AOS-10.7.1.1

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

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-10.7.1.1 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.

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-10.7.1.0. For more information, see *Aruba Central Help Center*.

New Features or Enhancements

There are no new features or enhancements introduced in this release.

Chapter 4
Supported Hardware Platforms

The following link provides a list of HPE Aruba Networking AP and Gateway models supported in AOS-10.7.

Supported Devices in 10.7

Chapter 5
Resolved Issues

This chapter describes the resolved issues in this release.

Table 3: *Resolved Issues in AOS-10.7.1.1*

Bug ID	Description	Reported Version
AOS-250092	The APs associate response for WPA3-SAE (Simultaneous Authentication of Equals) SSID client roaming without 11r cache on the neighbor AP reported **Invalid PMKID**. The issue occurred because the timeout value was not set, due to which the local cache was removed after a time interval of 15 minutes. To fix the issue the time interval is set to 8 hours when adding keycache for SAE and OWE.	AOS-10.4.1.0
AOS-253663	Some AP-515 access points failed to authenticate with uplink 802.1X. The log files listed the reason as, **EAP-TLS using TPM certs authentication failure(timeout)**. This issue was observed in APs running AOS-10.7.1.0. The fix ensures that the authentication works as expected.	AOS-10.7.1.0
AOS-255852	Some APs failed to establish a connection via OOF channel running AOS-10.7.0.0 or later versions. The fix ensures that the connection is established and work as expected.	AOS-10.7.0.0
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-256254	Tunnel events were displayed when the bucketmap was updated after the gateways reloaded. This issue was observed in HPE Aruba Networking 7210 gateways running AOS 10.4.1.1 or later versions. The fix ensures that the tunnel events are not displayed.	AOS-10.4.1.1
AOS-256659	In HPE Aruba Networking Central, users found the hostname field had dots missing in the endpoint details when some devices were enabled. The fix ensures that the hostname field displays correctly.	AOS-10.7.0.0
AOS-256916	Some clients connected to AP-635 access points with 5 GHz and WPA2-PSK-AES got disconnected. This issue occurred when another client tried to connect to the AP. The fix ensures that the clients function as expected.	AOS-10.4.1.0
AOS-256998	Some 7240 Branch Gateways running AOS-10.4.1.1 or later versions experienced WAN redundancy failure and the virtual uplink became unreachable. This issue occurred when the branch gateways were upgraded to AOS-10.4.1.1. The fix ensures that WAN redundancy works as expected for the branch gateway.	AOS-10.4.1.1

Bug ID	Description	Reported Version
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-10.0.11.0
AOS-257931	Some APs with a valid BSSID were incorrectly identified as rogue APs. Sometimes fake rogue BSSIDs were listed in the **show ap monitor ap-list** command output. The fix ensures that the command output contains accurate data.	AOS-10.4.1.0
AOS-258040 AOS-260100 AOS-260111 AOS-260811 AOS-260961 AOS-261010	Some AP-577 access points, running AOS-10.4.1.0 or later versions, rebooted unexpectedly. The log files listed the reason for the reboot as, **BUGSoftLockup:CPU#1 stuck for 22s! [kworker/1:3:27856] PC:wlc_bmac_suspend_mac_and_ wait+0x21c/0x440 [wl_v6]**. The fix ensures that the APs work as expected.	AOS-10.4.1.0
AOS-258055	Some AP-514 access points running AOS-10.7.0.0 version displayed incorrect antenna status when external antennas were connected and disconnected. The fix ensures that the APs work as expected.	AOS-10.7.0.0
AOS-258335	On upgrading the AOS version to AOS-10.6.0.3 or higher on the 9000 Series gateways, user experienced slow browsing if the **WebCC cache-miss-drop** feature was enabled. The fix ensures the improvement in the loading time of the pages at the first attempt.	AOS-10.6.0.3
AOS-258406	Some wireless clients were randomly assigned with the **default_ wired_port_profile** role. This issue was observed in AP-515 access points running AOS-10.4.1.4 or later versions. The fix ensures that the APs work as expected.	AOS-10.4.1.4
AOS-258415	A few APs crashed and rebooted unexpectedly. The log files listed the reason as, **Reboot caused by kernal Panic: Fatal exception in interrupt**. This issue was observed on AP-635 access points running AOS-10.6.0.1 or later versions. The fix ensures that the APs work as expected.	AOS-10.6.0.1
AOS-258773	The 2.4 GHz swept spectrogram chart displayed only the color corresponding to -90 dBm for APs in spectrum monitor mode. The issue was observed in APs running AOS-10.7.1.0 or later versions. The fix ensures that the 2.4 GHz swept spectrogram chart, accurately displays the full range of signal strengths with appropriate colors.	AOS-10.7.1.0
AOS-259231	Some AP-635 access points, running AOS-10.4.1.0 or later versions, randomly crashed with the error, **Reboot caused by kernel panic with whal_ sring.c:1403**. The fix resolved the crash so that clients can connect with the APs.	AOS-10.4.1.0
AOS-259265	Gateway LTE modem did not set PLMN setting when configured manually in LTE uplink configuration due to which Global LTE SIM was unable to switch to different vendors.	AOS-10.4.1.1

