AOS-10.4.1.8

Release Notes

Open Source Code

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components 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, please check if the code is available in the HPE Software Center at https://myenterpriselicense.hpe.com/cwp-ui/software but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd, Spring, TX 77389
United States of America

Contents

Chapter 1
Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

Chapter 2
Release Overview

This AOS-10.4.1.8 release notes includes the following topics:

- What's New
- Supported Hardware Platforms
- Resolved Issues
- Known Issues and Limitations

For the list of terms, refer Glossary.

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

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworking.hpe.com
Support Site	https://networkingsupport.hpe.com/home
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (US & Canada Toll-Free Number) +1-650-750-0350 (Backup—Toll Number)
International Telephone	www.hpe.com/psnow/doc/a50011948enw
Software Licensing Site	licensemanagement.hpe.com
End-of-life Information	networkingsupport.hpe.com/end-of-life
Security Incident Response Team	Site: support.hpe.com/connect/s/securitybulletinlibrary Email: networking-sirt@hpe.com

Chapter 3
What's New

This chapter describes the new features and enhancements introduced in AOS-10.4.1.8. For more information, see *Aruba Central Help Center*.

New Features

The following feature is introduced in this release:

Dot11r Failure Logs

The **show ap debug dot11r-failure** command is introduced to display debugging information about dot11r failure.

Enhancements

There are no new enhancements introduced in this release.

Supported Hardware Platforms

See Supported Devices in AOS-10.4 for a list of HPE Aruba Networking AP and gateway models supported in AOS-10.4.

Chapter 4
Resolved Issues

This chapter describes the resolved issues in this release.

Table 3: *Resolved Issues in AOS-10.4.1.8*

Bug ID	Description	Reported Version
AOS-234532	Some APs triggered multiple alerts stating **Radio frames retry percent for AP has been above 90% for about 15 minutes**, under the **Analyze** > **Alerts & Events** > **Critical** > **OPEN ALERTS** section of HPE Aruba Networking Central. The issue was related to a miscalculation in the Radio Frames Retry Percent process, due to a miscount of the Tx MPDU values. The issue was observed in APs running AOS-10.4.1.0 or later versions. The fix includes an enhancement to the total Tx MPDU transmitted counter, resolving the issue and eliminating the alerts.	AOS-10.4.1.0
AOS-237720	Some modem configuration commands, including frequency bands, PLMN, and network mode, worked for all modems. This issue occurred because some Uplink commands specific to 9004-LTE and Skylark modems were also enabled on other switches and modems. The fix ensures modem configuration commands work only for Skylark and 9004-LTE modems.	AOS-10.4.1.0
AOS-239411	When console access was used to reset the access points, the device serial number served as the default password after the reset. However, intermittently the device accepted **admin** as the password, instead of the serial number. The fix ensures that the device serial number is set as the default password.	AOS-10.4.1.0
AOS-244321 AOS-244371	Some RADIUS server users were unable to connect to Passpoint due to exhausted reqIDs error. This issue occurred in gateways running AOS-10.4.1.0 or later version. The fix introduces enhanced logic to clean up and reconnect sockets during failures and mark reqIDs as free.	AOS-10.4.1.0
AOS-246103	Some AP-635 and AP-535 access points reboot randomly with reboot reason, **kernel panic: Take care of the TARGET ASSERT at ar_wal_tx_send.c:11778 first**. This issue is observed on APs running AOS-10.4.0.2. A few AP-635 and AP-535 access points running on AOS-10.4.0.2 rebooted randomly. The log files listed the reason for the reboot as **kernel panic: Take care of the TARGET ASSERT at ar_wal_tx_send.c:11778 first**. The fix ensures that the APs do not crash.	AOS-10.4.0.2
AOS-247318	STM process crashed unexpectedly while running the **show ap debug radius-statistics** command. This issue occurred due to a parameter mismatch while running the command. This issue was observed in APs running AOS10.4.1.0 or later versions.	AOS10.4.1.0

