ArubaOS 6.5.4.22

a Hewlett Packard
Enterprise company

Release Notes

Copyright Information

Open Source Code

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

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

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Aruba will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

Revision History

The following table lists the revision numbers and the corresponding changes that were made in this release.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

Chapter 1
Release Overview

This ArubaOS release notes includes the following topics:

- New Features on page 9
- Regulatory Updates on page 10
- Resolved Issues on page 11
- Known Issues on page 12
- Upgrade Procedure on page 24

For the list of terms, refer Glossary.

Supported Browsers

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

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

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	https://asp.arubanetworks.com/
Airheads Social Forums and Knowledge Base	community.arubanetworks.com

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

Chapter 2
New Features

There are no new features introduced in ArubaOS 6.5.4.22 release.

Chapter 3
Regulatory Updates

This chapter contains the regulatory updates in ArubaOS 6.5.4.22.

NOTE

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

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

The following DRT file version is part of this release.

- DRT-1.0_82868

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

NOTE

The FCC has changed the rules for operation in all of the 5 GHz bands. For more information, refer to the *FCC DFS Regulatory Change Impact and Resolution Plan - Support Advisory* available in Support Advisories.

Chapter 4
Resolved Issues

This chapter describes the issues resolved in this release.

NOTE

We have migrated to a new defect tracking tool. Some bugs are listed with the new bug ID, which is prefixed by AOS.

Table 3: *Resolved Issues in ArubaOS 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-229991	–	**Symptom:** Clients were unable to connect to SSIDs that had the 802.11r option enabled. During this period, commands run in the CLI returned the error message, **Module AP STM Low Priority is busy**. **Please try later**. The fix ensures that SSIDs configured with 802.11r option service the client as expected. **Scenario:** This issue was observed in APs running ArubaOS 6.5.4.21 or later versions. **Duplicates:** AOS-230192, AOS-230290, AOS-230554, AOS-230604, AOS-230721, AOS-230871, AOS-229972, AOS-230416, and AOS-230725	Station Management	All platforms	ArubaOS 6.5.4.21

Chapter 5 Known Issues

This chapter describes the known issues identified in this release:

NOTE

We have migrated to a new defect tracking tool. Some bugs are listed with the new bug ID, which is prefixed by AOS.

Table 4: *Known Issues in ArubaOS 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-127982 AOS-145349	154887 177271	**Symptom:** Some APs display incorrect IPv6 addresses when checked using SNMP. **Scenario:** This issue is observed in APs running ArubaOS 6.5.1.9 or later versions. **Workaround:** None.	SNMP	All platforms	ArubaOS 6.5.1.9
AOS-128831 AOS-147829 AOS-148994	155936 180912 182485	**Symptom:** A controller does not respond to the PPP LCP echo request messages from a PPPoE server making the PPPoE link unusable. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.1.2 or later versions. **Workaround:** None.	PPPoE	All platforms	ArubaOS 6.5.1.2
AOS-130510 AOS-177783	158149 176715	**Symptom:** The BLE scanning in an AP is slow and fewer BLE devices are reported. **Scenario:** This issue is observed in AP-207 access points running ArubaOS 6.5.2.0 or later versions. **Workaround:** None.	BLE	AP-207 access points	ArubaOS 6.5.2.0
AOS-133222	161655	**Symptom:** Some high-frequency radio statistics like Tx time, Rx time, and Rx clear are not collected correctly per beacon period in an AP. **Scenario:** This issue is observed in APs running ArubaOS 6.5.2.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 6.5.2.0

