AOS-10.5.1.1

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

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

Chapter 3
Release Overview

This AOS-10.5.1.1 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.

Important Upgrade Information for HPE Aruba Networking 9000 Series and HPE Aruba Networking 9114 Gateways

Upgrading to AOS-10.5.1.1 from 10.4.1.0/10.5.1.0 or earlier versions may take longer than usual if the BIOS version is out of date and requires an update. This upgrade is estimated to take up to 15 minutes and should not be interrupted for any reason. Power failures and interruptions during the upgrade may make the gateway unusable. Please use caution and plan accordingly.

In a scenario (very rare) when post reload command, the unit does not come up in 15-20 minutes, apply power cycle only once and wait for minimum 15 minutes without re-applying power cycle again.

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 4
What's New

This chapter describes the new features and enhancements introduced in AOS-10.5.1.1. For more information, see *Aruba Central Help Center*.

New Features

There are no new features introduced in this release.

Enhancements

The following enhancement is introduced in this release:

Debug Packet Dump Enhanced for Enforce DHCP Violations

The output for the **debug packet dump** CLI command now includes information regarding packet drops that occur due to enforce DHCP violations.

Supported Hardware Platforms

The following link provides a list of HPE Aruba Networking AP and gateway models supported in AOS-10.5.

Supported Devices in 10.5

Chapter 5
Resolved Issues

This chapter describes the resolved issues in this release.

Table 3: *Resolved Issues in AOS-10.5.1.1*

Bug ID	Description	Reported Version
AOS-228357	Some standalone gateways encountered a PSM Watchdog error with signature **psmdebug 0x01ff000d phydebug 0x21 macctl 0x4160403 maccmd 0x4**. This issue was observed in AP-510 Series and AP-500 Series access points running AOS-10.4.1.0 or later versions. The fix ensures that the PSM Watchdog error does not occur.	AOS-10.4.1.0
AOS-239417 AOS-241359	A few AP-535 access points running AOS-10.5.1.0 or later versions crashed and rebooted due to low memory condition. The log files listed the reason for this error as **kernel panic: softlockup: hung tasks**. The bursts of kernel prints under low memory conditions caused Read-copy update (RCU) stall warnings. This issue was resolved by adding counters to track Packet Capture (PCAP) queue drop during a low memory condition.	AOS-10.5.0.1
AOS-242779	In some APs, a **Check sum mismatch** error was displayed. The issue occurred when the MPSK key name included a space. This issue was observed in APs running AOS-10.4.0.1 or later versions. The fix ensures that the correct checksum value is displayed when the MPSK key name includes a space.	AOS-10.4.0.1
AOS-244990	The Transport Profile configured on an AP-based IoT Connector failed to connect when using **auth server**. This issue occurred because an incorrect **auth-mode** was used for external server transport profiles with credentials for **auth**. This issue was observed in APs running AOS-10.5.0.0. The fix ensures that Transport Profile configured on an AP-based IoT Connector connects successfully.	AOS-10.5.0.0
AOS-245034	Some gateways running AOS 10.4.1.0 or later versions crashed unexpectedly due to a memory leak issue of the **FPAPPS** process. The fix ensures that there is no memory leak in the **FPAPPS** process.	AOS-10.4.1.0
AOS-245226	In Air Pass AOS-10 deployment with tunnel mode SSID, the AP did not send the **Event-timestamp** attribute in the radius accounting packets. This issue was observed in APs running AOS-10.4.0.1 or later versions. The fix ensures that the **Event-timestamp** attribute is sent.	AOS-10.4.0.1
AOS-245297 AOS-247646	In Branch Gateways running AOS-10.4.1.1 or later versions, the datapath crashed and rebooted unexpectedly with multiple uplink failovers with VPNC. The log files listed the reason for the event as **Datapath Timeout**. This issue occurred due to segmentation faults while processing the HCM UDP probe response packet in the Branch Gateway redundancy setup.	AOS-10.4.1.1