Bug ID	Description	Reported Version
	The fix ensures that the STM process does not crash and works seamlessly.	
AOS-248282	Some 7010 gateways running PVST+ (Per VLAN Spanning Tree protocol) experienced issues on peer switches, which blocked the port for 15 seconds due to inconsistent local VLAN configurations. The removal of VLANs led to the incorrect transmission of PVST+ BPDUs with both PVID and 802.1Q VLAN ID set to **0**. A check was added to avoid transmission of BPDUs with PVID equal to **0**.	AOS-10.4.1.0
AOS-249262	Some AP-535 access points running on AOS-10.4.1.0 rebooted randomly. The log files listed the reason for the reboot as **kernel panic: Take care of the TARGET ASSERT first - wlan_wmi.c:653**. The fix ensures that the APs work as expected.	AOS-10.4.1.0
AOS-250117	The **VOIP and PS aware scan rejects** counter was not incrementing on 2.4GHz, 5GHz, and 6GHz radio frequencies. This issue was observed in some AP-654 access points running AOS-10.4.0.3 or later versions. The fix ensures that the **VOIP and PS aware scan rejects** counter increments correctly.	AOS-10.4.0.3
AOS-251602 AOS-255118 AOS-257207 AOS-260667 AOS-264562	The CTB Agent module crashed on 7240XM gateways running AOS-10.4.1.0 and rebooted unexpectedly. This issue occurred due to kernel panic. The issue was resolved by handling the buffer issue.	AOS-10.4.1.0
AOS-252313 AOS-263688	Some 7210 Branch Gateways running AOS-10.4.1.1 or later versions crashed and rebooted unexpectedly. The log files listed the reason as, **Reboot Cause: Nanny rebooted machine - isakmpd process died (Intent:cause:register 34:86:50:2)**. The fix ensures that the gateways work as expected.	AOS-10.4.1.1
AOS-252793	When traffic statistics were captured with monitoring systems, the **aiClientTxDataBytes** and **aiClientRxDataBytes** MIB nodes counters were reset to **0**, after the 32-bit limit was reached. This issue was observed in APs running AOS-10.7.1.0 or later versions. The fix ensures that the statistics display as expected.	AOS-10.7.1.0
AOS-253050	The temperature threshold values of low, medium, and high are reported incorrectly as **255** in the **AMON—HWMON_SENSOR_THRS**. This issue is observed in HPE Aruba Networking 9106, 9114, and 9240 gateways running AOS-10.6.0.0. The fix ensures that the temperature threshold values are reported correctly.	AOS-10.6.0.0
AOS-253435	In some AP-315 and AP-375 access points, clients were able to access torrent sites and other applications despite having ACL entries configured to block such traffic. This issue was observed in access points running AOS-10.7.1.0 or later versions. The fix ensures that the access points block unwanted traffic.	AOS-10.7.1.0
AOS-254679 AOS-263383	The wired traffic client dropped and failed to obtain an IP from the gateway. The client's DHCP traffic dropped on the AP and was not forwarded to the ATA tunnel endpoints.	AOS-10.4.1.4

Bug ID	Description	Reported Version
	The fix ensures that DHCP traffic is forwarded through the tunnel, allowing clients to obtain IP addresses as expected.	
AOS-255909	Some APs crashed and rebooted with reason, **AP rebooted caused by internal watchdog reset**. This error was related to the driver image on the device. This issue was observed in AP-535 and AP-655 access points running AOS-10.7.0.1 or later versions. The fix ensures that the APs function as expected.	AOS-10.7.0.1
AOS-260853	Some 7240XM gateways running AOS-10-10.4.1.5 or later versions displayed stale station table entries for disconnected clients in HPE Aruba Networking Central. This issue occurs when a custom logon role was assigned to clients, which prevented the automatic removal of disconnected client entries from the station table. As a result, stale entries accumulated over time and displayed the incorrect client count. The fix ensures that the stale station table entries and incorrect client count are not displayed.	AOS-10.4.1.5
AOS-261707 AOS-257551	Clients failed to connect to the Netskope server when the LTE uplink was directly plugged into the AP-605R access point, either using a USB with Skylark or a direct LTE modem. This issue was observed on APs running AOS-10.6.0.3 or later versions. The fix ensures that clients can connect to the Netskope server using the LTE uplink.	AOS-10.6.0.3
AOS-257568 AOS-264539	Some APs running on AOS-10.7.0.2 rebooted randomly. The log files listed the reason for the reboot as **InternalError: 96000210 [#1] SMP PC: phy_utils_write_phyreg_nopi+0x70**. The fix ensures that the APs work as expected.	AOS-10.7.0.2
AOS-257808	The usage of per-user contract was wrongly displayed as almost maximum for the 7240XM gateway. This issue was seen even though the user count was less than 7000 and clients were assigned to user role with bandwidth contract. It occurred because of the leak and the update failure of bandwidth contract limit. The fix ensures that per-user bandwidth usage is accurately displayed for 7240XM.	AOS-10.4.1.0
AOS-258275 AOS-260095	While generating aggregated client sessions, blocked sessions were generated even though the user did not set any ACL (Access Control List) under **Devices** > **Access Points** > **Security**. The fix ensures that blocked sessions are not generated if ACL is not set.	AOS-10.4.1.0
AOS-258335	When the **WebCC cache-miss-drop** feature was enabled, a few 9004 gateways running AOS-10.6.0.3 or higher experienced slow browsing. The fix ensures that the browsing time is reduced.	AOS-10.6.0.3
AOS-258781	A few AP-615 access points running AOS-10.5.1.0 suppressed their default route, that impacted L3 connectivity of the AP's management VLAN. This issue occurred when the APs were assigned a static IP, and dot1x authentication of the AP occurred. The fix ensures that the default route is not suppressed.	AOS-10.5.1.0