Bug ID	Description	Reported Version
	The fix ensures that the Global LTE SIM is able to switch to different vendors.	
AOS-259380 AOS-259882	There was a difference in the values displayed for conductor IP and interface IP (Br0) for AOS-10 AP present in the same sub-net. This issue was seen when STM restarted because the uplink manager did not update the conductor IP when the IP address changed. The fix ensures that the same address is displayed for conductor IP and interface IP.	AOS-10.6.0.3
AOS-259401 AOS-260956 AOS-261680 AOS-262085 AOS-260344 AOS-260627	Some AP-535 access points crashed and rebooted unexpectedly. The log files listed the reason for the event as, **Reboot caused by kernel panic: Fatal exception in interrupt**. This issue was observed in APs running AOS-10.4.1.6 or later versions. The fix ensures that the APs work as expected.	AOS-10.7.0.0
AOS-259648	The gateway **Go Live** data continued to load, but no output was displayed in the device's **WAN** tab. This issue was observed in 9100 Series gateways running AOS-10.4.0.2 or later versions. The fix ensures that the gateway **Go Live** data displays output correctly.	AOS-10.4.0.2
AOS-259710	Several UCM crashes were observed on APs with UCC, due to memory corruption. This issue was observed on APs running AOS-10 versions. The fix resolves the memory corruption issue in APs with UCC.	AOS-10.4.1.0
AOS-259713	When users upgraded the software version to AOS-10.6.0.3 or later versions, they were unable to access the *www.gov.uk* website if the **WebCC cache-miss-drop** feature was enabled. This was observed in 9004 gateways. The fix ensures that the URL is categorized and cached correctly in Datapath.	AOS-10.6.0.3
AOS-259798	The Access Control Entries (ACEs) for Branch Gateways displayed under **Overview** > **Sessions** > **Sessions** table in HPE Aruba Networking Central UI did not match the client traffic data based on the configured policies. However, the CLI displayed accurate information in the datapath output collected from the client. This issue was observed in Branch Gateways running AOS-10.4.1.1 or later versions. The fix ensures that HPE Aruba Networking Central UI displays accurate data for the configured policies.	
AOS-259860 AOS-260096	Some AP-655 access points crashed and rebooted unexpectedly. The log files listed the reason for the event as, **Reboot after internal watchdog dump saved**. The issue was observed in APs running AOS-10.5.1.1 or later versions. The fix ensures that the APs work as expected.	AOS-10.7.0.0
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