Bug ID	Description	Reported Version
	The fix ensures that the datapath does not crash.	
AOS-246051	A few HPE Aruba Networking 7200 Series gateways running AOS 10.4.0.3 were unable to copy an image file from the flash memory to the system partition. The log files listed the reason for the event as **Error Determining image version**. The issue occurred because the wrong image path was used while copying an image file from flash memory to the system partition. The fix ensures that the correct image path is used so that the partition upgrade is successful.	AOS-10.4.0.0
AOS-246198	When users attempted to ping from the source VLAN, the following error message was displayed, **There is no IP address configured for Vlan 220.** even though the L3 interface was configured correctly and the VLAN was up and running. This issue occurred because the VRRP IP address was selected as the primary role. The fix ensures that the devices avoid assigning IP roles as Primary vs Secondary for VLAN and VRRP IP address, and prevents the unintentional removal of the secondary address when the primary address is deleted.	AOS-10.4.1.0
AOS-246552	HPE Aruba Networking 7210 gateways running AOS-10.4.0.0 displayed radius proxy error logs on the device. The log file listed the reason for the event as, **Radproxy context not PRESENT for response from server with key: key=, returning from rp_recv_server_response**. This issue occurred as the logs came in repetitively under **logs.log** entries. The fix ensures that the logs are logged correctly under the **debug** logs.	AOS-10.4.0.0
AOS-246730	Some AP-535 access points running AOS-10.4.1.0 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the crash as **Reboot caused by kernel panic Take care of the TARGET ASSERT first(wlan_peer.c:3218 Assertion (vdev->bss->ni_chan.phy_mode >= peer_ratectrl_params.phymode)**. The fix ensures the APs do not crash.	AOS-10.4.1.0
AOS-246891 AOS-247564	The **AAA profile NOT found for network profile WirelessGuest_#1692621711321_2995#_** error message was displayed when connecting to the guest SSID. This issue occurred because the radius proxy did not receive the configuration updates. The fix ensures that clients successfully connect to the guest SSID.	AOS-10.5.0.0
AOS-247058	The Minew app could be installed twice on the same IoT Connector. This issue was observed on APs running AOS-10.5.0.0. This issue was resolved by adding a check to ensure that the app is not already installed.	AOS-10.5.0.0
AOS-247206	Clients connected to APs across multiple sites were unexpectedly disconnected with the **AP is resource constrained** message appearing in **Analyze** > **Alerts & Events** > **Events** page in HPE Aruba Networking Central. This issue occurred because of insufficient information for correlating specific events with client disconnections. This issue was observed in APs running AOS-10.3.1.2 or later versions.	AOS-10.3.1.2