Bug ID	Description	Reported Version
AOS-259202	Users were unable to establish PPTP connection as gateways were dropping PPTP packets. This issue was observed in 9004 gateways running AOS-10.4.1.3 or later versions. The fix ensures that the gateways work as expected.	AOS-10.4.1.3
AOS-259241	HPE Aruba Networking Central connection and OAP channel incorrectly showed connectivity issues even when the gateway had an active LTE uplink. This issue was observed in gateways running AOS-10.5.1.1 or later versions. The issue was resolved by showing correct connectivity information in HPE Aruba Networking Central.	AOS 10.5.1.1
AOS-259606	Some clients connected to a 6GHZ SSID with security mode set to **enhanced-open**, faced low throughput due to problems with Block Acknowledgment. This issue was observed in APs running in AOS-10.4.1.0 or later versions. The fix ensures that clients get the expected throughput in this scenario.	AOS-10.4.1.0
AOS-259665	While roaming, Intel AX211 clients frequently disconnected and sent multiple deauthentication frames. The fix is to ensure that the AP sends beacons in a timely manner. This issue was observed in AP-615 access points running AOS-10.4.1.0 or later versions.	AOS-10.4.1.0
AOS-259868	A few AP-635 access points running on AOS-10.7.0.0 rebooted unexpectedly due to kernel panic. The log files listed the reason for reboot as, **Rebooting the AP. NSS FW crashed**. The issue occurred because of the duplicated cookie used in rx descriptors. The fix ensures that the access points work as expected.	AOS-10.7.0.0
AOS-260140	In HPE Aruba Networking Central, the free station count **CL_ CLUSTER_FREE_STA_COUNT** in **CLUSTER_SELF_NODE_STATS AMON** displayed an incorrect value. This issue occurred because the total station count was calculated twice the actual capacity of the gateway platform. The fix ensures that the free station count displays the correct value.	AOS-10.6.0.0
AOS-260367	AP-635 access points running AOS-10.6.0.2 crashed repeatedly. This issue occurred due to corruption in the **/etc/dnsmasq.conf** configuration file. The fix ensures that APs do not crash, and work as expected.	AOS-10.6.0.2
AOS-260423	Some access points crashed unexpectedly due to memory spikes under heavy traffic. The log files listed the reason for the crash as _ **_efistub_memcpy+0x48/0x180**. This issue was observed in APs runningAOS-10.4.1.0 or later versions. The fix ensures APs will not encounter any memory issues.	AOS-10.4.1.0
AOS-260590	Data loss was observed in gateways and Zscaler tunnels when WAN redundancy was enabled. The fix ensures that gateways work as expected. This issue was observed in gateways running AOS-10.4.1.0 or later versions.	AOS-10.4.1.0

