch. **Scenario:** This issue was observed when IAP database had more than six subnets-per-branch although a maximum of six subnets-per-branch is allowed. IAP-VPN branch with six subnets went down for more than idle timeout and came up with different DHCP profiles which led to more than six subnet entries for the branch in the IAP database.

Role/VLAN Derivation

Table 67: *Role/VLAN Derivation Fixed Issues*

Bug ID	Description
88508	**Symptom:** User derived roles were not considered for DHCP options. This issue is resolved by removing the ceiling limit set on the packet length. **Scenario:** This issue was observed when the DHCP packet length was greater than 1000 bytes in controllers running ArubaOS versions 6.3.x or earlier versions.

SNMP

Table 68: *SNMP Fixed Issues*

Bug ID	Description
85119	**Symptom:** The **wlsxNLowMemory** trap could not be triggered when the free memory of a controller was low. This issue is fixed by allowing a controller to send the **wlsxNLowMemory** trap, when the free memory of a controller reaches a threshold of 50 Mb. When the free memory of a controller reaches more than 50 Mb, the controller sends the **wlsxMemoryUsageOK** trap. **Scenario:** This issue occurred because the **wlsxNLowMemory** trap was not implemented. This issue was observed in controllers running ArubaOS 6.x.
83948 85146 87842	**Symptom:** The Simple Network Management Protocol (SNMP) module crashed when the management interface was deactivated while an SNMP query was running. A build option was modified to avoid generating code that may access invalid memory. **Scenario:** This issue was observed when SNMP was enabled and AirWave was used to monitor 620 and 3600 controllers running ArubaOS 6.3.0.0.
90453	**Symptom:** The **wlsxStackTopologyChangeTrap** SNMP trap was seen on AirWave from the controller AirWave doesn't support. This issues is resolved by updating to the latest ArubaOS MIBs on AirWave. **Scenario:** This issue was observed on controllers running AirWave 7.7.4 and ArubaOS 6.3.0.1.
94205	**Symptom:** The **sysExtFanSTatus** MIB could not be queried. This issue is resolved by initializing the value of the fanCount. **Scenario:** This issue was triggered when the **hwMon** process dis not return the proper value for fanStatus SNMP queries. This issue occurred in 7200 Series controllers running ArubaOS 6.3.1.1.

Station Management

Table 69: *Station Management Fixed Issues*

Bug ID	Description
85662 84880 88009 88319 89321 91963 92164 93243 93388 93389 93984	**Symptom:** The state of APs were displayed as **down** on the master controller even if these APs were connected and UP. Internal code changes resolved this issue. **Scenario**: This issue was observed when AP's system profile had a local controller as the primary Local Management Switch (Primary-LMS) and master controller was configured as a backup Local Management Switch (Backup-LMS). This issue was not limited to any specific controller model and occurred in ArubaOS running 6.3 or later.
86357	**Symptom:** Station Down messages were not logged in the syslog messages. Changes to syslog messaging resolved this issue. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.x.x.
88938 88999	**Symptom:** A controller's internal station management module stopped responding, causing the AP-125 access points associated to that controller to rebootstrap. Improvements to the process that updates internal tables for the client match feature resolve this issue. **Scenario:** This issue occurred on controllers running ArubaOS 6.3.0.1 and using the client match feature.

TACACS

Table 70: *TACACS Fixed Issues*

Bug ID	Description
89676	**Symptom:** Users were not able to authenticate against a TACACS server. **Scenario:** This issue was observed in controllers running ArubaOS 6.1.3.7 and later. This was triggered when non-blocking sockets for TCP connect() were not polled long enough (at least 2-3 seconds are required) before closing the tcp socket.

VLAN

Table 71: *VLAN Fixed Issues*

Bug ID	Description
95622	**Symptom:** The even VLAN distribution did not work correctly as the VLAN assignment number and the AP VLAN usage number did not match. The fix ensures that the VLAN assignment and AP VLAN usage numbers match. **Scenario**: This issue was observed in clients that were frequently roaming when even VLAN distribution was enabled. This issue was observed in controllers running ArubaOS 6.3.1.2.

Voice

Table 72: *Voice Fixed Issues*

Bug ID	Description
77716 88996 90000	**Symptom:** Incompatibility issues observed between a 3600 controller and a Cisco CUCM using SCCP version 20. Users were able to make and receive calls using a Cisco phone but there was no audio. This issue is resolved by changes that allow the controller to handle Open Receive Channel Acknowledge (ORCA) messages for SCCP Version 20. **Scenario:** The Cisco CUCM was compatible with the Skinny Client Control Protocol (SCCP) version 20, while the 3600 controller supported only up to version 17 of the SCCP. This incompatibility issue resulted in media traffic not passing through the 3600 controller as the controller was not able to parse the SCCP signaling packets. This issue was observed in a 3600 controller running ArubaOS 6.0 or later.
86224	**Symptom:** Calls dropped after 30 seconds when performing a blindly transferred SIP call. Ignoring the mid call re-invite message (by SIP ALG state machine) handling process resolves the issue. **Scenario:** This issue was observed on the M3 controller module running ArubaOS version 6.2.1. It occurred when Ascom phones sent a DELTS request upon receiving either an "invite" message from the SIP server or after sending a "180 Ringing" message back to the server.
86683	**Symptom:** The **show voice call-cdrs** and **show voice client-status** command outputs did not display the call details for Lync wired clients with media classification configured on session ACL. This issue is resolved by ensuring to handle the message appropriately for wired clients. **Scenario**: This issue was observed when Lync clients were identified as voice clients via media classification. This issue occurred on ArubaOS running 6.2 and 6.3 versions, and not limited to any specific controller version.
93517	**Symptom:** Access point rebooted unexpectedly resulting in wireless clients losing network connectivity. Releasing CDR events for AP statistics and AP event in the CDR buffer resolved the issue. **Scenario:** This issue was observed in a VoIP deployment when the Station Management (STM) process that handles AP management and user association crashed on the controller. This issue was observed in controllers running ArubaOS 6.1 or later versions.

