Extreme IQ Engine v10.8.7 Release Notes

New Features, Fixes, and Known Issues

9039242-11 Rev AA
May 2026

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

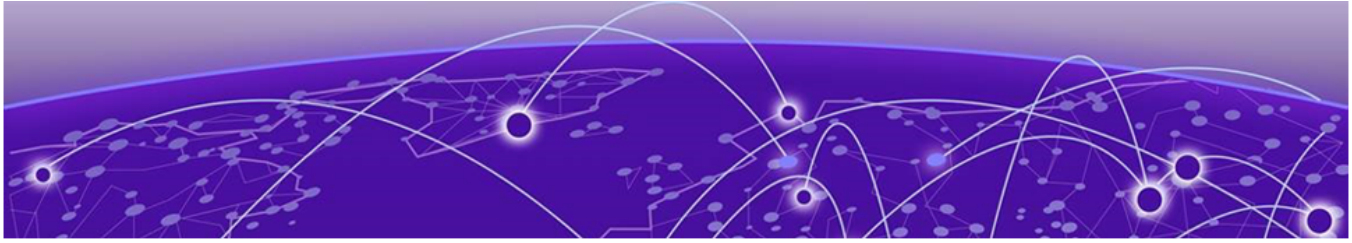
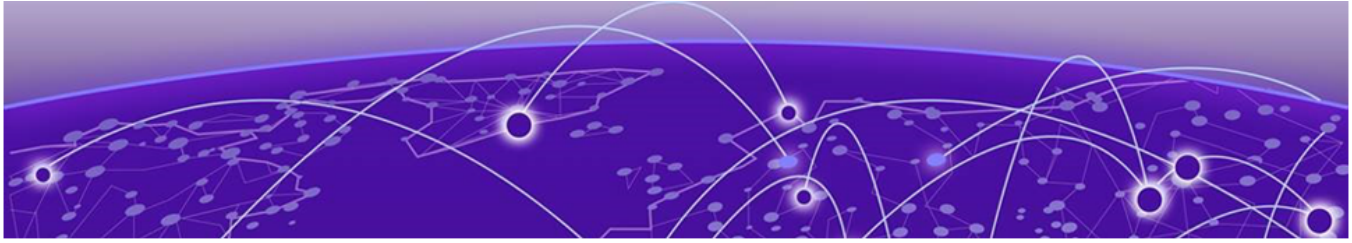
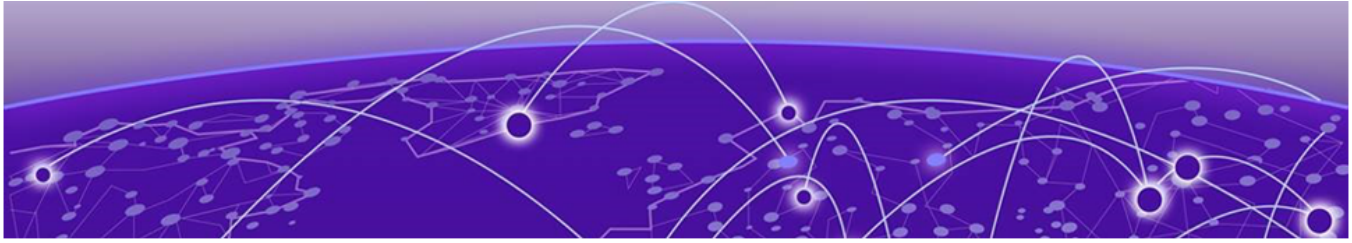


Table of Contents



Abstract

This release notes document for Extreme Networks IQ Engine version 10.8.7 details new features, addressed issues, known limitations, and platform support for cloud-managed enterprise wireless access point deployments integrated with ExtremeCloud IQ 25.10.0 and later. The release introduces functional enhancements across Wi-Fi 6, Wi-Fi 6E, and Wi-Fi 7 platforms, including optional NAT and DHCP behavior in client mode, IEEE 802.3az Energy-Efficient Ethernet support, Wi-Fi Alliance OpenRoaming, RadSec-based UZTNA authentication, and expanded AirDefense Service Platform (ADSP) capabilities on AP4020, AP4060, and AP5020 models. Addressed issues in this release focus on authentication reliability (802.1X, EAP-TLS, WPA2/WPA3, legacy PEAP-MSCHAPv2), Management Frame Protection enforcement, SNMP stability, QoS rate-limit enforcement, roaming behavior with ECWP fallback, and resilience against driver- and kernel-level failures. A known issue documents boot restrictions related to unsupported micro-USB console cables. Information about earlier 10.8 maintenance releases is included for reference. The content targets experienced network administrators and wireless engineers managing production-scale IQ Engine environments.



Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

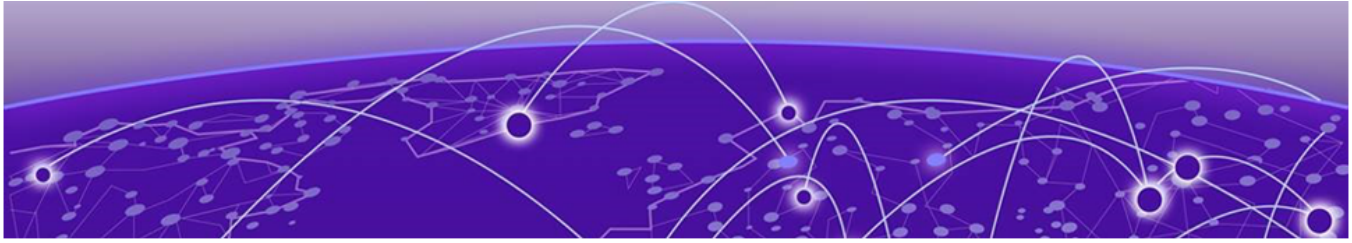
Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.

4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.



General Release Information for Release 10.8.7

Release Date

May 2026

New Hardware Support

There is no new hardware supported for Release 10.8.7.

Hardware Platforms Support

- AP302W
- AP305C
- AP305CX
- AP305C-1
- AP410C
- AP410C-1
- AP460C
- AP460S6C
- AP460S12C
- AP510C
- AP510CX
- AP630
- AP650
- AP650X
- AP3000
- AP3000X
- AP4000
- AP4000-1
- AP4020
- AP4020FX
- AP4020X
- AP4060X
- AP5010

- AP5020
- AP5050D
- AP5050U

Management Platforms Supported

ExtremeCloud IQ 25.10.0 and later

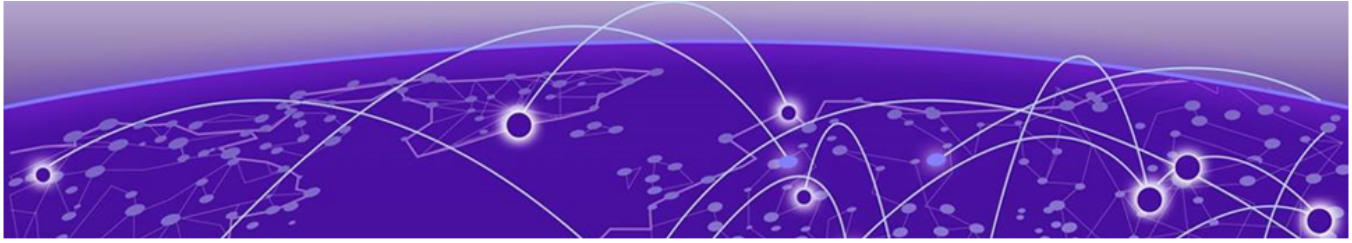
Related Links

New Features in Release 10.8.7 on page 10
Addressed Issues in Release 10.8.7 on page 12
Known Issues in Release 10.8.7 on page 15