Table 4: *Known Issues in ArubaOS 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-133616 AOS-144468 AOS-144501	162140 176047 176088	**Symptom:** The BLE devices connected to an AP display the value of the output as **Ineligible** for the **show ap debug ble-update-status ap-name** command. **Scenario:** This issue is observed in APs running ArubaOS 6.5.3.3 or later versions. **Workaround:** None.	IoT	All platforms	ArubaOS 6.5.3.3
AOS-134588	163341	**Symptom:** Some clients stop sending data traffic after every three hours approximately. **Scenario:** This issue occurs due to broken L3 connectivity. This issue is observed in APs running ArubaOS 6.5.1.5 or later versions. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 6.5.1.5
AOS-137064 AOS-140141	166426 167050 170409	**Symptom:** A master controller and a standby controller reboot unexpectedly. The log file lists the reason for this event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. **Scenario:** This issue occurs when clients send A-MSDU traffic to controllers. This issue is observed in 7000 Series controllers running ArubaOS 6.5.1.9 or later versions in a master-standby topology. **Workaround:** None.	Controller-Datapath	7000 Series controllers	ArubaOS 6.5.1.9
AOS-137371 AOS-142604	166800 173645	**Symptom:** False detections of type-5 radars are triggered in the FCC domain. **Scenario:** This issue is observed in 200 Series and 220 Series access points running ArubaOS 6.5.1.5 or later versions. **Workaround:** None.	AP-Wireless	200 Series and 220 Series access points	ArubaOS 6.5.1.5
AOS-138939	168789	**Symptom:** An AP with 802.1X supplicant configuration fails to boot. **Scenario:** This issue occurs when an ACL denies a DNS response from the DNS server. This issue is observed in APs running ArubaOS 6.5.4.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 6.5.4.0

Table 4: *Known Issues in ArubaOS 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-139580	169622	**Symptom:** A syslog server displays the error message, **aruba_change_channel 512 channel 6 mode 3 not found** for some APs. **Scenario:** This issue is observed in AP-314 and AP-315 access points running ArubaOS 6.5.1.5. **Workaround:** None.	AP-Wireless	AP-314 and AP-315 access points	ArubaOS 6.5.1.5
AOS-139880 AOS-139898	170037 170055	**Symptom:** An AP does not discover a master controller through ADP. **Scenario:** This issue occurs when a static IP address is configured in an AP and the ACL denies ADP packets. This issue is observed in APs running ArubaOS 6.5.4.2 or later versions. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 6.5.4.2
AOS-140642	171103	**Symptom:** A controller crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.1.9 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 6.5.1.9
AOS-141091	171726	**Symptom:** A controller crashes and reboots unexpectedly. The log lists the reason for the event as **Datapath timeout (SOS Assert) (Intent: cause:register 54:86:50:2)**. **Scenario:** This issue is observed in 7220 controllers running ArubaOS 6.5.3.3. **Workaround:** None.	Controller-Datapath	7220 controllers	ArubaOS 6.5.3.3
AOS-141528	172305	**Symptom:** A controller sends multiple SNMP error messages, **snmp[21466]: PAPI_Send: To: 7f000001:8419 Type:0x4 Timed out**. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.1.9 or later versions. **Workaround:** None.	SNMP	All platforms	ArubaOS 6.5.1.9

Table 4: *Known Issues in ArubaOS 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-141755	172593	**Symptom:** ACLs are not displayed in the output of the **show datapath acl ap-name** command because acl entry parameters (d->index and d->entry.flags) are not set correctly on little endian APs. **Scenario:** This issue is observed in ArubaOS 6.5.1.9 or later versions. **Workaround:** None.	Captive Portal	All platforms	ArubaOS 6.51.9
AOS-142093	172987	**Symptom:** A controller crashes and reboots unexpectedly. The log file lists the reason for the event as **Kernel panic: Fatal exception**. **Scenario:** This issue is observed in 7210 controllers running ArubaOS 6.5.3.3 or later versions. **Workaround:** None.	Controller-Datapath	7210 controllers	ArubaOS 6.5.3.3
AOS-142230	173168	**Symptom:** AppRF does not block Hotspot-Shield traffic in a controller. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.1.9 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 6.5.1.9
AOS-142392	173359	**Symptom:** A controller crashes and reboots unexpectedly. The log file lists the reason for this event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in 7240 controllers running ArubaOS 6.5.3.3 or later versions. **Workaround:** None.	Controller-Datapath	7240 controllers	ArubaOS 6.5.3.3
AOS-142474	173465	**Symptom:** A controller crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in 7220 controllers running ArubaOS 6.5.4.3 or later versions. **Workaround:** None.	Controller-Datapath	7220 controllers	ArubaOS 6.5.4.3