Bug ID	Description	Reported Version
	The issue was resolved by adding an index (**idx**) to the end of EAP packets, enabling better log correlation and troubleshooting.	
AOS-247319	Users reported that the datapath sessions showed different flags for WLAN and wired users. This issue was observed in HPE Aruba Networking 9012 gateways running AOS-10.4.0.2 or later versions. The fix ensures that the datapath sessions show the correct flags for WLAN and wired users.	AOS-10.4.0.2
AOS-247335	Some 9240 gateways rebooted with the reason **Reboot Cause: Datapath timeout (Intent:cause: 86:56)**. This issue occurred due to DPI packets being passed to the CPU with ID **0**. This issue was observed in gateways running AOS 10.4.0.2 or later versions. The fix ensures that packets are sent to the DPI engine only if the DPI FP is not zero.	AOS-10.4.0.2
AOS-247362 AOS-249361 AOS-251835 AOS-253220	A few boot arguments were missing for HPE Aruba Networking 9000 Series and 9004-LTE gateways running AOS-10.4.1.0 or later versions. This issue occurred after the gateways were upgraded to AOS-10.5.1.0. The fix ensures that the missing parameters are present in the configuration file.	AOS-10.5.1.0
AOS-247551	The output of the **show aaa auth-survivability-cache** command displayed station names in uppercase. This issue was observed in devices running AOS-10.4.1.0 or later versions. The fix ensures that the output is displayed in lowercase where expected.	AOS-10.4.0.2
AOS-247679	Some HPE Aruba Networking 9004 branch gateways running AOS-10.4.0.2 did not allow internal traffic to internal servers for few ACLs. This issue was seen due to endianness. A correction of the endian sequence solved the issue.	AOS-10.4.0.2
AOS-247727 AOS-251147	In Branch Gateways running AOS-10.3.1.0 or later versions, the DNS IP allocation failed because the DNS IP list was not cleared periodically. The Netdestination allowlist did not work because the DNS entries were not added to the firewall DNS Name. The fix ensures that allowlist DNS entries are added to the DNS IP list successfully.	AOS-10.4.0.0
AOS-247952	The output of the **show ap bss-table ap-name** and **ap monitor ap-list ap-name** commands showed incorrect Tx BSSID flag information. Some Virtual APs showed an incorrect (*+) flag next to their BSSID in the CLI output. This issue was observed in AP-635 access points running AOS 10.4.1.0 or later versions. The fix ensures the table output of the commands is accurate.	AOS-10.4.1.0
AOS-248212 AOS-249063	In AOS 10.4.1.0 or later versions, certain Port-Based Tunnel (PBT) user-table entries were not deleted. As a result, new entries for the same users were not created and authenticated. This issue is resolved by altering the way the deleted messages are processed for PBT user-table entries.	AOS-10.4.1.0

Bug ID	Description	Reported Version
AOS-248267 AOS-251592	The RADIUS/RadSec server could not connect to the FQDN host after rebooting the gateway, resulting in IP loopbacks. This issue occurred due to replication problems during validation. This issue was observed in standalone gateways running AOS-10.5.1.1 or later versions. The fix ensures that the server can successfully establish a connection.	AOS-10.5.1.1
AOS-248371	Users were unable to copy the **crash.tar** file while troubleshooting to get the tar crash. This issue occurred when the size of the **crash.tar** file was greater than 2 GB. This issue was observed on HPE Aruba Networking 7240XM gateways running AOS 10.4.1.0 or later versions. The fix ensures that the **crash.tar** file is copied successfully.	AOS-10.4.1.0
AOS-248422	The output of the **show est status** command incorrectly displayed **EST Status :Enabled** message when an AP failed EST re-enrolment. This issue was observed in APs running AOS-10.4.1.2 or later versions. The fix ensures that the command output displays correct status when the AP fails re-enrolment.	AOS-10.5.0.2
AOS-248571 AOS-248645	The tunnel to Axis SSE did not establish when LTE uplink was used in Microbranch. This issue occurred because the traffic skipped the tunnel process and dropped the packet. The fix ensures that the tunnel to Axis SSE establishes successfully.	AOS-10.5.0.0
AOS-248607	APs supporting 802.11ac randomly broadcasted in 20MHz, despite the minimum channel bandwidth set to 40 MHz. The issue occurred because the APs changed channel after receiving a broadcasted CSA frame. This issue was observed in APs running on AOS 10.4.0.3 or later versions. The fix ensures that the APs broadcast in the appropriate channel.	AOS-10.4.0.3
AOS-248680 AOS-250829	Some APs running AOS 10.5.0.0 crashed and rebooted with the reason **BUGSoftLockup: CPU#1 stuck for 23s! [kworker/1:3:20931] PC: __udelay+0x34/0x48 Warm-reset**. The fix ensures that the APs work as expected.	AOS-10.5.0.0
AOS-248742	A few clients failed to connect to an SSID with WPA3-SAE encryption. This issue occurred due to a BSSID mismatch during WPA3 SAE authentication, resulting in frames being sent to incorrect APs. This issue was observed in gateways running AOS-10.4.1.0 or later versions. The fix ensures that the BSSID values match during authentication.	AOS-10.4.1.0
AOS-248972	Some AP-534, AP-535, AP-555, AP-635, and AP-655 access points, running AOS 10.4.1.0 or later versions, rebooted unexpectedly. The log files listed the reason for the reboot as **Reboot caused by WLAN firmware TARGET ASSERT at twt_ap.c:847**. The fix ensures that the APs work as expected.	AOS-10.4.1.0
AOS-249004	In APs running AOS-10.4.1.0 or later versions, the **Cellular Status** and **USB Modem Information** details were missing from the output of the **show cellular status** command. This issue occurred because the standard error data stream was not sent to HPE Aruba Networking Central.	AOS-10.4.1.0