New Features in Release 10.8.7

Issue ID	Summary	Description
HOS-17657	Client Mode Enhancement (NAT & DHCP Optional) — 11AX, Wi-Fi 6E, AP4020/4060	IQ Engine provides a configuration option to make NAT optional in client mode on 11AX, Wi-Fi 6E, AP4020, and AP4060 access points. When NAT is disabled, DHCP is not applied, enabling the AP to operate as a bridge with secure access methods such as PPSK. When NAT is enabled, DHCP is required. NAT is enabled by default.
HOS-20285	802.3az Support on the AP4000 and AX Series APs	IQ Engine supports the IEEE 802.3az Energy-Efficient Ethernet (EEE) standard on AP305C/X, AP302W, AP410C, AP460C/S6C/S12C, and AP510C/X access points.
HOS-21126	WBA OpenRoaming Support in IQ Engine — 11AX	IQ Engine supports Wi-Fi Alliance (WBA) OpenRoaming on 11AX access points.
HOS-23909	AP5020: ADSP Support for Wi-Fi 7 Cloud APs	AirDefense Service Platform (ADSP) support is extended to the AP5020 Wi-Fi 7 cloud-managed access point for both ExtremeCloud IQ and ExtremeCloud Private deployment options.
HOS-24351	AP4020/AP4060: ADSP Support for Wi-Fi 7 Cloud APs	AirDefense Service Platform (ADSP) support is extended to AP4020 and AP4060 Wi-Fi 7 cloud-managed access points, including support for the fourth radio on the AP4020, for both ExtremeCloud IQ and ExtremeCloud Private deployment options.

Issue ID	Summary	Description
HOS-24976	Direct RadSec Tunnel for UZTNA Authentication — AP4000 and 11AX APs	AP4000 and 11AX access points establish a direct RadSec tunnel with the Universal Zero Trust Network Access (UZTNA) RADIUS server to perform 802.1x (EAP-TLS, EAP-TTLS) and MAC authentication for UZTNA-enabled SSIDs.
HOS-25288	Client Mode Enhancement (NAT & DHCP Optional) — AP5020	IQ Engine provides a configuration option to make NAT optional in client mode on AP5020 access points. When NAT is disabled, DHCP is not applied, enabling the AP to operate as a bridge with secure access methods such as PPSK. When NAT is enabled, DHCP is required. NAT is enabled by default.



Addressed Issues in Release 10.8.7

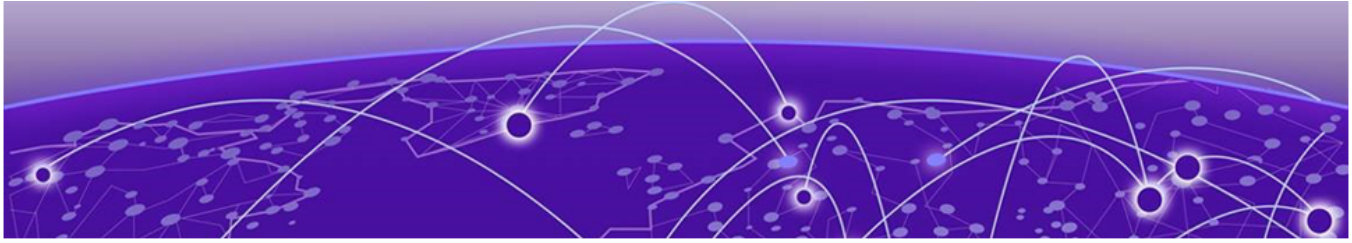
Issue ID	Description
CFD-13082 (03046606)	Addressed the issue where AP305C and AP410C reported a +2 dBm transmit power control (TPC) value for the WIFI1 interface in packet captures, while the correct value was displayed via the AP CLI commands `show acsp` and `show interface wifi1`. The WIFI0 interface was not affected.
CFD-14035 (03098163)	Addressed the issue where SNMP polling stopped working on AP3000 after an AP reboot in environments that also use ExtremeCloud IQ-SE. After rebooting, ExtremeCloud IQ-SE displayed the AP as disconnected and SNMP polling failed. The root cause was incorrect SNMPv3 user creation on the AP after reboot.
CFD-14600 (03141235)	Addressed the issue where a RADIUS user with no Filter-Id attribute was incorrectly assigned the user profile of a previously authenticated user who had a Filter-Id on a WPA2/802.1x CCMP SSID. The AP cached the user profile ID (UPID) from the previous authenticated session and applied it to the subsequent client authentication even when RADIUS returned no Filter-Id.
CFD-15880 (000131745)	Addressed the issue where the SNMP process failed intermittently on AP5020 devices running IQ Engine 10.8.2a. The failure persisted after AP reboots and full configuration pushes, and generated core dumps when the process crashed.
CFD-15948 (03202131)	Addressed the issue where Windows clients failed to connect to a WPA3 SSID on AP410C running IQ Engine 10.8.5, both with and without WPA3 transition mode enabled. macOS clients were not affected. Standard WPA-PSK support was added for Windows client compatibility in WPA3 transition mode.
CFD-16013 (03223115, 03231632, 03233679, 03226780)	Addressed the issue where Windows 11 clients could not connect to an 802.1x SSID when the AP acting as the RADIUS server ran firmware 10.8.5. Clients on Android and iOS connected successfully. The issue was specific to the RADIUS server AP running 10.8.5. The OpenSSL TLS version for the FreeRADIUS application was restricted to TLS 1.2 to resolve the issue.