Table 4: *Known Issues in ArubaOS 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-143005	174150	**Symptom:** A controller crashes and reboots unexpectedly. The log file lists the reason for this event as **Datapath crash**. **Scenario:** This issue is observed in7280 controllers running ArubaOS 6.5.4.2 or later versions. **Workaround:** None.	Controller-Datapath	7280 controllers	ArubaOS 6.5.4.2
AOS-143252	174473	**Symptom:** A controller crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath crash**. **Scenario:** This issue is observed in7280 controllers running ArubaOS 6.5.4.0 or later versions. **Workaround:** None.	Controller-Datapath	7280 controllers	ArubaOS 6.5.4.0
AOS-143457	174743	**Symptom:** A controller crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath crash**. **Scenario:** This issue is observed in7280 controllers running ArubaOS 6.5.4.0 or later versions. **Workaround:** None.	Controller-Datapath	7280 controllers	ArubaOS 6.5.4.0
AOS-143904	175340	**Symptom:** The AP logs for a Remote AP displays the error message, **connect-debounce failed, port 1 disabled**. **Scenario:** This issue is observed in Remote Access Points running ArubaOS 6.5.3.1 or later versions. **Workaround:** None.	AP-Platform	RAP-3WNP access points	ArubaOS 6.5.3.1
AOS-144022	175493	**Symptom:** A controller crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in a 7240 controllers running ArubaOS 6.5.3.3 or later versions. **Workaround:** None.	Controller-Datapath	7240 controllers	ArubaOS 6.5.3.3
AOS-144689	176344	**Symptom:** A controller does not retain the cached ACR license. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.3.3-FIPS version. **Workaround:** None.	Licensing	All platforms	ArubaOS 6.5.3.3-FIPS

Table 4: *Known Issues in ArubaOS 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-144882	176622	**Symptom:** The UCC data export function is missing from the ArubaOS 6.5.1.9 version running in a controller. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.1.9 or later versions. **Workaround:** None.	UCC	All platforms	ArubaOS 6.5.1.9
AOS-145636	177651	**Symptom:** Some Windows 64-bit clients detected 32-bit version of VIA while trying to download it using Microsoft Edge browser. **Scenario:** This issue is observed in AP-225 access points running ArubaOS 6.5.1.4 or later versions. **Workaround:** None.	AP-Wireless	AP-225 access points	ArubaOS 6.5.1.4
AOS-145876 AOS-156159 AOS-157877	177969 192218 194648	**Symptom:** On a 2.4 GHz radio, channel utilization is very low for a few APs. **Scenario:** This issue is observed in AP-203R, AP-207, and AP-315 access points running ArubaOS 6.5.4.0 or later versions. **Workaround:** None.	AP-Wireless	AP-203R, AP-207, and AP-315 access points	ArubaOS 6.5.4.9
AOS-146105 AOS-179536	185354	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **rebooted caused by external watchdog reset**. **Scenario:** This issue occurs in the driver when multicast or DMO performance test is done either in bridge mode or tunnel mode. This issue is observed in AP-203H, AP-203R, and AP-207 access points running ArubaOS 6.5.4.8 or later versions. **Workaround:** None.	AP-Wireless	AP-203H, AP-203R, and AP-207 access points	ArubaOS 6.5.4.8
AOS-146948	179408	**Symptom:** A controller log file displays **|localdb| |wl-sync| Skipping db_sync** messages. **Scenario:** This issue is observed in 7220 controllers running ArubaOS 6.5.3.4 or later versions. **Workaround:** None.	802.1X	7220 controllers	ArubaOS 6.5.3.4