Bug ID	Description	Reported Version
	The fix ensures that the command output includes the **Cellular Status** and **USB Modem Information** details.	
AOS-249109	A ping latency was observed on the HPE Aruba Networking 9012 and 9004-LTE gateways running AOS 10.4.0.2 or later versions, while pinging the default gateway. This issue occurred because the response for every 15th ping packet was delayed as the system was busy gathering port statistics. The fix ensures that the ping latency for the gateways is reduced to 23ms and 7ms respectively.	AOS-10.4.0.2
AOS-249112	In AP-515 access points running AOS 10.4.1.0 or later versions, users were unable to upload videos to the FTP server with Deep Packet Inspection (DPI) enabled. This issue occurred when the camera consistently dropped connections before data transfer, even though the Windows Filezilla FTP client was able to establish a connection. This fix ensures that the videos are uploaded to the FTP server successfully.	AOS-10.4.1.0
AOS-249127 AOS-251681	Some HPE Aruba Networking 9004 gateways running AOS-10.4.0.2 or later versions rebooted intermittently. This issue occurred when the **Datapath** module crashed unexpectedly. The fix ensures that the gateways do not crash.	AOS-10.4.0.2
AOS-249133	Some HPE Aruba Networking 9240 gateways running AOS-10.4.0.1 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Nanny rebooted machine - fpapps process died (Intent:cause: 86:34)**. This issue occurred due to a memory leak in the **fpapps** module. The fix ensures that there is no memory leak in the **fpapps** module.	AOS-10.4.0.1
AOS-249330	An AP received two Transport Profiles with identical names. This is because HPE Aruba Networking Central allows for (as of now) multiple profiles with same name. This issue was observed in APs running AOS-10.6.0.0. The fix ensures that Transport Profiles with identical names are handled correctly.	AOS-10.6.0.0
AOS-249514	The output of the **show running-config** CLI command incorrectly displayed the destination IP address as the source IP address. This issue occurred when site-to-site configuration was created using HPE Aruba Networking 7210 and 7240XM gateways configured as VPNCs. The fix ensures that valid address is displayed in the configuration map.	AOS-10.4.0.3
AOS-249520	HPE Aruba Networking 9004 Branch Gateway running AOS 10.4.0.2 generated a very high number of logs as **Unexpected HCM runtime error at hcm_rtpa_calc_latency 640 s_done 0 for Seq 35832 ip: 63.35.63.34 vlan 776**. This issue occurred because the probe packet was not identified as UDP probe and timestamped when the Egress scheduler profile was configured on the PPPoE interface. The fix ensures that the UDP probe packet is handled correctly when Egress scheduler profile is configured on the PPPoE.	AOS-10.4.0.2