Bug ID	Description	Reported Version
AOS-256160	Users were unable to save the AP tech-support log for AP-515 access points. The issue was observed in APs running AOS-10.7.1.0 or later versions. The fix ensures that tech support log collection is optimized, and users can save the logs successfully.	AOS-10.7.1.0
AOS-260223	A gaming console could not connect to a WPA3 pre-shared key SSID on AP-6xx. The authentication failed due to a message integrity check failure. This issue occurred due to a timing issue within the station management module. The fix ensures that the timing event does not occur and the gaming console connects as expected.	AOS-10.6.0.2
AOS-260224	The results of memory related OIDs were negative in the SNMP walk. This issue was observed in AP-735 access points running AOS-10.7.0.1 or later versions. The fix ensures that memory related OID results are positive in the SNMP walk.	AOS-10.7.0.1
AOS-260258 AOS-260383	The output of the **show ap monitor ap-list** commands did not show information for neighboring 5 GHz BSSIDs. This issue was caused by a hardware monitor buffer ring getting stuck, and it also led to APs crashing with the reason, **wal_soc_dev_hw.c:918 Assertion !(panic_mask & WHAL_UMCMN_WBM0_ASSERT_INT_MASK) failed**. The fix ensures APs do not experience these issues. This issue was observed in APs running AOS-10.4.0.2 or later versions.	AOS-10.4.0.2
AOS-260317	Some access points running AOS-10.7.0.1 rebooted unexpectedly. The log files listed the reason for the event as **BadPtr:0000004e PC:spktq_deq+0x14/0x88 [wl_v6] Warm-reset**. The fix ensures that the APs work as expected.	AOS-10.7.0.1
AOS-260357	The access point did not send out accounting start after the client machine authentication when the AP had a machine authentication token. This issue was observed in access points running AOS-10.7.0.1 or later versions. The fix ensures that the AP sends accounting start after client machine authentication.	AOS-10.7.0.1
AOS-260363 AOS-261914 AOS-262403	Some clients connected to 500 Series access points experienced latency and performance issues. The fix brings back the latency and performance to the expected level for these clients. This issue was observed in access points running AOS-10.6.0.3 or later versions.	AOS-10.6.0.3
AOS-260386	Some users intermittently disconnected from the internet and experienced DHCP timeouts from HPE Aruba Networking Central events when connected to AP-635 access points running AOS-10.6.0.1. This issue occurred when SSID in the tunnel mode and bridge mode coexisted on AP and bridge mode SSID with dynamic vlan assignment. The fix ensures that the users are not disconnected from the network.	AOS-10.6.0.1
AOS-260391	High channel utilization (99%) and interference was observed on all 2.4 GHz channels (1,6,11). Clients were unable to connect with 2.4 GHz when channel utilization was high. This issue was observed in AP-635 access points running AOS-10.6.0.1.	AOS-10.6.0.1

Bug ID	Description	Reported Version
	The fix ensures that clients are able to connect on the 2.4 GHz channel.	
AOS-260441	Some AP-635 access points running AOS-10.7.0.0 randomly rebooted with the reason, **Kernel panic: Fatal exception in interrupt**. This issue occurred in an IPsec environment, where a tunneled device was deleted after IPsec encryption. The fix ensures proper validations are made, preventing the AP crash.	AOS-10.7.0.0
AOS-260475 AOS-260960	A few AP-505 and AP-615 access points crashed unexpectedly after the upgrade from AOS-8 to AOS-10. The log file listed the reason for this event as, **AP Reboot reason: BadPtr: 00000006 PC: fips_selftest_gcm+0x1cc/0x36c [fips_tool] Warm-reset**. This issue occurred as the APs were in FIPS mode before the upgrade, which is not supported in AOS-10. The fix ensures that the FIPS mode is disabled by default on AOS-10 versions.	AOS-10.4.0.0
AOS-260599	When clients connected to a Branch Gateway pinged clients on the DC side and vice versa, a 50% packet drop was observed during the switch from the backup LTE cellular uplink to the primary uplink. This issue was observed in Branch Gateways running AOS-10.4.1.5 or later versions. The fix ensures that the IPSec map updates are processed when the LTE cellular uplink status changes to **DOWN**.	AOS-10.4.1.5
AOS-260858	An AOS-10 mesh point failed to forward Spanning Tree Protocol (STP) Bridge Protocol Data Units (BPDUs) to the downlink port when switches were bridged across the mesh link. The log file listed the reason for the STP BPDUs drop as, **drop stp packet when mesh point && no enet0-briding mesh_auto enable:0**. This issue was observed in AOS-10 mesh setups with APs running AOS-10.5.0.0 or later versions as a mesh point and mesh portal. The fix ensures that the AOS-10 mesh setup works as expected.	AOS-10.6.0.2
AOS-260884	Some virtual gateways generated core files repeatedly because the **dnsmasq** process crashed. The issue was observed in gateways running AOS-10.7.0.0 or later versions. The fix ensures that the virtual gateways do not generate multiple core files.	AOS-10.7.0.0
AOS-261032	In a corner case scenario, when a client roamed the new host AP did not send a radius accounting start message to the gateway. As a result, the client would age-out of the gateway user-table and lose connectivity. This fix ensures the radius accounting start message is sent by the AP to gateway in all situations.	AOS-10.5.0.1
AOS-261065	Sometimes clients were unable to authenticate and connect to the guest SSID. This issue was observed on APs running AOS-10.7.1.0. The fix ensures that the clients are able to authenticate and connect to the guest SSID.	AOS-10.7.1.0
AOS-261039 AOS-261220	The dynamic event capture faced an issue where the AWC process crashed while processing some event data. The issue was observed in APs running AOS-10.4.1.5 or latest versions.	AOS-10.4.1.5