WebUI

Table 73: *WebUI Fixed Issues*

Bug ID	Description
73459	**Symptom:** The output of the **show acl hits** command and the firewall hits information on the **Monitoring** page of the controller WebUI shows inconsistent information. The issue is resolved by displaying consistent information in the CLI and WebUI. **Scenario:** This issue occurred because the formatting of the XML response from the controller to the WebUI was incorrect, when the output exceeded the specified limit. This issue was not limited to a specific controller model or release version.
76439	**Symptom**: The Spectrum Analysis section of the WebUI fails to respond when a connected spectrum monitor is in a DOWN state. Changes to how ArubaOS manages popup error messages resolve this issue. **Scenario**: This issue occurred in ArubaOS 6.2.0.0, when an AP-105 access point in hybrid AP mode failed to appear as a connected spectrum monitor in the controller WebUI.
85225	**Symptom:** The following two issues were observed when adding an SNMPv3 user under the **Configuration** > **Management** > **SNMP** page of the WebUI: **1. User Name** field was not editable. **2. Privacy Protocol** value changed to null, when the **Authentication Protocol** was edited in SNMPv3 user entry. The first issue is an expected behavior for SNMPV3 users and the button caption is changed to **DONE** in the **Edit** mode. The second issue is fixed by avoiding the **Privacy Protocol** value changing to null. **Scenario:** This issue was not limited to any specific controller model or release version.

Table 73: *WebUI Fixed Issues*

Bug ID	Description
87457	**Symptom:** The **PKCS#12 Passphrase** field was incorrectly enabled while provisioning a regular remote AP in the WebUI (under the **Configuration** > **Wireless** > **AP Installation** > **Provision** page). The **PKCS#12 Passphrase** field is now enabled in the WebUI only for provisioning a certificate based remote AP. **Scenario:** This issue was not limited to a specific controller model or software version.
87078	**Symptom:** While accessing **AP Configuration** or **Authentication** options, the system displayed **show aaa authentication mgmt: data null** error. This issue is resolved by restarting an internal process in the controller. **Scenario:** This issue was observed in 3200 Series controllers running ArubaOS 6.1.3.5.
87720	**Symptom:** The **Reset** button on the **Monitoring** page was not functioning correctly. The **Reset** button now resets all Air Monitors correctly. **Scenario:** This issue was not limited to a specific controller model or release version.
88066	**Symptom:** Users were unable to generate Certificate Signing Request (CSR) with a comma in the **Organization** field in the WebUI and displayed a message **Invalid Character(s) Input for Organization**. This issue is fixed by GUI updates to allow comma in the **Organization** field. **Scenario:** This issue occurred only in the WebUI and there was no impact in the Command Line Interface (CLI). This issue was not limited to any specific controller model or release version.
88398	**Symptom:** Network administrators were unable to manually contain or reclassify a group of detected rogue APs in the **Dashboard** > **Security** page of the WebUI. This issue is fixed by adding support to select multiple rouge APs . **Scenario:** This issue occurred when multiple rogue APs were selected in the **Dashboard** > **Security** page. This issue was observed in controllers running ArubaOS 6.2.1.3.
88802 91141	**Symptom:** When the client tried to access the **Air Group** option from the WebUI, the system did not respond. To resolve this issue the **Air Group** option is now removed from the WebUI for 600 Series controllers. **Scenario:** This issue was observed only in 600 Series controllers running ArubaOS 6.3.x.
89092	**Symptom:** When an administrator added bulk VLANs under **Configuration > Network > VLAN > VLAN ID**, the controller did not add the bulk VLANs and the web page displayed a JavaScript error. Correction in the formatting of the XML response from the controller to the WebUI fixed this issue. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.
90110	**Symptom:** The ArubaOS Campus WLAN Wizard was not accessible. This issue is resolved by changing the LDAP server filter to include an ampersand (&). **Scenario:** The Campus WLAN wizard was not accessible due to the presence of an ampersand (&) in the LDAP server filter. This issue was observed in a 650 controller running ArubaOS 6.2.1.3, but could impact any controller model.
90264	**Symptom:** Layer 2 Tunneling Protocol (L2TP) pool was not displayed when the user-role was configured in the WebUI of a controller without an AP license. This issue is fixed by removing the WLAN_REMOTE_AP license validation while configuring L2TP pool. **Scenario:** This issue was triggered by Policy Enforcement Firewall (PEF) license with WLAN_REMOTE_AP validation while configuring L2TP pool on a controller. This issue was not limited to any specific controller model or release version.

Table 73: *WebUI Fixed Issues*

Bug ID	Description
92340 92649	**Symptom:** The WebUI of a controller failed to load in Internet Explorer 11 with the error message **can't create XMLHttpRequest object: Object doesn't support property or method 'creatXMLHttpRequest**. The ArubaOS WebUI is updated to be compatible with the new standards in Internet Explorer 11. **Scenario:** This issue was caused by changes in Internet Explorer 11 from Internet Explorer 10. This issue was observed in Internet Explorer 11 and not limited to any specific controller model or release version.
92620	**Symptom:** When TPM Initialization failed, the following error message was displayed: **TPM Initialization or Certificate Initialization failed. For debug information see /tmp/deviceCertLib.log**. The fix ensures that the error message points to the **show tpm errorlog** command. **Scenario:** This issue was observed when the Trusted Platform Module (TPM) Initialization or Certificate Initialization failed. This issue was not limited to a specific controller model.
93606	**Symptom:** Clients were not displayed in the **Monitoring** > **Controller** > **Clients** page of the WebUI when filtered with AP Name. This issue is fixed by changing the **show user-table location <ap-name>** command to **show user-table ap-name <ap-name>**. **Scenario:** This issue was triggered by changes to CLI commands. This issue was observed in controllers running ArubaOS 6.2 and 6.3.