Issue ID	Description
CFD-16019 (03213922)	Addressed the issue where the AP sent a disassociate frame to a client that was actively attempting to reassociate after roaming, when the External Captive Web Portal (ECWP) Fallback option was enabled with MAC authentication. This caused frequent reconnection failures. The issue was specific to AP410C; the behavior was not observed when roaming between AP4000 units.
CFD-16085 (03225809)	Addressed the issue where the client count displayed in **Manage** > **Devices** in ExtremeCloud IQ was incorrect for some APs. The AP reported the correct number of connected clients, but ExtremeCloud IQ displayed only one active client. The issue occurred in environments with both ExtremeCloud IQ-SE-managed and standard cloud-managed APs, and was caused by the DCD library not being initialized correctly.
CFD-16175 (03230588)	Addressed the issue where the QoS rate limit for upstream traffic was not enforced on AP5020 devices running IQ Engine 10.8.5. Downstream rate limiting and upstream rate limiting on AP4000 functioned correctly under the same configuration. The forwarding engine failed to detect the QoS flag on upstream packets, causing them to bypass the configured rate limit.
CFD-16492 (03240753)	Addressed the issue where the `show memory detail` command returned no output on AP4020 and AP5020 devices running IQ Engine 10.8.6. Other AP models were not affected. A kernel upgrade introduced after 10.8.5 changed the output format of the statm file from eight fields to seven fields. We updated the code to handle both formats.
CFD-16508 (03220996, 03243636)	Addressed the issue where port-based 802.1X authentication failed on APs running firmware 10.8.5 and 10.8.6. An OpenSSL upgrade caused the AP supplicant to fail when loading the private key, which caused EAP-TLS initialization to fail and authentication to be aborted. The fix loads the private key in the application and attaches it directly to the SSL object.
CFD-16517 (03240349, 03241206)	Addressed the issue where refreshing or navigating the AP web UI caused a CGI 500 Internal Error and restarted the php-cgi process on APs running IQ Engine 10.8.5 and 10.8.6. The issue was caused by a missing PHP 8 fix and increased memory usage by the PHP 8 process, which caused the process manager to terminate php-cgi when memory exceeded the configured limit.
CFD-16706 (03250843)	Addressed the issue where the authentication process on AP410C devices running IQ Engine 10.8.6 crashed when memory usage gradually increased beyond 20 MB. The crashes caused frequent connection failures on 802.1x eduroam SSIDs and occurred even when no clients were actively connected to the AP.

Issue ID	Description
CFD-16974 (03262594)	Addressed the issue where the word "accounting" was misspelled as "accouting" in the AP log message for accounting interim update packets.
HOS-23531	Addressed the issue where wireless clients connected with 802.11w (MFP) protection enabled were disconnected by deauthentication attacks. When Management Frame Protection (MFP) was configured in mandatory mode on WPA2 or WPA3 SSIDs, forged deauthentication frames from an attacker could still cause clients to disconnect, even though MFP is designed to protect against such attacks. This issue affected multiple AP models (AP510C, AP650, AP460S6C) and client operating systems (Windows, Apple, Android). This fix ensures that MFP-protected clients correctly ignore forged deauth frames and maintain their connection during deauthentication attacks.

Known Issues in Release 10.8.7

Issue ID	Description
HOS-18313	AP5010, AP5050D, and AP5050U devices will not boot when some non-Extreme micro-USB cables are connected. **Note:** Use the Extreme Networks certified ACC-WIFI-MICRO-USB console cable for all Extreme Networks access points. Other MICRO-USB console cables are not tested and certified by Extreme Networks. **Workaround:** Use an Extreme Networks-certified console cable, or plug in the cable after the AP boots.