Table 4: *Known Issues in ArubaOS 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-147232 AOS-158495 AOS-184142	179942 195511	**Symptom:** A client is unable to send or receive traffic to or from an AP. **Scenario:** This issue occurs when the station management process in an AP sends a PAPI message to the AAC instead of the UAC. This issue is observed in controllers in a cluster topology running ArubaOS 6.4.4.22 with 802.11r enabled. **Workaround:** None.	Station Management	All platforms	ArubaOS 6.4.4.22
AOS-147309	180094	**Symptom:** The console output of an AP shows **asap_user_set_acl: no name for id 0** message with the MAC address of the associated clients. **Scenario:** This issue is observed in APs running ArubaOS 6.5.3.6 or later versions. **Workaround:** None.	Authentication	All platforms	ArubaOS 6.5.3.6
AOS-148146 AOS-180312	181354	**Symptom:** Some clients experience ping loss while pinging a controller. **Scenario:** This issue occurs when the controller is connected to a mesh point. This issue is observed in controllers running ArubaOS 6.5.4.8 or later versions. **Workaround:** None.	Mesh	All platforms	ArubaOS 6.5.4.8
AOS-148329	181606	**Symptom:** The output of the **show ap debug log** command displays the **Bridge entry insertion failure** error message. **Scenario:** This issue is observed in AP-225 and AP-335 access points running ArubaOS 6.5.4.5 or later versions. **Workaround:** None.	AP Datapath	AP-225 and AP-335 access points	ArubaOS 6.5.4.5
AOS-149135	182683	**Symptom:** The redirect page is blank and displays only **URL=** for WISPR clients. **Scenario:** This issue occurs when CPU utilization is high. This issue is observed in controllers running ArubaOS 6.5.1.6 or later versions. **Workaround:** None.	WISPR Interoperability	All platforms	ArubaOS 6.5.1.6

Table 4: *Known Issues in ArubaOS 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-151814	186224	**Symptom:** Clients are unable to connect to a bridge mode virtual AP after a VLAN assignment failure. **Scenario:** This issue occurs when the VLAN in a controller is removed, causing subsequent deauthentication of all the clients associated with the virtual APs. This issue is observed in controllers running ArubaOS 6.5.4.6 or later versions. **Workaround:** None.	Station Management	All platforms	ArubaOS 6.5.4.6
AOS-152338	186981	**Symptom:** The SNMP polling displays **incorrect privacy password** mismatch error though the credentials are correct. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.3.6 or later versions. **Workaround:** None.	SNMP	All platforms	ArubaOS 6.5.3.6
AOS-153087	188021	**Symptom:** A controller generates the console error message, **|snmp| An internal system error has occurred at file ../unix/aruba_main.c function snmpRequestProcessing line 704 error Cannot send snmp response**. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.4.6 or later versions. **Workaround:** None.	SNMP	All platforms	ArubaOS 6.5.4.6
AOS-153844	189017	**Symptom:** A few 802.11b clients are unable to pass traffic. **Scenario:** This issue is observed in AP-305 access points running ArubaOS 6.5.4.0 or later versions. **Workaround:** None.	AP-Wireless	AP-305 access points	ArubaOS 6.5.4.6
AOS-154191	189490	**Symptom:** Some APs send AMON messages such as **CL_HT_MODE** with incorrect values displaying 0, 9, and 255. **Scenario:** This issue is observed in APs running ArubaOS 6.5.4.7 or later versions. **Workaround:** None.	Station Management	All platforms	ArubaOS 6.5.4.7
AOS-154324	189646	**Symptom:** Some clients using Fing mobile software are able to discover some wireless devices connected to the same AP. **Scenario:** This issue is not restricted to any specific controller model or ArubaOS release version. **Workaround:** None.	Multicast	All platforms	ArubaOS 6.5.4.8

Table 4: *Known Issues in ArubaOS 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-154460	189816	**Symptom:** The WebUI of a controller does not display the certificate information in the **Configuration** > **Management** tab. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.4.8 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 6.5.4.8
AOS-154965	190482	**Symptom:** The global timers in the **Configuration** > **Security** > **Authentication** > **Advanced** tab cannot be configured. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.4.9 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 6.5.4.9
AOS-155267	190912	**Symptom:** The **show datapath bridge ap-name** and **show ap mesh debug forwarding-table ap-name** commands run into an infinite loop and display the **Warning: Not enough memory to complete this operation** error message. **Scenario:** This issue occurs when the AP is configured as a Remote AP with PPPoE enabled. This issue is observed in controllers running ArubaOS 6.5.4.9 or later versions. **Workaround:** None.	RAP-NG	All platforms	ArubaOS 6.5.4.9
AOS-156027	192034	**Symptom:** An AP stops broadcasting on 2.4 GHz radios. **Scenario:** This issue is observed in AP-105 access points connected to controllers running ArubaOS 6.5.3.4 or later versions. **Workaround:** None. **Duplicates:** **New ID:** AOS-157576, AOS-158392, AOS-158580, AOS-182796, AOS-183992, AOS-184344 **Old ID:** 194197, 195377, 195607	AP-Wireless	AP-105 access points	ArubaOS 6.5.3.4
AOS-156223	192294	**Symptom:** Some BSSIDs are classified as interfering instead of being classified as **suspected-rogue**. **Scenario:** This issue occurs when **rules_match_mask** does not reset while resetting the Remote AP attributes. This issue is observed in APs running ArubaOS 6.5.1.10 or later versions. **Workaround:** None.	Air Management-IDS	All platforms	ArubaOS 6.5.1.10