Bug ID	Description	Reported Version
	The fix ensures that the APs work as expected, and event are sent correctly to Central without any issues.	
AOS-261113	When the user attempts to configure more than six DHCP profiles on the device using the Northbound API (NB API), the device running AOS-10.7.1.0 crashes. **Workaround**: Delete the excess profiles to recover the device.	AOS-10.7.1.0
AOS-261474	Intermittently, APs running on AOS-10.4.1.5 dropped the client traffic. The log files listed the reason for the drop as, **drop due to not dhcp addr. ue dhcp_addr 0.0.0.0**. The issue occurred when clients switched from one AP with **enforce-dhcp disable** to the other AP with **enforce-dhcp enable** and the client did not renew the IP address via DHCP during the client roaming process. The fix ensures that the client traffic flow is not dropped while roaming between APs.	AOS-10.4.1.5
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-261554	A few OTO tunnels went down and routes were not propagated from the Branch Gateways to VPNC. This issue occurred because of a DC connection issue on Branch Gateways. The fix ensures that the OTO tunnels are up and stable, and routes are propagating as expected.	AOS-10.7.0.1
AOS-261623 AOS-262233	Some AP-555 access points randomly crashed and rebooted. The log files listed the reason for the crash as, **Kernel panic - not syncing: Take care of the TARGET ASSERT**. The fix ensures that the APs do not crash. This issue was observed in APs running AOS-10.4.1.6.	AOS-10.4.1.6
AOS-261672	Some APs generated a **mini_httpd** core dump file with a **New core file generated in process** error message, although the APs did not report a crash. This issue was observed in APs running AOS-10.4.0.0 or later versions. The fix ensures that the AP do not generate an error message. **Duplicates**: AOS-262263, AOS-262434, AOS-262436, AOS-262458, AOS-262459, AOS-262550, AOS-262559.	AOS-10.4.1.6
AOS-261753	Some AP-305 access points running AOS-10.7.1.0 failed to authenticate with uplink 802.1x. The log files listed the reason as, **Failed(-1-256) to sign hash using TPM dev**. The fix ensures that the authentication works as expected.	AOS-10.7.1.0
AOS-261949	Some mobile devices were unable to connect to the Passpoint SSID. This issue occurred when EAP transactions were sent across different connections to the same destination IP. This issue was observed in gateways running AOS-10.4.1.6 or later versions. The fix ensures that the devices are able to connect to the Passpoint SSID.	AOS-10.4.1.6

Bug ID	Description	Reported Version
AOS-262158	Some AP-515 access points randomly crashed and rebooted. The log files listed the reason for the crash as, **BadPtr:00000036 PC:wlc_taf_pktfree_check+0x1b58/0x6140 [wl_v6] Warm-reset**. This issue was observed in APs running AOS-10.4.1.0 or later versions. The fix ensures APs work as expected.	AOS-10.4.1.0
AOS-262315	When Captive Portal authentication failed, the custom value in Radius-reject **Reply-Message** attribute was not displayed in the login page. Instead, **Login error. Please retry** was incorrectly displayed. The fix ensures that if Radius-reject packet contains the **Reply-Message** attribute when Captive Portal authentication fails, the string value of that attribute is displayed in the login page. If not, the message **Login error. Please retry** is displayed.	AOS-10.6.0.3

Chapter 6
Known Issues and Limitations

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

Limitations

Following are the limitations observed in this release:

Configuring Mesh on AP-730 and AP-750 Series

Due to MLO support and BRCM SDK on AP-730 and AP-750 Series access points, the mesh point takes more than 5 minutes to establish mesh link with the mesh portal. This leads to repeated crashes. To avoid the crash, follow the following steps:

1. If you want to provision an AP-730 or AP-750 Series access point to mesh point, first use ethernet to connect to cloud and wait for Central to push the configuration. Ensure that **mesh-role** is auto. Do not use **mesh-role** point.
2. After receiving mesh-related configuration, manually reboot mesh AP. After reboot (keep ethernet connection), mesh point will still use ethernet to connect to cloud since **mesh-role** was auto.