Earlier 10.8 Releases

The following sections provide information about changes for earlier IQ Engine 10.8 releases.

Release 10.8.1 New Features and Addressed Issues

Release Date

March 2025

New Hardware Supported

Release 10.8.1 adds support for the AP4020.

New Features in Release 10.8.1

Feature ID	New feature	Description
HOS-20155	AP4020: Imago Tag ESL Support	The AP4020 supports the VusionGroup ImagoTag ESL dongle.
HOS-20158	AP4020—Wi-Fi mesh support	IQ Engine 10.8.1 supports wireless backhaul mesh for the AP4020.
HOS-20690	AP5020: Wi-Fi 7 11BE—Support for UL MU-MIMO	IQ Engine 10.8.1 supports UL MU-MIMO for the AP5020.
HOS-20722	AP4020: Support for UL MU-MIMO	IQ Engine 10.8.1 supports UL MU-MIMO for the AP4020.

Feature ID	New feature	Description
HOS-20734	AP4020: Support for DL OFDMA	IQ Engine 10.8.1 supports downlink OFDMA for the AP4020.
HOS-20754	AP4020: Support for enhanced packet capture	The AP4020 supports Enhanced Packet Capture.
HOS-21715	AP5020: HotSpot 2.0 Configuration in IQ Engine support	IQ Engine 10.8.1 supports Hotspot 2.0 for the AP5020.
HOS-21793	AP5020: FA (Autosense) IQ Engine Default LLDP Handling	IQ Engine 10.8.1 LLDP is enabled by default for the AP5020.
HOS-22152	AP4020: Support 802.3az Green Ethernet	IQ Engine 10.8.1 supports Energy-Efficient Ethernet (EEE) or IEEE 802.3az for the AP4020. This feature allows physical-layer transmitters to consume less power during idle states or low data activity.
HOS-22381	AP4020—"RegreSSHion" Vulnerability in OpenSSH	CVE-2024-6387, also known as the "regreSSHion" vulnerability, is fixed.

Addressed Issues in Release 10.8.1

Issue ID	Description
CFD-13308	We increased the AUTH timeout value to give users sufficient time to enter the credentials for AP5000 and AP5020.
CFD-13309	We resolved an issue where the AP5020 sent probe responses with a basic rate of 24Mbps instead of the configured 36Mbps.
CFD-13374	We resolved an issue where AP5020 models with shut-down SSIDs were still broadcasting with Open Authentication, even after rebooting.

Release 10.8.2 New Features and Addressed Issues

New Hardware Support

There is no new hardware supported for Release 10.8.2.

Table 1: New features in 10.8.2

Feature ID	New feature	Description
HOS-18924	AP5020: Client mode support 2.4, 5G , 6G	IQ Engine supports Client Mode on 2.4 GHz, 5 GHz, & 6 GHz radios on the AP5020.
HOS-18929	AP5020: Support for Spectrum Analyzer 2.4G/5G	The 2.4 GHz & 5 GHz radios on the AP5020 support Spectrum Intelligence.

Table 1: New features in 10.8.2 (continued)