Table 4: *Known Issues in ArubaOS 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-187337	–	**Symptom:** The WebUI allows access to pages which are inaccessible to administrators. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.4.12 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 6.5.4.12
AOS-190911 AOS-192857	–	**Symptom:** The **fw_visibility** process crashes in a 4-node cluster after an upgrade. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.4.8 or later versions. **Workaround:** None.	Firewall Visibility	All platforms	ArubaOS 6.5.4.8
AOS-190927 AOS-192132 AOS-216689	–	**Symptom:** A few controllers are unresponsive without console access. **Scenario:** This issue occurs due to memory leak in STM process. This issue is observed in controllers running ArubaOS 6.5.4.17 or later versions. **Workaround:** None.	Controller Platform	All platforms	ArubaOS 6.5.4.17
AOS-193751	–	**Symptom:** Some controllers do not display certificate information in the WebUI. **Scenario:** This issue occurs when the account type is read-only. This issue is observed in controllers running ArubaOS 6.5.4.8 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 6.5.4.8
AOS-194739	–	**Symptom:** A controller crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:20)**. **Scenario:** This issue is observed in 7280 controllers running ArubaOS 6.5.4.13 or later versions. **Workaround:** None.	Controller-Datapath	7280 controllers	ArubaOS 6.5.4.13

Table 4: *Known Issues in ArubaOS 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-194919 AOS-195565 AOS-205648 AOS-206010	–	**Symptom:** The **HTTPD** process in a controller crashes unexpectedly. The log files list the reason for the event as **Reboot Cause: User reboot (Intent:cause: 86:50)**. **Scenario:** This issue occurs when the controller is scanned for security vulnerabilities. This issue is observed in controllers running ArubaOS 6.5.4.0 or later versions. **Workaround:** None.	Web Server	All platforms	ArubaOS 6.5.4.0
AOS-198003	–	**Symptom:** Network firewall drops fragmented packets and hence, clients face connectivity issues. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.4.9 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 6.5.4.9
AOS-200084 AOS-204429	–	**Symptom:** A few APs crash and reboot unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: Rebooting the AP because of FW ASSERT**. **Scenario:** This issue was observed in AP-305 access points running ArubaOS 6.5.4.13 or later versions. **Workaround:** None.	AP-Wireless	AP-305 access points	ArubaOS 6.5.4.13
AOS-200762	–	**Symptom:** Disabling **Prohibit IP spoofing** in the firewall does not work as expected. This is because the ARP request frame is getting flooded as a broadcast instead of unicast. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.4.14 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 6.5.4.14
AOS-200993	–	**Symptom:** Active IP goes missing when a controller is reloaded after the next hop is configured with the IPsec map. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.4.16 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 6.5.4.16
AOS-203139	–	**Symptom:** The user table does not list the entire list of available users. **Scenario:** This issue occurs when BCMC optimization is enabled. This issue is observed in controllers running ArubaOS 6.5.4.13 or later versions. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 6.5.4.13

Table 4: *Known Issues in ArubaOS 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-212300	–	**Symptom:** The **show processes** command displays defunct entries. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.4.17 or later versions. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 6.5.4.17
AOS-196042 AOS-217995 AOS-221263	–	**Symptom:** The **show ucc dns-ip-learning** command displays **Unknown** for **Service Provider**. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.4.12 or later versions. **Workaround:** None.	UCC	All platforms	ArubaOS 6.5.4.12
AOS-219177	–	**Symptom:** Some controllers crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Soft Watchdog reset (Intent:cause:register de:86:70:2).** **Scenario:** This issue is observed in controllers running ArubaOS 6.5.4.18 or later versions. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 6.5.4.18