Bug ID	Description	Reported Version
AOS-260790	Some issues were seen in the RF Health report. This occurred because the average error value in the health report was greater than 100%. This issue was observed in AP-655 access points running AOS-10.4.1.0 or later versions. The fix ensures that the issues are resolved.	AOS-10.4.1.0
AOS-261263	Some gateways randomly dropped DNS queries initiated by iPad clients when the SaaS Express application skype_teams was enabled, and iPad users accessed teams.microsoft.com through the browser. Despite stable connections, the gateway intermittently failed to process these DNS queries, impacting the iPad user's ability to access Microsoft Teams. This issue was observed in HPE Aruba Networking 9004 gateways running AOS-10.4.0.2. The fix ensures that iPad users are able to access Microsoft Teams when connected on 9004 gateways.	AOS-10.4.0.2
AOS-261412	While enabling Branch Mesh between gateways, OTO was using STUN-learnt addresses/ports for MPLS circuits. Hence, some of the tunnel definitions received from OTO were pointing to the public IP address of the MPLS, which is the same for all sites, rather than the physical IP address of the destination gateway. The fix ensures that OTO sends the correct IP address of the destination gateway.	AOS-10.4.1.1
AOS-261347	The UCM process crashed on some APs in a customer deployment of mixed-type APs such as AP-518, AP-555, and AP-514 running version 10.4.1.6. The issue occurred due to memory corruption that scaled across various parts of the UCM. The fix ensures that the UCM process does not crash.	AOS-10.4.1.6
AOS-261440	The ANI feature was disabled for some AP-535 access points running AOS-10.4.1.0 or later versions. This issue occurred due to consistently high PHY error rates disabling ANI. The fix ensures that the ANI feature works as expected.	AOS-10.4.1.0
AOS-261536	A DHCP outage was reported on tunnel mode SSIDs in the network. This issue occurred because wireless clients failed to receive a DHCP address from the DHCP servers connected to the Branch Gateway running AOS-10.7.0.1 or later versions. The fix ensures that DHCP allocation works as expected for wireless clients.	AOS-10.7.0.1
AOS-261601	The **show arp** command did not display any output for some 9004-LTE gateways. This issue was observed on 9004-LTE gateways running AOS-10.7.1.0 or later versions. The fix ensures that the **show arp** command valid output.	AOS-10.4.1.0
AOS-261610 AOS-262298	The wired clients connected to a Microbranch AP remained in a state of authentication loop. This issue occurred because the VPNC marked the client MAC address as aged out due to not receiving the accounting start. The fix ensures that the wired clients are authenticated successfully.	AOS-10.4.1.5

Bug ID	Description	Reported Version
AOS-261731	The AirGroup server cache on the APs retained the previous IPv4 address even after the server was reconnected with a new IP address. This issue was observed in the AOS-10 setup with access points running AOS-10.4.0.0 or later versions. The fix ensures that the AirGroup records always reflect the latest IPv4 address.	AOS-10.4.0.0
AOS-258682	A few APs crashed and rebooted unexpectedly. The log files listed the reason as **kernel panic: Fatal exception in interrupt**. This issue was observed in AP-635 access points running AOS 10.4.1.0 or later versions. The fix ensures the APs work as expected. **Duplicates**: AOS-261973, AOS-261978, AOS-262382, AOS-262498, AOS-264108, AOS-265054, and AOS-265158.	AOS-10.4.1.0
AOS-262274	A few APs displayed the status of eth0 interface as **DOWN** in the SNMP server. This issue was observed in APs running AOS 10.4.1.0 or later versions. The fix ensures the APs work as expected.	AOS-10.4.1.0
AOS-262522	The connection to RadSec failed intermittently for gateways running AOS-10.4.1.5. This issue occurred because the cert-download process did not fetch the device certificate from HPE Aruba Networking Central. The resolution adds a mechanism to periodically check and download the certificates that are not present in the gateway.	AOS-10.4.1.5
AOS-262759	Some AP-515 access points sporadically sent packets out of sequence, causing the Wi-Fi adapter to stop passing traffic and disconnect. The issue occurred because the packet stayed in the suppressed queue for too long. This issue was observed in APs running AOS-10.4.1.5 or later versions. The fix ensures that the APs work as expected and the Wi-Fi adapter is not interrupted.	AOS-10.4.1.5
AOS-262784	Some gateways unexpectedly crashed and were unable to execute commands because of large temporary files generated by repetitive USB logs. This issue was observed in 9004 gateways running AOS-10.4.1.0 or later versions. The fix ensures that unnecessary USB logs are not created when a USB flash drive is inserted and removed from the gateway.	AOS-10.4.1.0
AOS-262804	Some 9004 gateways using non-HPE Aruba Networking USB modems went offline randomly in HPE Aruba Networking Central. This issue occurred when the software version was upgraded from AOS-8.7.0.0-2.3.0.7 to 10.4.1.3 or later. The fix ensures that the 9004 gateways work as expected.	AOS-10.4.1.3
AOS-263154	When branch gateways at different sites communicate over a VPNC, packets over 1473 bytes experience intermittent packet loss. This issue is observed in branch gateways running AOS-10.4.1.1 or later versions. The fix ensures that the gateways works as expected.	AOS-10.4.1.1
AOS-263312	User role was not working when **Destination NAT** was configured using a **FQDN**. However, it worked correctly when **Destination NAT** was configured with an **IP Address**.	AOS-10.4.1.3