Feature ID	New feature	Description
HOS-20276	Enhancement to Reduced Neighbor Report (RNR) - AP3K, AP5010/5050	The AP3000, AP3000X, AP5010, AP5050U, and AP5050D support Enhanced Reduced Neighbor Report (eRNR). This feature adds advanced RNR capability and provides useful information to Wi-Fi 6E/7 clients by probing in the 2.4 and 5 GHz bands for Wi-Fi 6 SSID capabilities for the radio housed in the AP. The probe also looks for neighbor APs to which the client could eventually roam. The Co-Located bit in the RNR IE indicates that the 6 GHz radio is housed in the same AP. A value of 0 indicates a different BSSID for a neighboring 6 GHz radio.
HOS-20642	AP5020: Support for WPA3 Beacon Protection	The AP5020 supports Wi-Fi 7 Beacon Protection to protect Wi-Fi beacon frames from disruption or interference.
HOS-20751	AP4020: Support for AKM 24 for WPA3-Personal (SAE)	The AP4020 supports WPA-3 Personal (SAE) AKM 24.
HOS-20752	AP4020: Support for WPA3 Beacon Protection	The AP4020 supports Wi-Fi 7 Beacon Protection to protect Wi-Fi beacon frames from disruption or interference.
HOS-21357	AP4020: Support for Spectrum Analyzer 2.4G/5G	The 2.4 GHz & 5 GHz radios on the AP4020 support Spectrum Intelligence.
HOS-21359	AP4020: Client Mode supports 2.4, 5G, 6G	IQ Engine supports Client Mode on 2.4 GHz, 5 GHz, & 6 GHz radios on the AP4020.
HOS-21537	AP4020: Support for Essentials Sensing 4th radio	IQ Engine supports the 4th radio on the AP4020 reporting to Essentials.
HOS-21713	AP4020: Support for dynamic packet capture	The AP4020 supports Dynamic Packet Capture.
HOS-21979	Port Description (TLV) to LLDP Neighbor (AX & 4000)	We added the "Port Description" to the **`#show LLDP Neighbor`** output in IQ Engine (AP305C, AP410C, AP460C, AP305CX, AP460S6, S12, and 4000)
HOS-22052	HotSpot 2.0 Configuration In IQ Engine for the AP4000	The AP4000 supports HotSpot 2.0.
HOS-22053	HotSpot 2.0 Configuration In IQ Engine for the AP4020	The AP4020 supports HotSpot 2.0.

Table 1: New features in 10.8.2 (continued)

Feature ID	New feature	Description
HOS-22078	Enable the FIPS feature for AP4020	The AP4020 supports Secure-Mode for GovRAMP-compliant RDCs.
HOS-22239	Report BLE Scan Results via HTTPS with Token Renewal for WiFi 6E	WiFi 6E APs support a token-based secure method of sending BLE Data to an HTTPS server.

Table 2: Addressed issues in 10.8.2

Issue ID	Description
CFD-12903 (03038362)	We resolved an issue where the error "^-- unknown keyword or invalid input" occurred when using CLI Access from ExtremeCloud IQ.
CFD-12949 (03038743)	We resolved an issue where a vulnerability was detected for HTTP/HTTPS on APs running IQ Engine 10.7r3.
CFD-13238 (03056232)	We resolved a latency issue with the AP5010 running IQ Engine Release 10.7.3 or 10.7.5.
CFD-13524 (03074406)	We resolved an issue where local PPSK user groups caused the configuration audit for APs running IQ Engine Release 10.7.5 to report missing users.
CFD-13628 (03082265)	We resolved an issue where some APs in the same management VLAN flooded logs with "pmksa_cache_auth_add". The issue occurred with the 11r feature enabled in ExtremeCloud IQ, when an 11r-supported client connected or disconnected. This issue is fixed in Release 10.8.2 by enabling the log only when debug auth is on.
HOS-22363	We resolved an issue where packet captures for an AP4020 running IQ Engine 10.8.1 using the Enhanced Packet Capture tool in ExtremeCloud IQ did not include beacon frames.
HOS-22445	We resolved an issue with the AP4020 and ADSP-sensor mode and BSS/air-termination, where the sensor successfully sent DeAuth packets, and errors occurred after a few hours.
HOS-22670	We resolved an issue with the error: Check certificates and key files failed. For IQ Engine Release 10.8.2, we strongly recommend updating your certificates to use cryptographic keys of at least 2048 bits with a widely accepted strong algorithm.

Release 10.8.2a New Features and Addressed Issues

New Hardware Support

There is no new hardware supported for Release 10.8.2a.

New Features in Release 10.8.2a

There are no new features in this release.

Addressed Issues in Release 10.8.2a

This patch release resolves an issue for the AP4020 and AP5020 access points, where the ACSP (RRM protocol) could select the same 6 GHz channel as a neighboring access point.

Release 10.8.3 New Features and Addressed Issues

New Hardware Support

There is no new hardware supported for Release 10.8.3.

New Features in 10.8.3

Feature ID	New feature	Description
HOS-21750	Wi-Fi 7 Platforms - Enhancement to Reduced Neighbor Report (RNR)	Enhanced Reduced Neighbor Report (RNR) provides improved roaming for 6 GHz clients.
HOS-22323	Fabric-Attach (Autosense) IQ Engine new Default LLDP Handling (AP302W, AP305C, AP410C, AP460C, AP510C)	IQ Engine 10.8.3 enables LLDP for the AP302W, AP305C, AP410C, AP460C, and AP510C by default.
HOS-22984	Fabric-Attach (Autosense) IQ Engine new Default LLDP Handling (AP4000)	IQ Engine 10.8.3 enables LLDP for the AP4000 by default.