WLAN Management System

Table 74: *WLAN Management System Fixed Issues*

Bug ID	Description
84146	**Symptom:** WLAN Management System (WMS) slowed down with redundant database queries in a controller. This issue is fixed by ignoring queries to the database that determine if there are more Virtual APs (VAPs) present on the probe. Now, the information on VAP presence can be retrieved from the in-memory data structures. **Scenario:** This issue occurred when many APs rebooted, WMS marked them as down. This caused the WMS to slow down by generating redundant database queries. This issue was not limited to any specific controller model or release version.

XML API

Table 75: *XML API Fixed Issues*

Bug ID	Description
84801	**Symptom:** Clients connected to the local controller were unable to access the Captive Portal (CP) page from an external server. This issue is resolved by configuring the **default-xml-api** parameter in the AAA profile. **Scenario:** This issue was observed when the **default-xml-api** was not configured. This issue was not limited to any specific controller or AP model.

This chapter describes known and outstanding issues identified in previous ArubaOS 6.4.x release versions.

Known Issues and Limitations in ArubaOS 6.4.0.1

The following are the known issues and limitations found in ArubaOS 6.4.0.1. Applicable Bug IDs and workarounds are included.

Controller-Platform

Table 76: *Controller-Platform Known Issues*

Bug ID	Description
97789 98763	**Symptom:** Controllers running ArubaOS 6.4 fail to copy a new ArubaOS image using TFTP. **Scenario:** This issue is seen when you copy a new ArubaOS image onto the non-boot partition of the controller using TFTP. The following error message is displayed: • In CLI: **Error determining image version** • In WebUI: **Error determining new default boot partition version** This issue is not limited to any specific controller model and observed in controllers running ArubaOS 6.4. **Workaround:** Use File Transfer Protocol (FTP) or Secured Copy (SCP) to copy a new ArubaOS image onto the non-boot partition.

PhoneHome

Table 77: *PhoneHome Known Issues*

Bug ID	Description
96901	**Symptom**:The auto-report of the PhoneHome statistics is displayed incorrectly in the **show phonehome stats** command output though the report is sent successfully. **Scenario**: This issue occurs when auto-report is triggered from support mode. This issue is observed in controllers running ArubaOS 6.4.0.1. **Workaround**: None.

Known Issues and Limitations in ArubaOS 6.4

The following are known issues and limitations in ArubaOS 6.4. Applicable Bug IDs and workarounds are included.

AirGroup

Table 78: *AirGroup Known Issues*

Bug ID	Description
91690	**Symptom**: Clients were unable to use AirGroup services to connect to other iChat clients. **Scenario**: This issue was observed in ArubaOS 6.3.0.1, and is triggered because AirGroup does not support unsolicited advertisements required by iChat. As a result, clients are unable to immediately discover each other when they log in to the network using Bonjour. **Workaround**: None.
94208	**Symptom:** Wireless Clients such as iPad and iPhone running the SONOS® Controller application do not discover the SONOS music system. **Scenario:** This issue is observed when AirGroup is enabled on a controller with the SONOS music system connected. **Workaround:** None.

AP-Platform

Table 79: *AP-Platform Known Issues*

Bug ID	Description
91172	**Symptom:** A controller crashes occasionally during freeing some corrupted memory packets. **Scenario:** This issue is not limited to any specific controller model or release version. **Workaround:** None.
93876	**Symptom:** Occasionally, the CPSEC CAPs unexpectedly reboot. **Scenario:** This issue occurs on all AP platforms with CPESEC and CAPs and may be caused by IKEv2 timing out. **Workaround:** None.
91805 93963	**Symptom:** An AP reboots occasionally without reboot reason or crash information. **Scenario:** This issue occurs on the AP-125 running ArubaOS 6.3.0.1. **Workaround:** None.
95056	**Symptom:** An AP-120 Series device crashes with the log message **Unhandled kernel unaligned access**. **Scenario:** This issue occurs on AP-120 Series models running ArubaOS 6.3.1.2. **Workaround:** None.
95260	**Symptom:** An AP occasionally reboots with crash information **cache_alloc_refill**. **Scenario:** This issue occurs on the AP-120 Series models running ArubaOS 6.3.1.2. **Workaround:** None.
95764	**Symptom:** An AP-125 device crashes and reboots, the log files for the event list the reason for the crash as **Kernel unaligned instruction access**. **Scenario:** This issue occurs in AP-125 access points connected to controllers running ArubaOS 6.3.1.2. **Workaround:** None.

AP-Wireless

Table 80: *AP-Wireless Known Issues*

Bug ID	Description
69424 71334 74646 75248 75874 78978 78981 79891 80054 85753 87250 87360 88619 88620 88989 89537 91689 92641 92975 93079 93455 93811 91689	**Symptom:** When upgraded to ArubaOS 6.2, AP-125 crashes and reboots. **Scenario:** This issue is observed when upgrading to ArubaOS 6.2 from ArubaOS 6.1.3.2 and later in any deployment with an AP-125.
86184	**Symptom:** Wireless clients are unable to associate to an access point on the 5GHz radio. **Scenario:** This issue is observed when a channel change in an access point fails after a Dynamic Frequency Selection (DFS) radar signature detection. This issue is observed in AP-125 running ArubaOS 6.1.x, 6.2.x, 6.3.x, and 6.4.x. **Workaround:** None.
91510	**Symptom**: An access point reboots occasionally without reboot reason or crash information. **Scenario**: This issue occurs on AP-134 and AP-135 connected to controllers running ArubaOS 6.3.0.1. **Workaround**: None.