Bug ID	Description	Reported Version
	The fix ensures that the user role function as expected.	
AOS-263362	When the user tried to deploy new sites, access to a specific resource from the data center via FTP was blocked. This issue was caused by the policy rule **all_local_networks**, which blocks the FTP control connection. This issue was observed in branch gateways running AOS-10.4.1.4. The fix ensures that traffic for FTP server is allowed.	AOS-10.4.1.4
AOS-263390	A few AP-535 access points running AOS-10.4.1.0 crashed and rebooted unexpectedly. The log file listed the reason for the event as, **kernel panic: Rebooting the AP. NSS FW crashed**. The fix ensures that the APs function as expected.	AOS-10.4.1.0
AOS-263472	The AP-575 access point running AOS-10.4.1.0 crashed and rebooted unexpectedly. The log file listed the reason for the event as, **BadPtr: 00000028 PC: anul_intf_init+0xb8/0x2b8 [anul] Warm-reset**. The fix ensures that the AP functions as expected.	AOS-10.4.1.0
AOS-263557	HPE Aruba Networking 9240 VPNCs running AOS-10.4.1.1 experienced continuous crashes and reboots. This issue occurred due to the **isakmpd** process dying, causing the Nanny process to reboot. The issue occurred because QAT (QuickAssist Technology) responses were delayed for different requests, leading to crashes when the system attempted to process responses using incorrect context data. The fix includes validation checks to ensure that responses from QAT match the requests made, thereby preventing crashes due to context mismatches.	AOS-10.4.1.1
AOS-263693 AOS-265106 AOS-265353	Some AP-515 access points crashed and rebooted unexpectedly with reason, **PC is at aruba_low_txq_flush_to_psq+0xc4/0x278 [wl_v6]**. This issue was observed in AP-515 access points running AOS-10.4.1.7. The fix ensures that APs work as expected.	AOS-10.4.1.7
AOS-264675	Some AP-655 access points running AOS-10.4.1.7 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as, **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the APs work as expected.	AOS-10.4.1.7
AOS-264612	Some clients showed them as connected to the gateway, though they were connected directly to a switch. This issue was observed in gateways running AOS-10.4.1.4 or later versions. The fix ensures that the clients show accurate connection status.	AOS-10.4.1.4

Chapter 5
Known Issues and Limitations

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

Limitations

Following are the limitations observed in this release:

APs Unable to Receive BBS Configuration Without IoT Connector

All APs running AOS-10.4.1 versions start BLE processes only if a transport profile is configured. As a result, if a customer is only using BLE Beacon Service (BBS) profiles, these profiles will not get pushed to APs.

Workaround

Assign APs running AOS-10.4.1 versions to a VM-based IoT Connector. This initiates a transport profile and allows for BBS profiles to flow to the APs.

Packet Trace Failure Observed

Packet trace functionality fails for PAPI ports despite being enabled. No packets are observed in the trace buffer when PAPI is used.

VAP Limitation on Access Point Platforms

When performing configuration changes on one VAP, clients associated to other non-modified VAPs may lose connectivity.

This issue is observed in the following AP models running AOS-10.3.1.0 or later versions—340 Series (344/345), 500 Series (503/504/505), 500H Series (503H/505H), 500R Series (503R), 510 Series (514/515/518), 560 Series (565/567), 560EX Series (565EX/567EX), 570 Series (574/575/577), 570EX Series (575EX/577EX), 600H Series (605H), 600R Series (605R), 610 Series (615) and all Wi-Fi 7 access point models.

For more information, contact support and make reference to bug ID AOS-131599.

Known Issues

Following are the known issues observed in this release.

Table 4: *Known Issues in AOS-10.4.1.8*

Bug ID	Description	Reported Version
AOS-195769	In some APs with dynamic VLAN assignment, ARP or GARP traffic is unexpectedly sent to wireless clients, even if they are connected to a different VLAN and VAP. This issue is observed in the following scenarios: ■ When the broadcast packets from VLAN 1 and all of the	AOS-10.4.1.0