Bug ID	Description	Reported Version
AOS-249528	End users experienced connectivity issues with a few gateways. The **OFA** process in a gateway continuously accessed the TPM (every minute) and entered the **not responding** or **critical** state impacting client connectivity. This caused contention with other services in gateway. This issue was resolved by allowing the **OFA** process to access the TPM only once, when establishing a connection for a client.	AOS-10.4.0.3
AOS-249553	Users were unable to disconnect clients through CoA and an error message, **Session-Context-Not-Found(503)**, was displayed. This issue occurred when the length of the AVP username was 32. This issue was observed in AP-515 access points running AOS-10.5.1.0 or later versions. The fix ensures that the CoA request is accepted when AVP username length is within 100.	AOS-10.5.0.1
AOS-249754 AOS-249851	The SNMP walk failed to retrieve data for the fan tray OID. This issue was observed in gateways running AOS-10.4.1.1 or later versions. The fix ensures that the fan tray OID is displayed correctly.	AOS-10.4.1.1
AOS-249815	A few AP-515 access points running AOS 10.4.1.0 or later versions in tunnel mode showed significantly lower single-client DL performance than the D-tunnel mode with MTU 1500. This issue occurred due to changes in the **TXQWORK_BUDGET** configuration, which caused the AP performance to degrade. The fix ensures improved performance for APs with single-client, tunnel mode, and with MTU 1500.	AOS-10.4.1.0
AOS-249817	The BLE antenna of the AP-635 access points running AOS-10.4.1.0 or later versions failed to scan the tag configured on BLE channel 39. The AP-635 access point comes with an AIC filter that filters out the BLE channels close to the operating Wi-Fi channel. This issue occurred because the AIC filter in the AP filtered out the BLE channel 39, which was near the operating Wi-Fi channel 11. The fix ensures that the AP-635 BLE antenna scans the BLE devices as expected.	AOS-10.4.1.0
AOS-249835	Users trying to migrate their Remote APs from AOS 8 to AOS-10.4.0.0 using the **ap-convert** command found that the external Captive Portal did not work. Although the Captive Portal page was not displayed, a client of a remote AP was able to connect to the SSID. The fix ensures that the Captive Portal page is displayed during the migration.	AOS-10.4.0.0
AOS-249946	Some AP-515 access points running AOS 10.4.0.2 version crashed unexpectedly. This issue occurred due to a **Segmentation** fault in the **ucm** process. The fix ensures that the APs work as expected.	AOS-10.4.0.2
AOS-249976	When the wireless client transferred more than 200 MB of files to the SCP server, the Rx Data Bytes value displayed in the output of **show ap debug radio-stats ap-name** and **show ap debug bss-stats bssid** commands was lower than the actual size of transfer. This issue was observed on APs running AOS-10.4.1.0 and later versions.	AOS-10.4.1.0

Bug ID	Description	Reported Version
	The fix ensures that the Rx Data Bytes displayed in the output of **show ap debug radio-stats ap-name** and **show ap debug bss-stats bssid** commands is about the same size as the file.	
AOS-250170	The mDNS entries of APs running AOS-10.5.1.1 were missing in **Central** cache. It was present in the **Discovered** cache. This issue occurred when the Airtame server was rebooted. The fix ensures that the **Discover** cache entries are not synchronized to the **Central** cache after an Airtame server reboots and the mDNS entries are available in **Central** cache.	AOS-10.5.0.1
AOS-250194	Users reported that the client roaming failed and there were coverage issues. The **AirMatch Reporting Radio** displayed the **EIRP Reason** as **Airmatch Init**, even though the EIRP settings were modified by **AirMatch Solver**. This issue was observed in AP-535 access points running AOS-10.4.0.3 version. The RF related issue was due to synchronization issues in the channel and power settings. The fix ensures that the client roaming works without any coverage issues.	AOS-10.4.0.3
AOS-250199	Users experienced connectivity issues when the primary uplink failed to connect to the network. This issue occurred when the Policy-based routing (PBR) failover mechanism failed between the primary and secondary uplink. This issue was observed in HPE Aruba Networking 9004 Branch Gateways running AOS 10.4.0.2 or later versions. The fix ensures that the PBR successfully fails over between the primary and secondary uplinks.	AOS-10.4.0.2
AOS-250278 AOS-250933	Users connected to the Captive Portal SSID faced frequent internet disconnections when they moved away from the AP. The issue occurred when the client disconnected and connected back within Inactivity Timeout, but the gateway treated the MAC authentication request from AP as a new MAC authentication. The fix ensures that the gateway puts the client in correct role.	AOS-10.5.0.1
AOS-250350	The **Resolve Wrap** process repeatedly crashed and restarted on some HPE Aruba Networking 9004-LTE gateways running AOS 10.5.0.0 or later versions. This issue occurred when the dnsmasq configuration file contained unsupported characters and multiple domain names. The fix ensures that the **Resolve Wrap** process works as expected.	AOS-10.5.0.0
AOS-250404	A few AP-345 access points running AOS-10.4.0.3 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Panic:MemLeak: mem low for 84 seconds, under 0MB 22 times, MB free 7 (1%), total 409 Warm-reset**. This issue occurred because the APs downloaded the ClearPass Certificate Authority (CA) repeatedly. As a result, the APs reported high memory utilization. The issue is resolved by removing the ClearPass CA download timer.	AOS-10.4.0.3