Table 80: *AP-Wireless Known Issues*

Bug ID	Description
93380 93494 93687 93744	**Symptom:** Occasionally, an AP stops responding and reboots. **Scenario:** This issue is observed because of the Ethernet connectivity problem leading to loss of connectivity between the AP and controller. This issue occurs on AP-224 and AP-225 models and is not limited to a specific ArubaOS version. **Workaround**: Ensure that the Ethernet connection issue does not lead to loss of connectivity between the AP and the controller.
93511 93953	**Symptom:** The user gets error **Could not read cached limits** and **License number mismatch in cached limits** messages in a controller with master-local topology. **Scenario:** This issue is not limited to any specific controller model and is observed in controllers running ArubaOS 6.3 or later. **Workaround**: None.
95113 95086 95088 95111 95114 95115 95116 95117 95123 95124	**Symptom**: An iPad connected in tunnel mode using CCMP encryption becomes unreachable from the network once Airplay mirroring is initiated from iPad to Apple TV. **Scenario**: This issue occurs when an iPad is connected to a wireless network in forward-mode: Tunnel and opmodes: wpa2-aes/wpa2-psk-aes. This issue is observed in controllers and APs running ArubaOS 6.3.x.x or 6.4.x.x. **Workaround**: Disable **Multiple Tx Replay Counters** parameter under SSID profile.

Base OS Security

Table 81: *Base OS Security Known Issues*

Bug ID	Description
93550	**Symptom:** Running the **aaa test-server** command for a TACACS authentication server displays **AAA server timeout** in spite of successful authentication. **Scenario:** This issue is not limited to a specific controller model or software release version. **Workaround:** Issue the **aaa test-server** command twice.
95449	**Symptom:** A controller reboots and displays the message **Reboot Cause: Nanny rebooted machine - fpapps process died**. **Scenario:** This issue may occur in M3 controllers running ArubaOS 6.3 in a master-local topology. **Workaround:** None.

Captive Portal

Table 82: *Captive Portal Known Issues*

Bug ID	Description
92927	**Symptom:** When Apple® clients try to access a web page using captive portal, the controller displays **error occurred** message on the client's browser. **Scenario:** This issue is observed in a Virtual AP (VAP)-SSID enabled network with external captive portal authentication. Further investigation suggested that the backslash (\) character is not URL-encoded. As a result, external captive portal stops working for Apple clients. **Workaround:** None.
95922	**Symptom:** Captive portal log out does not work. **Scenario:** This issue is observed when you configure a captive portal profile with an external login page and custom captive portal certificate. This issue not limited to any specific controller model or release version. **Workaround:** None.

Configuration

Table 83: *Configuration Known Issues*

Bug ID	Description
93922	**Symptom:** A custom banner with the **#** delimiter gets added as part of the **show running-config** command output. **Scenario:** The issue is observed when an administrator configures the banner using the **banner motd** command in the controller with the **#** delimiter. This issue is not limited to a specific controller model and is observed in ArubaOS 6.3.1.1 or later versions. **Workaround:** None.
95535	**Symptom:** The ACL configuration on the local controllers goes out of sync intermittently with the master controller. **Scenario:** This issue may occur if there is a change in licenses. This issue is observed in controllers running ArubaOS 6.3 in a master-local topology. **Workaround:** Use the **clear master-local-session <local IP>** command on the master controller to sync the ACL configuration.

Controller-Datapath

Table 84: *Controller-Datapath Known Issues*

Bug ID	Description
88629	**Symptom:** ACL enforcement for Skype doesn't work consistently. **Scenario:** This issue occurs on 7200 Series controllers running ArubaOS 6.4. **Workaround:** None.
89722	**Symptom:** Facebook apps traffic is not getting classified correctly. **Scenario:** This issue occurs on 7200 Series controllers with dpi turned On. **Workaround:** None.
91085	**Symptom:** Google hangout sessions are classified as Google when AppRFv2 is enabled. **Scenario:** This issue occurs on 7200 Series controllers running ArubaOS 6.4. **Workaround:** None.