Addressed Issues in 10.8.3

Issue ID	Description
CFD-13644 (03082327)	We resolved an issue where ExtremeCloud IQ and CLI displayed different values for the AP5020 WiFi2 channel width.
CFD-13950 (03056147)	We resolved an issue where ExtremeCloud IQ did not reflect a change in VLAN/Subnet in "show int usb0".
HOS-22705	We resolved an issue where the AP4020 crashed when using Spectrum Intelligence on WiFi0 (2.4 GHz).
HOS-22838	We increased the allocated memory for 3-radio access points (AP4000, AP4000U, AP4020, AP5010, AP5020, AP5050D, AP5050U) from 20 Mb to 64 Mb. This increase resolves issues reported in CFD-13612.

Issue ID	Description
HOS-22874	We implemented a fix to add 6G neighbors (different SSID) with ERNR enabled to all 2.4G and 5G BSS with ERNR enabled.
HOS-22959	We resolved an issue where an L7 crash occurred on the AP4020 with the AVC (ZOOM) application.
HOS-22967	We resolved an issue where IDM authentication (Enterprise and PPSK) failed on FIPS-enabled APs.
HOS-22982	We resolved an issue where parsing certificates and key files failed on the AP5020.
HOS-23131	We resolved an issue where the IDM Certificate failed to apply on AP3000, AP5010, and AP5050 devices. We strongly advise that you upgrade your certificates to use cryptographic keys of at least 2048 bits with a widely accepted strong algorithm.

Release 10.8.4 New Features and Addressed Issues

New Hardware Support

Release 10.8.4 introduces support for the following new hardware:

- AP4020FX
- AP4020X
- AP4060

New Features in 10.8.4

Feature ID	New feature	Description
HOS-20013	AP5020 to AP5020 WiFi mesh support for WDO	The AP5020 supports mesh/wireless bridge on 2.4 Ghz, 5 GHz, and 6 GHz.
HOS-21281	Change Primary Default IQE Public DNS (Including Factory Images)	OpenDNS became unavailable in certain countries and territories. Therefore, we changed the primary public DNS for IQ Engine from OpenDNS to Cloudflare (1.0.0.1). The secondary public DNS entry for IQ Engine is still OpenDNS (208.67.220.220). This change applies to the following models: AP3000, AP3000X, AP4020, AP4020X, AP4020FX, AP5010, AP5020, AP5050D, and AP5050U.
HOS-21553	IQ Engine Support for the AP4020FX Platform	IQ Engine supports the AP4020FX platform.
HOS-21554	IQ Engine Support for the AP4060X Platform	IQ Engine supports the AP4060X platform.
HOS-21556	IQ EngineSupport for the AP4060 Platform	IQ Engine supports the AP4060 platform.

Feature ID	New feature	Description
HOS-21587	AP4020FX: Support for Indoor AFC	The AP4020FX supports Indoor AFC.
HOS-21810	Solum dongle support for WiFi 7 APs	The AP4020, AP4020X, AP4020FX, and AP5020 support the Solum dongle.
HOS-21811	Hanshow dongle support for WiFi 7 APs	The AP4020, AP4020X, AP4020FX, and AP5020 support the Hanshow dongle.
HOS-22600	Update Curl in IQ Engine—11ax and AP4000	IQ Engine for the 802.11AX APs and the AP4000 has been updated to address two CVEs: • CVE-2018-1000005 • CVE-2018-1000007
HOS-22626	Update the OpenSSH Version to the Latest (AX & 4K)	We strongly recommend that you upgrade OpenSSH to the latest available version. For more information, see CVE-2024-6387.
HOS-22811	AP4060/X: Add Outdoor Mode to Access Point (IQ Engine Only)	The AP4060 and AP4060X support outdoor AFC for 6 GHz standard power (IQ Engine only).
HOS-22858	IQ Engine: Standards-Based GRE Failover	IQ Engine supports a secondary Standards-based GRE IP Address. This feature introduces the new **Failover IP Address** field.
HOS-23199	Fabric Attach Redundancy Support	Fabric Attach for IQ Engine supports redundancy (red0) on AP3000, AP3000X, AP4000, AP4000U, AP4020, AP5010, AP5020, and AP5050D. Therefore, when a failover from Eth0 to Eth1 occurs, the failover maintains the VLAN to I-SID mapping.
HOS-23248	WBA OpenRoaming Support In IQ Engine—AP4020X support	The AP4020X supports the WBA OpenRoaming feature.
HOS-23332	AP4060/AP4060X for Outdoor AFC Support	The AP4060 & AP4060X support outdoor AFC (6 GHz Standard Power, for IQ Engine only).