   Then wait more than 5 minutes or check the output of **show ap debug cloud-restore-status**, to ensure that **Verify Time** is N/A. Then plug out the ethernet cable so that mesh AP converts to mesh point (as mesh-role is auto).
3. Restart the mesh AP, then Mesh point will come up with mesh point mode.
4. Every time you change mesh-band or mesh-cluster, perform steps #1 to #3.

MLO Functionality on AP-730 and AP-750 Series

When MLO functionality is enabled on AP-730 and AP-750 Series access points,

1. With transition mode enabled, **enhance-open** SSID profile does not setup any VAP on any radio. In this case, the disable-reason is displayed as, **incompatible opmode or transition mode**.
2. With transition mode disabled, **enhance-open** SSID profile sets up one VAP on each radio.

Network Source or Destination only Supports Any with Third-party Vendors

With third-party vendors, set the network source or destination to **Any**. Site to site VPN tunnel fails to come up with a third-party firewall when the network source or destination is set to **VLAN** instead of **Any**.

No Support for 802.11r with EHT

802.11r is disabled internally if Extreme High Throughput (EHT) is enabled. This is applicable only for the 730 and 750 Series APs. The 6xx and 5xx Series APs work as per the 802.11r configuration in the SSID profile.

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-10.7.1.1*

Bug ID	Description	Reported Version
AOS-248282	7010 gateways display PVST+ issues where the removal of VLANs leads to the incorrect transmission of PVST+ BPDUs with both PVID and 802.1Q VLAN ID set to 0.	AOS-10.4.1.0
AOS-250883	When a logging server type was deleted, it causes the removal of all other logging types from the **show running-config** and **show logging server** commands output. This issue is observed in gateways running AOS-10.6.0.0 or later versions.	AOS-10.6.0.0
AOS-251173	Some APs do not send the correct DHCP decline package type when there is an IP address conflict. This issue is observed in AP-315 access points running AOS-10.7.0.1.	AOS-10.7.0.1
AOS-252114	In some 9240 gateways, egress packets are not properly load balanced across all LAG members; thus, the receive rate at the far end is significantly less than the total ingress packets. This occurs due to an endian issue.	AOS-10.4.1.0
AOS-257202	Some 7220 gateways crash unexpectedly. This issue occurs due to the SNMP process receiving invalid requests with source port 0 from multiple servers.	AOS-10.7.0.0
AOS-258307	Some HPE Aruba Networking 7240XM gateways running AOS-10.4.1.0 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2)**. This issue is observed on gateways with an uptime of more than 100 days and that handle a large number of WLAN access points terminating on them.	AOS-10.4.1.0
AOS-260367	AP-635 access points running AOS-10.6.0.2 crash repeatedly. This issue occurs due to corruption in the **/etc/dnsmasq.conf** configuration file.	AOS-10.6.0.2
AOS-260893	The One Touch Provision (OTP) screens for both static-activate and full-setup in AOS-10 gateways display IPv6 configuration options. However, 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

Bug ID	Description	Reported Version
AOS-260964	VLAN 1 is displayed as the default option for provisioning VLAN instead of 4086, under the static-activate and full-setup One Touch Provision (OTP) options for gateways. **Workaround**: Update VLAN to 4086, to be consistent with the uplink VLAN used by Central wizard.	AOS-10.7.0.0
AOS-261520	Some APs crash and reboot unexpectedly after a virtual AP is removed. The log files list the reason for the crash as, **BadPtr:0000030c PC:wl_pktc_tx+0x1d8/0x798 [wl_v6] Warm-reset**. This issue is observed in AP-505 access points.	AOS-10.7.0.0
AOS-262031	On warm start or cold start of 7000 Series gateways, the Aruba WLSX-TRAP-MIB defined traps (wlsxWarmStart, wlsxColdStart) are not sent, but the standard SNMPv2-MIB traps (warmStart, coldStart) are sent correctly.	AOS-10.4.0.0

Chapter 7

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**.