Bug ID	Description	Reported Version
AOS-250559	AP registration messages were received on all nodes immediately after Join causing both sub-clusters to have Active object for **cluster_ddg**. During Join, these active-active objects caused Deactivate events on leader due to wrong DDS resolution. Since the deactivate event was not handled properly, the subsequent DDG updates from the leader were not published to member nodes leading to issues. The fix ensures that the Deactivate event is handled similar to the Add event and that subsequent DDG updates from leader reach other nodes properly.	AOS-10.5.0.0
AOS-250722	Some AP-655 access points running AOS 10.5.0.1 or later versions experienced quality issues during Voice over Internet Protocol (VoIP) calls. This issue occurred when U-APSD was enabled on the APs. The fix ensures that the VoIP calls are established with improved quality.	AOS-10.5.0.1
AOS-251014	The **/flash/boot_log/dmesg.log** file kept increasing in size, leading to the disk being full for virtual gateways running AOS-10.5.0.1. This issue occurred because the output of the **dmesg** command was appended into the file every minute. This issue was resolved by redirecting the **dmesg** command output to **/flash/boot_log/dmesg.log**, instead of appending it to the file.	AOS-10.5.0.1
AOS-251057	In HPE Aruba Networking 7240XM gateways running AOS-10.4.0.3, the OpenFlow Agent (OFA) process in PAPI_Free continuously crashed. This issue occurred due to memory corruption in the OFA process. The fix ensures the OFA process works as expected.	AOS-10.4.0.3
AOS-251092	The output of the **show tunneled-node-mgr stats** command displayed an incorrect switch count. This issue occurred because the switch count was incorrectly incremented in case of cluster failover. This issue was observed on HPE Aruba Networking 9012 gateways running AOS-10.4.0.2. The fix ensures that the **switch_count** variable is incremented only if the switch mac is not present in the hash table.	AOS-10.4.0.2
AOS-251130	HPE Aruba Networking 9240 gateway using OID **sysExtFanStatus** returned the value, 2 (inactive). This issue was observed on HPE Aruba Networking 92xx and 91xx gateway platforms running AOS-10.4.1.0 or later versions. The fix ensures that the gateway returns the correct value for the **sysExtFanStatus** OID.	AOS-10.4.1.0
AOS-251226	A few APs running AOS 10.5.0.1 were unable to assign the correct role to the clients when the clients roamed to another AP. This issue occurred because the previous role overwrote the new role that returned from Authentication Server on the target AP. The issue was resolved by clearing the datapath L3 user when the AP receives the CoA disconnect-user request.	AOS-10.5.0.1

Bug ID	Description	Reported Version
AOS-251653	Users were unable to connect to SSIDs with **Enterprise** security running AOS-10.4.0.3 or later versions. The log files listed the error message, **Client 7c:70:db:0e:da:8f authenticate fail because client blocked due to repeated authentication failures**. The fix ensures that users are able to connect to the SSIDs with **Enterprise** security.	AOS-10.5.0.1
AOS-251742 AOS-252082	When a user upgraded from AOS-10.4.0.2 to AOS-10.4.0.3, high latency was reported while accessing the stock application on the client connected to AP-515. The issue persisted even after upgrading some sites to AOS-10.5.0.1. The fix ensures that the client operates with no latency.	AOS-10.4.0.3
AOS-251912	Following failover from primary to secondary gateway, HPE Aruba Networking Central erroneously reported that the traffic was blocked by ACL even though traffic was blocked by **IP Reputation**. This issue occurred because the denied reason was not set correctly. The fix ensures that: ■ The denied reason is set correctly in all cases. ■ The denied reason is set to 0 when it is not applicable or unknown.	AOS-10.5.1.0
AOS-251932 AOS-252698	A few AP-635 access points with 11r enabled on AOS-10.5.1.0 and connected to Intel 11ac clients, reported MIC failure. This issue occurred because end-of-life Intel 11ac cards were used. The fix ensures that end-of-life Intel 11ac cards are handled correctly.	AOS-10.5.1.0