Table 84: *Controller-Datapath Known Issues*

Bug ID	Description
92248	**Symptom:** A crash occurs on a master controller and the log files for the event listed the reason for the crash as **datapath timeout**. **Scenario:** The trigger of this issue is not known and this issue is observed in 3400controllers running ArubaOS 6.3.1.0 in a master-local topology. **Workaround:** None.
92477	**Symptom:** Bittorrent sessions are not denied only when the deny rule is added in the middle of a bittorrent file download. **Scenario:** This issue occurs because the bittorrent control session information is teared down once the traffic is classified. This issue occurs on 7200 Series controllers with dpi turned On. **Workaround**: Creating a bittorrent rule in the user role to start with denies the bittorrent traffic.
92955	**Symptom:** When sending small sized data packets at high speed data rate through IPSec tunnel, the controller crashes due to **datapath timeout**. **Scenario:** This issue is observed when the controller sends IPSec traffic at 400 Mbps with 64 bytes packet size. This causes the controller's ingress queue run out of buffer. This issue is not limited to a specific controller model or software release version. **Workaround:** None.
93285	**Symptom:** An M3 controller reboots unexpectedly. The log files for the event listed the reason as **datapath timeout**. **Scenario**:This issue occurs in M3 controllers running ArubaOS 6.3.X.X. **Workaround:** None
93327	**Symptom:** World of warcraft (Wow) sessions are not getting classified with AppRF. **Scenario**: This issue occurs on 7200 Series controllers running ArubaOS 6.4 when AppRF is enabled. **Workaround:** None
93582	**Symptom:** A 7210 controller crashes. The logs for this error listed the reason for the crash as **datapath timeout**. **Scenario:** This issue is observed in 7210 controllers running ArubaOS 6.3.1.0. **Workaround:** None.
93817	**Symptom:** The master controller throws an internal error while provisioning APs that belong to a specific local controller. **Scenario:** This issue occurs on 3200 controllers running ArubaOS 6.3.1.1 in a master-local topology. **Workaround:** None.
94143	**Symptom:** A 3200 controller reboots unexpectedly. The log files for the event listed the reason as **datapath timeout**. **Scenario:** This issue is observed on a 3200 controller running ArubaOS 6.3.1.1. **Workaround:** None.
93203 94200	**Symptom:** A local controller reboots unexpectedly. The log files for the event listed the reason for the reboot as **datapath exception**. **Scenario:** This issue is observed in 7220 controller running ArubaOS 6.3.1.1 in a master-local topology. **Workaround:** None.
94267	**Symptom**: After an upgrade to ArubaOS 6.3.1.x, clients were unexpectly disconnected from the network, or were unable to pass traffic for 2-3 minutes after roaming between APs. **Scenario**: This issue was observed in Psion Omni handleld scanners roaming between AP-175 and AP-120 Series APs running ArubaOS 6.3.1.1. **Workaround**: None.
94636	**Symptom:** A crash occurs on a local controller and the log files for the event listed the reason for the crash as **datapath timeout**.

Table 84: *Controller-Datapath Known Issues*

Bug ID	Description
	Scenario: The trigger of this issue is not known and this issue is observed in 7210 controllers running ArubaOS 6.3.0.1. **Workaround:** None.
93203 94965 95719	**Symptom:** A 7210 controller crashes. The logs for this error listed the reason for the crash as **datapath timeout**. **Scenario:** The trigger of this issue is not known and this issue is observed in 7210 controllers running ArubaOS 6.3.1.1 in a master-local topology. **Workaround:** None.
95286	**Symptom:** A master controller crashes with log message **datapath timeout**. **Scenario:** The trigger of this issue is unknown and is observed in 7220 controllers running ArubaOS 6.3.1.1. **Workaround:** None.

Controller-Platform

Table 85: *Controller-Platform Known Issues*

Bug ID	Description
80200 81225 81752 81930 84672 85422 87079 89014 89243 89726	**Symptom:** The 600 Series and 3000 Series controllers reboots with kernel panic. **Scenario:** This issue is observed because of high traffic in control plane for a sustained period. This issue occurs on 600 Series and 3000 Series controllers running ArubaOS 6.3.0.0 or later. **Workaround:** Configure bandwidth contracts depending on the incoming traffic.
92968	**Symptom:** Generating the **tech-support.log** file from the WebUI of the controller gets truncated at times. **Scenario:** This issue is not limited to a specific controller model and is observed in ArubaOS 6.2.1.3, ArubaOS 6.3.1.0 or later versions. **Workaround:** Issue the **tar logs tech-support** command from the CLI to download the **tech-support.log** file.
93465	**Symptom:** A local controller reboots unexpectedly. The log files for the event listed the reason for the reboot as **Control Processor Kernel Panic**. **Scenario:** This issue occurs when the controller releases the memory of corrupted data packets. This issue is observed in 3000 Series and M3 controllers running ArubaOS 6.3.1.1 in a master-local topology. **Workaround:** None.
94862	**Symptom:** The master controller reboots unexpectedly with the message: "user reboot (shell)." **Scenario:** This issue occurs on the 7200 Series controllers with AP-225 APs following an upgrade to ArubaOS 6.4. **Workaround:** None.
95071	**Symptom**: Issuing a show command from the CLI of a standby controller running ArubaOS 6.3.1.1 triggers the error "Module Configuration Manager is Busy" **Scenario**: This issue was observed in a standby 3600 controller in a master-standby topology, **Workaround**: None.

DHCP

Table 86: *DHCP Known Issues*

Bug ID	Description
94345	**Symptom:** The Symbol N410 and Android devices do not receive an IP address from the internal DHCP Server. **Scenario:** This issue is observed on controllers running ArubaOS 6.3.1.1 and occurs when the controller's internal DHCP is configured to serve IP addresses for these devices. **Workaround:** Use an external DHCP server.
95166	**Symptom:** When a controller is configured as a DHCP server,by default it attempts Dynamic DNS updates and the following log message appears: "dhcpd: if CU-iPad-2-64-GB.aspect.com IN A rrset doesn't exist add CU-iPad-2-64-GB.aspect.com 10800 IN A 169.136.135.108: destination address required." **Scenario:** This issue is observed on controllers running ArubaOS 6.3 and later. It is caused when the DHPCD server issues a DHCP address and then attempts a DDNS update. **Workaround:** None.

Hardware-Management

Table 87: *Hardware-Management Known Issues*

Bug ID	Description
87191 87808	**Symptom:** A controller unexpectedly stops responding and reboots. **Scenario:** This issue is observed when a module (hwMon) crashes on the controller. This issue occurs on M3 series controllers running ArubaOS 6.3.0.1 or later. **Workaround:** None.