Bug ID	Description	Reported Version
	clients on the SSID are on VLAN 2, the packets are sent to all VAPs belonging to the same SSID. ■ When the SSID has two VAPs that belong to the same VLAN, but only one VAP has clients on that VLAN, the traffic is forwarded to both VAPs. ■ When all of the VAPs of a given SSID have clients on different VLANs, the packets are broadcasted to all VLANs.	
AOS-231129	Sometimes 600 Series APs do not send the cold and warm SNMP traps when rebooted.	AOS-10.4.1.0
AOS-232875	The **mon_serv** process crashes in specific high-load situations, especially when there are numerous APs and users with high roaming rates. This issue is observed in gateways running AOS-10.4.1.0 or later versions.	AOS-10.4.1.0
AOS-233988 AOS-263521	Wired clients are unable to ping each other on the same VLAN when the ACL is set to **user any any permit** policy. This issue occurs because SIP is used as the user for both forward and reverse session creation during session ACL lookup.	AOS-10.3.1.0
AOS-236889	When the user runs commands starting with **show user** from the API, the output displayed is empty. This issue is observed on 7240XM gateways.	AOS-10.4.1.0
AOS-238799	Clients experience connectivity issues when attempting to connect to an SSID using native VLAN. This issue occurs when LACP is configured with an uplink switch on the AP.	AOS-10.4.1.0
AOS-236177 AOS-240026 AOS-240633 AOS-240068 AOS-247688 AOS-247786	A few customers are unable to access gateways through the CLI or WebUI. This issue is related to third-party monitoring tools such as Armis, which keep the CLI sessions open for a long time, accumulating memory leaks that affect the functioning of the gateways.	AOS-10.4.1.0
AOS-240185	Clients are unable to obtain user roles from ClearPass Policy Manager and fall into their initial role. This issue occurs due to radius accounting.	AOS-10.4.0.0
AOS-241233	Some APs do not capture AP response packets even when Live Events Capture is enabled. This issue occurs because of a mismatch in the captured data frame header structure.	AOS-10.4.0.0
AOS-241316	The output of the **show ap debug lldp** command displays incorrect information when executed.	AOS-10.4.1.0
AOS-242271	In HPE Aruba Networking Central, multiple DHCP server connection errors are observed on the **AI Insights** dashboard for multiple sites. This issue is observed in Mesh scenarios with APs running AOS-10.5 or lower versions.	AOS-10.5.0.0
AOS-243414	When DNS server details are updated, AP receives the updates but does not send the updated DNS server details to HPE Aruba Networking Central.	AOS-10.4.1.0

Bug ID	Description	Reported Version
AOS-245191	A few gateways are unable to establish an SSH connection to the devices due to login sessions not timing out. This issue is observed in devices running on AOS-10.4.1.0 or later versions.	AOS-10.4.1.0
AOS-246232	Users are unable to upgrade 7008 gateways from HPE Aruba Networking Central. The **Audit Trail** displays two error messages: ■ Upgrade: failed File copied successfully and Saving files to Flash ■ Error upgrading the image: Basic image verification This issue is observed on 7008 gateways running AOS-10.4.0.2.	AOS-10.4.0.1
AOS-248392	While deploying an AOS-10 cluster for a site, 9004-LTE gateways crash and reboot with datapath timeout when downgraded to AOS-10.4.0.3.	AOS-10.4.0.3
AOS-260853	Some 7240XM gateways running AOS-10-10.4.1.5 or later versions display stale station table entries for disconnected clients in HPE Aruba Networking Central. This issue occurs when a custom logon role is assigned to clients, which prevents the automatic removal of disconnected client entries from the station table. As a result, stale entries accumulate over time and display the incorrect client count.	AOS-10.4.1.5
AOS-260893	The One Touch Provision (OTP) screens for both static-activate and full-setup in AOS-10 gateways display IPv6 configuration options, even though IPv6 support is not yet available in AOS-10. **Workaround**: Select **No** when prompted with the option to configure IPv6 address.	AOS-10.4.0.0
AOS-263158	Some users are unable to access certain external sites, even when no ACLs are blocking the traffic. This issue occurs due to the IP reputation filtering feature. This issue is observed in branch gateways running AOS-10.4.1.4 or later versions.	AOS-10.4.1.4
AOS-264431	Users are unable to establish SSH or remote console access to APs from HPE Aruba Networking Central. This issue occurs when the default **terminal-access** configuration is missing from the AP's running configuration. Hence, when HPE Aruba Networking Central initiates SSH or remote console sessions, the AP rejects the connection, leading to inconsistent behavior. This issue is observed in APs running AOS-10.4.1.0 or later versions. **Workaround**: Manually verify and enable the **terminal-access** configuration on the AP.	AOS-10.4.1.0

Upgrading to AOS-10

This section describes the procedure to upgrade AOS-10 devices.

This section only applies to devices that are running AOS-10. If your device is running AOS-8, you will have to first migrate to AOS-10 either manually or as part of the Aruba Central Firmware Compliance Policy, before attempting an upgrade. For more information on migrating to AOS-10, see Migrating APs to AOS-10.