Known Issues and Limitations

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

Limitations

Following is the limitation observed in this release:

Important Upgrade Information for HPE Aruba Networking 9000 Series and HPE Aruba Networking 9114 Gateways

Upgrading to AOS-10.5.1.1 from 10.4.1.0/10.5.1.0 or earlier versions may take longer than usual if the BIOS version is out of date and requires an update. This upgrade is estimated to take up to 15 minutes and should not be interrupted for any reason. Power failures and interruptions during the upgrade may make the gateway unusable. Please use caution and plan accordingly.

In a scenario (very rare) when post reload command, the unit does not come up in 15-20 minutes, apply power cycle only once and wait for minimum 15 minutes without re-applying power cycle again.

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-10.5.1.1*

Bug ID	Description	Reported Version
AOS-238251	A few clients that are connected to the APs using Distributed L3 mode fail to update the group policy in gateways running AOS-10.5.1.0. This issue occurs because of reassembly failure.	AOS-10.3.1.0
AOS-238397	User-role policies are not applied on user IPs generated by static Network Address Translation (NAT). This issue occurs because the Access Control List (ACL) is applied only if the pre-NAT IP is a user IP, and is not applied if the post-NAT IP is a user IP.	AOS-10.3.1.1
AOS-241150	HPE Aruba Networking gateways running AOS-10.3.1.3 fail to send TACACS accounting information even though TACACS accounting is enabled. **Workaround**: 1. Navigate to **Device** > **System** > **Admin** > **Admin Authentication Servers**.	AOS-10.3.1.3

Bug ID	Description	Reported Version
	2. Under **Admin Authentication Servers**, select the group (AMV). 3. From the Server Group dialogue, select the **Options** tab. 4. Uncheck **Action** and **Configuration**. 5. Save the configuration.	
AOS-242784	Zscaler HC IP routes are not installed as the maximum number of default ECMP paths is set to 5.	AOS-10.5.0.0
AOS-243092	Tagged BPDU packets, from a VLAN that are not allowed in the trunk, pass from one port channel to another. This issue was observed on HPE Aruba Networking gateways in a cluster network running AOS-10.4.0.0. **Workaround**: Enable the spanning tree for the VLAN.	AOS-10.4.0.0
AOS-243386	When the L3 user role changed, the AP did not clear the datapath session resulting in traffic leak from a client assigned with the **denyall** role. This issue was observed on APs running AOS 10.3.1.3.	AOS-10.3.1.3
AOS-245562	The VRRP interface tracking configuration disappears after rebooting the HPE Aruba Networking 9240 gateways running AOS-10.4.0.0. This issue occurs when tracking interface configuration is added during gateway boot-up. **Workaround**: To recover the VRRP interface tracking configuration, re-push the configuration from HPE Aruba Networking Central.	AOS-10.4.0.0
AOS-246107	Client traffic to specific destinations in the same subnet gets dropped when connected to random AP's. This issue occurs on overlay virtual APs running AOS-10.4.0.0. **Workaround**: Reboot the AP or disable **deny-intra-vlan-traffic**.	AOS-10.4.0.0
AOS-246116	9240 gateways running AOS 10.5.0.0 crash due to memory leak when the bandwidth contracts are re-configured dynamically. **Workaround**: Perform bandwidth configuration changes on gateways during the maintenance window.	AOS-10.5.0.0

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**.