Upgrade Procedure

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

CAUTION

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

Topics in this chapter include:

Upgrade Caveats

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

- 120 Series access points, 600 Series, 3000 Series, M3, and 6000 controllers are not supported in ArubaOS 6.5.x. Do not upgrade to ArubaOS 6.5.x if your deployment contains a mix of these controllers in a master-local setup.
- If your controller is running ArubaOS 6.4.0.0 or later versions, do not use a Windows-based TFTP server to copy the ArubaOS image to the nonboot partition of the controller for upgrading or downgrading. Use FTP or SCP to copy the image.
- Starting from ArubaOS 6.4.x, you cannot 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 or alias
  - destination IP or alias
  - proto-port or 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 following ACL, both ACE entries could not be configured in ArubaOS 6.4.x. When the second ACE is added, it overwrites the first.

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

- When upgrading the software in a multi-controller network (one that uses two or more Aruba controllers), upgrade all the controllers in the proper sequence listed in Upgrading in a Multi-controller Network on page 29.

ArubaOS 6.5.0.0-FIPS Upgrade Failure

Customers upgrading from any FIPS version of ArubaOS prior to ArubaOS 6.5.0.0-FIPS to ArubaOS 6.5.0.0-FIPS or later version may experience symptoms that indicate an upgrade failure. Symptoms may include loss of configuration or administrative access to the controller, and/or hostname reset of the controller to default value.

This condition is caused by a change in the FIPS requirement for the strength of the hashing algorithm that is used to protect the configuration file from outside tampering. Starting from ArubaOS 6.5.0.0-FIPS, all versions of ArubaOS are changed to use stronger hashing algorithm to meet FIPS requirements. This change is known to create a challenge when upgrading or downgrading a controller between ArubaOS 6.4.0.0-FIPS version and ArubaOS 6.5.0.0-FIPS version. In some instances, the new stronger hash value may be missing or incorrect. This may disrupt controller reboot.

The most common scenario is:

1. When a controller running any version of ArubaOS 6.5.0.0-FIPS or later version is downgraded to any version of ArubaOS 6.4.0.0-FIPS or prior version
2. Controller is upgraded to ArubaOS 6.5.0.0- FIPS or later version.

To restore service, roll back to the previous ArubaOS version:

1. Connect an administrative terminal to the console port of the controller.
2. Reboot the controller.
3. On the administrative terminal, interrupt the boot process when prompted to enter the cpboot bootloader.
4. Execute the **osinfo** command to display the versions of ArubaOS hosted on partition 0 and partition 1.
5. Execute the **def_part 0** or **def_part 1** command depending on which partition hosts the ArubaOS 6.4.0.0-FIPS or later version.

6. Execute the **reset** or **bootf** to reboot the controller.

This restores the controller configuration and the previous ArubaOS version. Contact Aruba support for instructions to upgrade.

GRE Tunnel-Type Requirements

This section describes the important points to remember when configuring an L2 GRE tunnel:

- ArubaOS 6.5.4.22 continues to support L2 GRE tunnel type zero, but it is recommended to use a non-zero tunnel type.
- If both L2 and L3 tunnels are configured between endpoint devices, you must use a non-zero tunnel type for L2 GRE tunnels.

Important Points to Remember and Best Practices

To upgrade your controller:

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of the network by answering the following questions:
  - How many APs are assigned to each controller? Verify this information by navigating to the **Monitoring > NETWORK > All Access Points** page in the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the controller (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS runs on your controller?
  - Are all controller running the same version of ArubaOS?
  - What services are used on your controller (employee wireless, guest access, Remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load ArubaOS images to the controller. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If you encounter any issue during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path, if required.
- Before you upgrade to this version of ArubaOS, assess your software license requirements and load any new or expanded licenses that you might require. For a detailed description of these new license modules, refer to the “Software Licenses” chapter in the *ArubaOS 6.5.x User Guide*.