This chapter includes the following topics:

Important Points to Remember

To upgrade your gateway or AP:

- 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. These steps are not required if the upgrade type is a live 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 gateways and APs are present in the group you are upgrading?

    To view the number of devices in each group, complete the following steps in HPE Aruba Networking Central:

    1. In the HPE Aruba Networking Central app, set the filter to an AP group.
    2. Under **Manage**, click **Devices**.

       By default, the **Access Points** device page is displayed.
  - What version of AOS runs on your gateways or APs?
  - Ensure all the devices are assigned a license such as foundation or advanced. If the upgrade type is live upgrade, ensure all the APs are assigned with an advanced license. For more information, see Overview of HPE Aruba Networking Central Foundation and Advanced Licenses.
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- Ensure the devices are reachable to public networks and the uplinks have sufficient bandwidth to download the image from the Aruba Activate Server.
- Multiversion is supported within the gateway cluster. The gateways and the APs can be in different AOS versions. For more information, see Mixing AOS-10 Software Versions.

RAM and FLASH Storage Requirements

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

- Ensure sufficient RAM and flash space is available on the gateway/controller/MD/BGW before proceeding with the upgrade.
- Execute the **show memory** command to identify the available free RAM.
- Execute the **show storage** command to identify the available flash space.
- If the output of the **show storage** command indicates that there is insufficient flash RAM, free some used memory. Copy any log files, crash data, or flash backups from your gateways to a desired location. Delete the following files from the gateway/controller/MD/BGW to free FLASH storage:
  - **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 to copy the **crash.tar** file to an external server. Execute the **tar clean crash** command to delete the file from the gateway/controller/MD/BGW.
  - **Flash backups:** Use the procedures described in Backing up Critical Data to back up the flash directory to a file named **flashbackup.tar.gz**. Execute the **tar clean flash** command to delete the file from the gateway/controller/MD/BGW.
  - **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 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the gateway/controller/MD/BGW.
- The show commands are available under **Analyze** > **Tool** > **Commands** section of HPE Aruba Networking Central.

If available RAM is not suffiicient to meet the requirements stated in the appropriate release notes, it may be necessary to reboot the device and then immediately upgrade, or disable some functionality. Please consult HPE Aruba Networking technical support for guidance.

The device CLI can be accessed from HPE Aruba Networking Central. Select the device, **Overview** > **Summary** > **Actions** > **Console**.

Deleting a File

You can delete a file using the following command:

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

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 CLI.

The device CLI can be accessed from HPE Aruba Networking Central. Select the device, **Overview** > **Summary** > **Actions** > **Console**.

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

1. 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 take the flash backup.......
   File flashbackup.tar.gz created successfully on flash.
   Please copy it out of the controller and delete it when done.
   ```
2. Execute either of the following commands to transfer the flash backup file to an external server or storage device.
   ```
   (host) #copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpuser> <remote-directory>
   <destinationfilename> <ftpuserpassword>

   (host) #copy flash: flashbackup.tar.gz usb: partition <partition-number>
   <destinationfilename>
   ```
   You can transfer the flash backup file from the external server or storage device to the flash memory by executing either of the following commands:
   ```
   (host) #copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz

   (host) #copy usb: partition <partition-number> <filename> flash:
   flashbackup.tar.gz
   ```
3. Execute the following command to untar and extract the **flashbackup.tar.gz** file to the flash memory.
   ```
   (host) #restore flash
   Please wait while we restore the flash backup........
   Flash restored successfully.
   Please reload (reboot) the controller for the new files to take effect.
   ```

Upgrading a Single Device or Multiple Devices

To upgrade a single device or multiple devices, complete the following steps:

1. In the HPE Aruba Networking Central app, select one of the following options:
   a. To select a group, site or global in the filter:
      - Set the filter to one of the options under **Group** or **Sites**. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
      - Under **Maintain**, click **Firmware**.
      - Select one or more devices from the device list and click the **Upgrade** icon at the bottom of the page or hover over one of the selected device and click the **Upgrade** icon. The **Upgrade <Device> Firmware** pop-up window opens.

b. To select a device in the filter:
   - Set the filter to **Global**.
   - Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Gateways**. A list of devices is displayed.
   - Click a device listed under **Device Name**. The dashboard context for the device is displayed.
   - Under **Maintain**, click **Firmware** and click **Upgrade** in the **Firmware Details** window. The **Upgrade <Device> Firmware** pop-up window opens.

2. In the **Upgrade <Device> Firmware** pop-up window, select the desired firmware version.
   You can either select a recommended version or manually choose a specific firmware version.

- To obtain custom build details, contact HPE Aruba Networking Technical Support.
- The recommended firmware versions can be different for different devices and depends on the device model and software architecture.

3. Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time:
   - **Now**—Allows you to set the compliance to be carried out immediately.
   - **Later Date**—Allows you to set the compliance to be carried out at the later date and time. Select a specific time zone from the **Select Zone** drop-down options to schedule the firmware compliance in a specific time zone.

Steps 4 and 5 are applicable only if you are upgrading HPE Aruba Networking Switches, Aruba CX Switches, and Branch Gateways. If you are upgrading an Access Point, proceed to step 6.

4. From the **Install On** drop-down, select any one of the following partition options:
   - **Primary partition**—Select this if you want to install the firmware version in the primary partition.
   - **Secondary partition**— Select this if you want to install the firmware version in the secondary partition.
5. Select the check box if you want HPE Aruba Networking Central to automatically reboot after device upgrade.
6. Click **Upgrade**. The device downloads the image from the server, saves it to flash, and reboots.
   Depending on the progress and success of the upgrade, one of the following messages is displayed:
   - **Upgrading**—While image upgrade is in progress.
   - **Upgrade failed**—When the upgrade fails.
7. If the upgrade fails, retry upgrading your device.

After upgrading a switch, click **Reboot**.

Important Points When Upgrading Gateway Devices

When you upgrade a gateway device from any AOS-8 version to an AOS-10 version, it is recommended to do **write erase all**, and then upgrade the image. Most of the AOS-8 command and license mechanism is not supported in AOS-10.

When you downgrade a branch gateway or VPNC or Mobility gateway from AOS-10 to AOS-8, it is recommended to do **write erase all**, and then downgrade the image. In AOS-10, license (capacity) and other configurations are not supported in AOS-8.

Upgrading Devices using Upgrade All Option

To upgrade multiple devices using the **Upgrade All** option, complete the following steps:

1. In the HPE Aruba Networking Central app, set the filter to one of the options under **Group** or **Sites**.

   For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
2. Under **Maintain**, click **Firmware**.
   The firmware dashboard for Access Points is displayed by default.
3. Click **Upgrade All**.

   The **Upgrade <Device> Firmware** pop-up window opens.
4. In the **Upgrade <Device> Firmware** pop-up window, select the specific site or multiple sites from the **Sites** drop-down list.

   This option is available only at the global context.
5. Select the desired firmware version (for Access points and Gateways) and AOS-S firmware version and CX firmware version (for HPE Aruba Networking Switches and Aruba CX Switches) from their respective drop-down list.

   You can either select a recommended version or manually choose a specific firmware version.

- To obtain custom build details, contact HPE Aruba Networking Technical Support.
- The recommended firmware versions can be different for different devices and depends on the device model and software architecture.

6. In the **Upgrade Type**, select one of the following options:
   - **Standard**
   - **Live**

- Live upgrade is only supported for APs and gateways in cluster mode. For more information, see Live Upgrades.

- Live upgrade operation requires the devices to be assigned with Advanced license. On the group dashboard, live upgrade is not initiated for the group if any of the device within the group is assigned with Foundation license. HPE Aruba Networking Central recommends that you create a group with devices that are assigned with Advanced license for seamless operation.

7. Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time:
   - **Now**—Allows you to set the compliance to be carried out immediately.
   - **Later Date**—Allows you to set the compliance to be carried out at the later date and time. Select a specific time zone from the **Select Zone** drop-down options to schedule the firmware compliance in a specific time zone.

Steps 8 and 9 are applicable only if you are upgrading HPE Aruba Networking switches (AOS-S and AOS-CX) and Branch gateways. If you are upgrading an Access Point, proceed to step 10.

8. From the **Install On** drop-down, select any one of the following partition options:
   - **Primary partition**—Select this if you want to install the firmware version in the primary partition.
   - **Secondary partition**— Select this if you want to install the firmware version in the secondary partition.
9. Select the check box if you want HPE Aruba Networking Central to automatically reboot after device upgrade.

The **Install On** drop-down option and auto reboot check box option is available only for HPE Aruba Networking switches (AOS-S and AOS-CX) and Branch gateways.

10. Click **Upgrade**.

    The device downloads the image from the server, saves it to flash, and reboots. Depending on the progress and success of the upgrade, one of the following messages is displayed:
    - **Upgrading**—While image upgrade is in progress.
    - **Upgrade failed**—When the upgrade fails.
11. If the upgrade fails, retry upgrading your device.

After upgrading a switch, click **Reboot**.