IPSec

Table 88: *IPSec Known Issues*

Bug ID	Description
80460	**Symptom:** Remote client and Site-to-Site VPN performance is low and does not scale to the controller limit when IKEv2 with GCM256-EC384 encryption algorithm configured. **Scenario:** This issue is observed on 600 Series, 3000 Series, and M3 controllers and occurs when the IKE session is established to a standby unit in a failover deployment. **Workaround:** None.
95634	**Symptom:** Site-to-Site IPsec VPN tunnels randomly lose connectivity on a 7210 controller. **Scenario:** This issue is observed where there are 500 or more remote sites terminating IPsec VPN tunnels on a 7210 controller. This issue is observed on a 7210 controller running ArubaOS 6.3.1.2. **Workaround:** None.

Local Database

Table 89: *Local Database Known Issues*

Bug ID	Description
95277	**Symptom:** The Remote AP whitelist on a master controller is not correctly synchronizing entries to local controllers. **Scenario:** This issue occurs in ArubaOS 6.3.x.x when the description field of a remote whitelist entry contains an apostrophe ('). **Workaround:** Remove the apostrophe from the whitelist entry description.

LLDP

Table 90: *LLDP Known Issues*

Bug ID	Description
92998	**Symptom:** The remote interface name appears as **Not received** while issuing the **show lldp neighbor** command. **Scenario**: This issue occurs when Link Layer Discovery Protocol (LLDP) is enabled on the controller and if the neighbor is a third-party device such as Arista or Alcatel. This issue is not specific to any controller model and occurs on ArubaOS running 6.4. **Workaround:** None.
94647	**Symptom:** In rare cases, a **lldp GSM PORT_INFO Lookup failed at Function: sm_handle_lldp_info_events** error message appears in the log. **Scenario:** This issue occurs when the script to shut or open the interface is executed multiple times. This issue is not limited to any specific controller model and occurs on ArubaOS running 6.4. **Workaround:** None.

Master-Local

Table 91: *Master-Local Known Issues*

Bug ID	Description
88430	**Symptom:** User-role configuration is lost after upgrading master, standby, and local controllers to ArubaOS 6.3.1 or later versions. **Scenario:** This issue is observed on a 7200 Series controller running ArubaOS 6.3.1 or later versions. **Workaround:** Disabling the configuration snapshot by executing the **cfgm set sync-type complete** command on master and standby controllers prevents partial configuration loss. Wait at least five (5) minutes after the upgraded master and standby have rebooted before reloading the upgraded local controller.
88919	**Symptom:** Global configuration like user-role on the master controller does not synchronize with the local controller after issuing the **write memory** command. **Scenario:** This issue is observed in a master-local topology. This issue is observed in 7200 Series controller running ArubaOS 6.3.0.0 or later versions. **Workaround:** On the master controller, issue the **cfgm set sync-type complete** command, followed by the **write memory** command to send the complete configuration file to the local controller.

RADIUS

Table 92: *RADIUS Known Issues*

Bug ID	Description
94081	**Symptom:** Multiple authentication failures are observed in the controllers. **Scenario:** This issue is observed when external LDAP server is used for authentication. This issue is not limited to a specific controller models and occurs in ArubaOS running 6.3.x versions. **Workaround:** Reduce LDAP timeout parameter value to 3 seconds for LDAP servers.

Remote AP

Table 93: *Remote AP Known Issues*

Bug ID	Description
95572	**Symptom:** Wired clients are unable to access the internet when connected to a Remote AP (RAP). **Scenario:** This issue is observed when wired clients cannot pass traffic locally with source NAT in split-tunnel forwarding mode. This issues is observed when the 3200 controller is upgraded from ArubaOS 6.1.3.6 to ArubaOS 6.3.1.2. **Workaround:** None.
95658	**Symptom:** Cisco® Unified IP Phone 7945G reboots randomly during an active voice call. **Scenario:** This issue is observed when a Cisco Unified IP Phone 7945G is connected to a Power over Ethernet (PoE) port of a RAP-3WNP remote AP. This issues is observed in ArubaOS 6.3.0.1. **Workaround:** None.

Station Management

Table 94: *Station Management Known Issues*

Bug ID	Description
85662 84880 88009 88319 89321 92164 93243 93388 93389 93984	**Symptom:** The state of APs are displayed as **down** on the master controller even if these APs are connected and UP. **Scenario**: This issue is observed when AP's system profile has a local controller as the primary Local Management Switch (Primary-LMS) and master controller is configured as a backup Local Management Switch (Backup-LMS). This issue is not limited to any specific controller model and occurs in ArubaOS running 6.3 or later. **Workaround:** Remove master controller as backup LMS during initial phase.
91758	**Symptom**: Stationary Apple® MacBook laptops unexpectedly disassociated from APs, and were temporarily unable to pass traffic for 3-5 minutes during a period when many users on the network were roaming between APs. **Scenario**: This issue occurs on a network with a controller running ArubaOS 6.3.1.1 with ARM channel assignment and scanning features enabled. **Workaround**: Disable ARM channel assignment and scanning features.

Voice

Table 95: *Voice Known Issues*

Bug ID	Description
87316	**Symptom:** The Call Detailed Record (CDR) for a VoIP client goes into **ABORTED** state due to session age out. **Scenario:** This issue is observed in an L3 mobility deployment when the Real-time Transport Protocol (RTP) packets do not tunnel to the Home Agent (HA) while the call is active. This issue is observed in controllers running ArubaOS 6.4. **Workaround:** None.
90888	**Symptom:** The **show voice real-time-analysis** command does not display any result for voice calls between Microsoft® Lync clients. **Scenario:** This issue is observed when Microsoft Lync clients are connected to the same Remote AP (RAP) in split-tunnel forwarding mode. In such a case, the voice packets are locally routed through the RAP without forwarding it to the controller. As a result, the controller does not display any Real-time Transport Analysis (RTPA) report. This issue is observed in controllers running ArubaOS 6.4. **Workaround:** None.