Memory Requirements

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

- Do not proceed with an upgrade unless 60 MB of free memory is available for an upgrade using the WebUI or execute the **show memory** command to confirm that there is at least 40 MB of free memory available for an upgrade using the CLI. To recover memory, reboot the controller. After the controller comes up, upgrade immediately.
- Do not proceed with an upgrade unless 75 MB of flash space is available for an upgrade using WebUI or execute the **show storage** command to confirm that there is at least 60 MB of flash space available for an upgrade using the CLI. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your the controller to a desired location. Delete the following files from the controller to free some memory:
  - **Crash Data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 27 to copy the **crash.tar** file to an external server, and then execute the **tar clean crash** command to delete the file from the controller.
  - **Flash Backups:** Use the procedures described in Backing up Critical Data on page 27 to back up the flash directory to a file named **flash.tar.gz.** Execute the **tar clean flash** command to delete the file from the controller.
  - **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 27 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the controller.

CAUTION

In certain situations, a reboot or a shutdown could cause the controller to lose the information stored in its flash memory. To avoid such issues, it is recommended that you execute the **halt** command before power cycling.

Backing up Critical Data

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

- Configuration data
- WMS database
- Local user database
- Licensing database
- Custom captive portal pages
- x.509 certificates
- Log files
- Flash backup

Backing up and Restoring Flash Memory

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

In the WebUI

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

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

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

In the CLI

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

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

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

   ```
   (host) # backup flash
   Please wait while we tar relevant files from flash...
   Please wait while we compress the tar file...
   Checking for free space on flash...
   Copying file to flash...
   File flashbackup.tar.gz created successfully on flash.
   ```
3. Execute either of the following command to transfer the flash backup file to an external server or storage device.

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

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

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

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

Upgrading in a Multi-controller Network

In a multi-controller network, upgrade the controller based on the controller type (master or local). Backup your controller before upgrading as described in Backing up Critical Data on page 27.

NOTE

All controllers in the network must be upgraded with the same version of ArubaOS software. Ensure that the controller model is the same for redundant environments such as VRRP.

To upgrade a multi-controller:

1. Load the ArubaOS image on all controllers (including redundant master controllers).
2. If all the controllers cannot be upgraded and rebooted simultaneously, use the following guidelines:
   a. Upgrade the software image on all the controllers.
   b. Reboot the master controller.
   c. After the master controller reboots, reboot the local controllers simultaneously.
   d. Ensure that the master and local controllers are upgraded to the ArubaOS version.

Installing ArubaOS 6.5.x-FIPS Version

Before you install ArubaOS-FIPS version on a controller that is currently running a non-FIPS version, perform the following steps:

CAUTION

If you are currently running a ArubaOS-FIPS version on the controller, do not execute the **write erase** command.

1. Download the ArubaOS-FIPS image from the customer support site.
2. Install the ArubaOS-FIPS image on the controller.
3. Execute the **write erase** command to reset the configuration to the factory default.
4. Reboot the controller by executing the **reload** command.

Upgrading ArubaOS

Upgrade ArubaOS using the WebUI and the CLI.

CAUTION

Ensure that there is enough free memory and flash space on your controller. For details, see Memory Requirements on page 27.

NOTE

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

In the WebUI

The following steps describe how to upgrade ArubaOS from one of these versions using local file:

- ArubaOS 3.4.4.1 or later
- ArubaOS 5.0.3.1 or later
- ArubaOS 6.0.1.0 or later

NOTE

When upgrading from an existing ArubaOS 6.4.x release, it is required to set AMON packet size manually to a desired value. However, the packet size is increased to 32K by default for fresh installations of ArubaOS 6.4.3.9.

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

NOTE

The ArubaOS image file is digitally signed, and is verified using RSA2048 certificates preloaded at the factory. The controller will not load a corrupted ArubaOS image.

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

NOTE

The upgrade will not take effect until reboot.

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

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

    The controller reboots automatically based on your selection in step 8.

Verifying the ArubaOS Upgrade

The following steps describe how to verify that the controller is functioning as expected.

1. Log in to the WebUI to verify all your controllers are up after the reboot.
2. Navigate to the **Monitoring > NETWORK > Network Summary** page to determine if your APs are up and ready to accept clients.
3. Verify that the number of APs and clients are what you would expect.
4. Verify that the number of access points and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 27 for information on creating a backup.

In the CLI

The following steps describe how to upgrade ArubaOS from one of these versions using the CLI:

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

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

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

   or

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

   or

   ```
   (host)# ping <scphost>
   ```
4. Execute the **show image version** command to check if the ArubaOS images is loaded on the flash partition. 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**.

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

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

   or

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

   or

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

   or

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

NOTE

The USB option is available on the 7000 Series and 7200 Seriescontrollers.

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

   ```
   (host)# reload
   ```

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

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

Verifying the ArubaOS Upgrade

The following steps describe how to verify that the controller is functioning as expected.

1. Log in to the CLI to verify that all your controllers are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
4. Test a different type of client in different locations, for each access method used.
5. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 27 for information on creating a backup.

Downgrading ArubaOS

A controller has two partitions, 0 and 1. If the upgrade fails on one of the partitions, you can reboot the controller from the other partition.

CAUTION

Database versions are not compatible between different ArubaOS releases.

CAUTION

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 6.5.4.22 to 5.0.3.2, changes made to WIPS in ArubaOS 6.x prevent the new predefined IDS profile assigned to an AP group from being recognized by the older version of ArubaOS. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error.
These new IDS profiles begin with *ids-transitional* while older IDS profiles do not include *transitional*. If you have encountered this issue, execute the **show profile-errors** and **show ap-group** commands to view the IDS profile associated with the AP group.

CAUTION

When reverting the controller software, use the previous version used on the controller.

Prerequisites

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

1. Back up your controller. For details, see Backing up Critical Data on page 27.
2. Verify that the control plane security is disabled.
3. Set the controller to boot with the previously saved configuration file.
4. Set the controller to boot from the system partition that contains the pre-upgrade ArubaOS version.

   When you specify a boot partition or copy an image file to a system partition, controller checks if the ArubaOS version is compatible with the configuration file. An error message is displayed if the boot parameters are incompatible with the ArubaOS version and configuration files.
5. After switching the boot partition, perform the following steps:
   - Restore the pre-upgrade flash backup from the file stored on the controller. Do not restore the ArubaOS flash backup file.
   - Do not import the WMS database.
   - If the RF plan is unchanged, do not import it. If the RF plan was changed before switching the boot partition, the changed RF plan does not appear in the downgraded ArubaOS version.
   - If any new certificates were added in the upgraded ArubaOS version, reinstall these certificates in the downgraded ArubaOS version.

Downgrade ArubaOS version using the WebUI or CLI.

In the WebUI

The following steps describe how to downgrade the ArubaOS version.

1. If the saved pre-upgrade configuration file is on an external FTP or TFTP server, copy the file to the controller by navigating to the **Maintenance > File > Copy Files** page.
   a. For **Source Selection**, select FTP or TFTP server, and enter the IP address of the FTP or TFTP server and the name of the pre-upgrade configuration file.

   b. For **Destination Selection**, enter a file name (other than default.cfg) for Flash File System.

2. Set the controller to boot with your pre-upgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the saved pre-upgrade configuration file from the **Configuration File** drop-down list.
   b. Click **Apply**.
3. Determine the partition on which the previous ArubaOS image is stored by navigating to the **Maintenance > Controller > Image Management** page. If there is no previous ArubaOS image stored on the system partition, load it to the backup system partition by performing the following steps:

CAUTION

You cannot load a new image into the active system partition.

   a. Enter the FTP or TFTP server address and image file name.
   b. Select the backup system partition.
   c. 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 and click **Continue**.

   The controller reboots after the countdown period.
6. After the controller reboots, log in to the WebUI and navigating to the **Maintenance > Controller > Image Management** page to verify the ArubaOS version.

In the CLI

The following steps describe how to downgrade the ArubaOS version:

1. If the saved pre-upgrade configuration file is on an external FTP or TFTP server, use the following command to copy it to the 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 pre-upgrade ArubaOS version is stored.

CAUTION

You cannot load a new image into the active system partition.

```
#show image version
```

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

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

5. Reboot the controller.

```
(host) # reload
```

6. When the boot process is complete, verify that the controller is using the correct ArubaOS version.

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

Before You Call Technical Support

Provide the following information when you call the Technical Support:

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