WebUI

Table 96: *WebUI Known Issues*

Bug ID	Description
90026	**Symptom:** When a user attempts to access the controller WebUI, the WebUI returns the **Session Invalid** error message. **Scenario:** The user is forced to attempt to access the WebUI two to three times before successfully logging in. Each failed attempt returns the **Session Invalid** error message. This error occurs on controllers running ArubaOS 6.3.0.1. **Workaround:** None.
93454	**Symptom:** The **Dashboard** > **Spectrum** page of the WebUI is not loading and re-subscription fails frequently. **Scenario:** This issue is observed in AP-105 access points associated to controllers running ArubaOS 6.3.0.1. **Workaround:** Use the **ap spectrum clear-webui-view-settings** command to avoid this issue.
95185	**Symptom:** Collecting the **logs.tar** and **tech-support** logs from the controller's WebUI fails with **Error running report… Error: receiving data from CLI, interrupted system call** error message. **Scenario:** This issue is not seen under the following cases: • Downloading the **logs.tar** without the **tech-support** log from the WebUI. • Downloading the **logs.tar** and **tech-support** logs from the CLI. This issue is observed in 7220 controller running ArubaOS 6.3.1.2. **Workaround:** Download the **logs.tar** and **tech-support** logs from the CLI.

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 any version of ArubaOS 6.4.0.2, take note of these known upgrade caveats.

- If your deployment includes AirWave, you must upgrade to AirWave 7.7.10. For more information, see ArubaOS-AirWave Cross-Site Request Forgery Mitigation on page 13.
- If your controller is running ArubaOS 6.4, do not use TFTP to copy an ArubaOS image onto the non-boot partition of the controller for upgrading or downgrading. Use FTP or SCP to copy the image. For more information, see bug ID 97789 on page 21.
- AP LLDP profile is not supported on AP-120 Series in ArubaOS 6.4.
- Starting from ArubaOS 6.3.1, the local file upgrade option in the 620 and 650 controller WebUI has been disabled.
- The local file upgrade option in the 7200 Series controller WebUI does not work when upgrading from ArubaOS 6.2. When this option is used, the controller displays the error message **Content Length exceed limit** and the upgrade fails. All other upgrade options work as expected.
- ArubaOS 6.4 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. Once the second ACE entry is added, the first would be over written.

```
(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 is supported only on the newer MIPS controllers (7200 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 if your deployment contains a mix of MIPS and PPC controllers in a master-local setup.
- When upgrading the software in a multi-controller 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 Multi-Controller Network on page 91.)
- PhoneHome setting will be disabled when the controller is upgraded from ArubaOS 6.4.0.0 to ArubaOS 6.4.0.2, regardless of whether PhoneHome was enabled or disabled. The current PhoneHome setting will be preserved if the controller is upgraded directly to ArubaOS 6.4.0.2 from ArubaOS 6.1, 6.2, or 6.3.

Installing the FIPS Version of ArubaOS 6.4.0.2

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

Before Installing FIPS Software

Before you install a FIPS version of software on a controller that is currently running a non-FIPS version of the software, you must reset the configuration to the factory default or you will not be able to login to the CLI or WebUI. Do this by running the **write erase** command just prior to rebooting the controller. This is the only supported method of moving from non-FIPS software to FIPS software.

Important Points to Remember and Best Practices

Ensure a successful upgrade and optimize your upgrade procedure by taking the recommended actions listed below. 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 during the upgrade, such as configuration changes, hardware upgrades, or changes to the rest of the network. 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 issuing 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 then 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 ArubaOS 6.4.0.2, assess your software license requirements and load any new or expanded licenses you require. For a detailed description of these new license modules, refer to the "Software Licenses" chapter in the 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, Aruba recommends the following compact memory best practices:

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

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 issue the **halt** command before power cycling.

If the output of the **show storage** command indicates that insufficient flash memory space is available, you must free up additional 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 memory before upgrading:

- **Crash Data:** Issue 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 89 to copy the **crash.tar** file to an external server, then issue the command **tar clean crash** to delete the file from the controller.
- **Flash Backups:** Use the procedures described in Backing up Critical Data on page 89 to back up the flash directory to a file named **flash.tar.gz**, then issue the command **tar clean flash** to delete the file from the controller.
- **Log files:** Issue 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 89 to copy the **logs.tar** file to an external server, then issue the command **tar clean logs** 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

Back Up and Restore 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 on 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. Click **Restore**.

Back Up and Restore Compact Flash in the CLI

The following steps describe the back up and restore procedure for the entire compact flash file system using the controller's command line:

1. Enter **enable** mode in the CLI on the controller, and enter the following command:
   ```
   (host) # write memory
   ```
2. Use 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. Use 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> [<remote directory>]

   Password: <ftp-password>
   (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 with the copy command:
   ```
   (host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
   (host) # copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
   ```
4. Use the restore command to untar and extract the **flashbackup.tar.gz** file to the compact flash file system:
   ```
   (host) # restore flash
   ```

Upgrading in a Multi-Controller Network

In a multi-controller 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 89.

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 the same model.

To upgrade an existing multi-controller system to ArubaOS 6.4.0.2:

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. Once 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 6.4.0.2

Install using the WebUI

CAUTION

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash available for an upgrade using the WebUI. For details, see Memory Requirements on page 89

NOTE

When you navigate to the **Configuration** tab of the controller's WebUI, the controller may display an error message **Error getting information: command is not supported on this platform**. 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 6.4.0.2.

- For ArubaOS 3.x.versions earlier than ArubaOS 3.4.4.1, download the latest version of ArubaOS 3.4.5.x.
- For ArubaOS 3.x or 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 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 91 to install the interim version of ArubaOS, then repeat step 1 to step 11 of the procedure to download and install ArubaOS 6.4.0.2.

Upgrading From a Recent version of ArubaOS

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

- 3.4.4.1 or later
- 5.0.3.1 or later 5.0.x (If you are running ArubaOS 5.0.3.1 or the latest 5.0.x.x, review Upgrading to ArubaOS 6.4.0.2 on page 91 before proceeding further.)
- 6.0.1.0 or later 6.x

Install the ArubaOS software image from a PC or workstation using the Web User Interface (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 6.4.0.2 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 file **Aruba.sha256** from the download directory.
   b. To verify the image, load the image onto a Linux system and execute the command **sha256sum <filename>** 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 pre-loaded onto 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. Select the **Upload Local File** option, then click **Browse** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. In the **partition to upgrade** field, select the non-boot partition.
8. In the **Reboot Controller After Upgrade** option field, best practices is to select **Yes** to automatically reboot after upgrading. If you do not want the controller to reboot immediately, select **No**. Note however, that the upgrade will not take effect until you reboot the controller.
9. In the **Save Current Configuration Before Reboot** field, select **Yes**.
10. Click **Upgrade**.
11. When the software image is uploaded to the controller, a popup window displays the message **Changes were written to flash successfully**.Click **OK**. If you chose to automatically reboot the controller in step 7, 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 > Controller > Controller Summary** page to verify the upgrade.

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

1. Log in into the WebUI to verify all your controllers are up after the reboot.
2. Navigate to **Monitoring > Network Summary** to determine if your APs are up and ready to accept clients.
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 back up 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 89 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 available for an upgrade using the CLI. For details, see Memory Requirements on page 89.

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 6.4.0.2.

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

Follow step 2 - step 7 of the procedure described in Upgrading From a Recent Version of ArubaOS on page 93 to install the interim version of ArubaOS, then repeat step 1 to step 7 of the procedure to download and install ArubaOS 6.4.0.2.

Upgrading From a Recent Version of ArubaOS

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

- 3.4.4.1 or later
- 5.0.3.1 or later 5.0.x (If you are running ArubaOS 5.0.3.1 or the latest 5.0.x.x, review Upgrading to ArubaOS 6.4.0.2 on page 91 before proceeding further.)
- 6.0.1.0 or later 6.x

To install the ArubaOS software image from a PC or workstation using the Command-Line Interface (CLI) on the controller:

1. Download ArubaOS 6.4.0.2 from the customer support site.
2. Open a Secure Shell session (SSH) 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. Use the **show image version** command to check the ArubaOS images 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**
   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
   ```

5. Use the **copy** command to load the new image onto the non-boot 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 only available on the 7200 Series controllers.

6. Issue the **show image version** command to verify the new image is loaded:

```
(hostname)# show image version

---------------------------------
Partition               : 0:0 (/dev/hda1) **Default boot**
Software Version        : ArubaOS 6.4.0.2 (Digitally Signed - Production Build)
Build number            : 42757
Label                   : 42757
Built on                : Tue Mar 18 09:38:33 PDT 2014
---------------------------------
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
```

7. Reboot the controller:

```
(hostname)# reload
```

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

```
(hostname)# show version
```

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

1. Log in into the command-line interface to verify all your controllers are up after the reboot.
2. Issue the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Issue 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 89 for information on creating a backup.

Downgrading

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

If you upgraded from 3.3.x to 5.0, the upgrade script encrypts the internal database. New entries created in ArubaOS 6.4.0.2 are lost after the downgrade (this warning does not apply to upgrades from 3.4.x to 6.1).

If you do not downgrade to a previously-saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from ArubaOS 6.4.0.2 to 5.0.3.2, changes made to WIPS in 6.x prevents 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 think you have encountered this issue, use the **show profile-errors** and **show ap-group** commands to view the IDS profile associated with 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 pre-upgrade software version, you must perform the following steps:

1. Back up your controller. For details, see Backing up Critical Data on page 89.
2. Verify that control plane security is disabled.
3. Set the controller to boot with the previously-saved pre-6.4.0.2 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 displays if system boot parameters are set for incompatible image and configuration files.
5. After downgrading the software on the controller:
   - Restore pre-6.4.0.2 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.4.0.2 flash backup file.
   - You do not need to re-import the WMS database or RF Plan data. However, if you have added changes to RF Plan in ArubaOS 6.4.0.2, the changes do not appear in RF Plan in the downgraded ArubaOS version.
   - If you installed any certificates while running ArubaOS 6.4.0.2, you need to reinstall the certificates in the downgraded ArubaOS version.

Downgrading Using the WebUI

The following sections describe how to use the WebUI to downgrade the software on the controller.

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

c. Click **Upgrade**.

4. Navigate to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the system partition that contains the pre-upgrade image file as the boot partition.
   b. Click **Apply**.
5. Navigate to the **Maintenance > Controller > Reboot Controller** page. Click **Continue**. The controller reboots after the countdown period.
6. When the boot process is complete, verify that the controller is using the correct software by navigating to the **Maintenance > Controller > Image Management** page.

Downgrading Using the CLI

The following sections describe how to use the CLI to downgrade the software on the controller.

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

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

   or

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

2. Set the controller to boot with your pre-upgrade configuration file.

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

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

   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 6.4.0.2 image:

   ```
   #show image version
   ---------------------------------
   Partition               : 0:0 (/dev/hda1) **Default boot**
   Software Version        : ArubaOS 6.4.0.2 (Digitally Signed - Production Build)
   Build number            : 42757
   Label                   : 42757
   Built on                : Tue Mar 18 09:38:33 PDT 2014
   ---------------------------------
   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 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) 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.