Addressed Issues in 10.8.4

Issue ID	Description
CFD-13173 (03053176)	We resolved an issue where a scheduled scan did not run, even when a trigger condition existed.
CFD-13506 (03064391)	We resolved an issue where communication occurred between devices connected to an AP5020, with the **Inter-station Traffic** setting disabled.
CFD-13749 (03087413)	We resolved an issue where incorrectly displayed network health as 0/100 **Poor**.

Issue ID	Description
CFD-13977 (03094885)	We resolved an issue where AP302W devices configured for a maximum power drop of 3dB, were dropping by 11dB.
CFD-14176 (03101888)	We resolved an issue where ExtremeCloud IQ ignored the RADIUS VLAN attribute when using PPSK with MAC authentication and user profile classification.
CFD-14224 (03097693)	We resolved an issue where neighboring APs chose the same 5GHz DFS channel when the SDR profile was enabled.
CFD-14289 (03123431)	We resolved an issue where AP410C devices experienced random high CPU usage spikes.
CFD-14436 (02916216)	We resolved an issue where an AP5010 repeatedly experienced an **Unable to handle kernel paging request at virtual address 000103f4aa00040b** error.
CFD-14956 (03154832)	We resolved an issue where wifi0 radio went down for AP5020 devices upgraded to 10.8.3 and was restored after downgrading to 10.8.2a.
HOS-23136	We resolved an issue where beacon protection was not enabled for all 6GHz SSIDs. For example, if an SSID is on both the 5GHz and 6GHz bands and beacon protection is disabled on 5GHz, beacon protection is still mandatory for the 6GHz band.

Release 10.8.5 New Features and Addressed Issues

New Hardware Support

There is no new hardware supported for Release 10.8.5.

New Features in 10.8.5

Feature ID	New Feature	Description
HOS-23332	AP4060/4060X Outdoor AFC Support	Added Automated Frequency Coordination support for AP4060 and AP4060X access points operating in outdoor mode.
HOS-23092	AP4060/X Essentials Sensing 4th Radio Support	Introduced shared sensing support for 2.4 GHz and 5 GHz bands on the fourth radio to enable WIPS Essentials applications and ADSP on-premises functionality on AP4060/X platforms.
HOS-23079	AP4020FX Essentials Sensing 4th Radio Support	Introduced shared sensing support for 2.4 GHz and 5 GHz bands on the fourth radio to enable WIPS Essentials applications and ADSP on-premises functionality on AP4020FX platforms.

Feature ID	New Feature	Description
HOS-23062	AP4020X Essentials Sensing 4th Radio Support	Introduced shared sensing support for 2.4 GHz and 5 GHz bands on the fourth radio to enable WIPS Essentials applications and ADSP on-premises functionality on AP4020X platforms.
HOS-22905	Open SSH Version Update	Updated Open SSH to version 10.0p2 for AX and 4K series access points (platforms 302W, 305C, 410C, 460C, 510C, 4000) to address CVE-2024-6387 security vulnerability.
HOS-22811	AP4060/X Outdoor Mode Support	Added outdoor operational mode configuration capability for AP4060 and AP4060X access points, including support for outdoor omni-angle mount and outdoor fixed-angle mount deployment options.
HOS-22770	LLDP System Capabilities Enhancement	Enhanced LLDP neighbor information by adding system capabilities and enabled capabilities data to the LLDP/CDP Info EVENT, enabling improved network topology visibility and switch identification.
HOS-21556	AP4060 IQ Engine Platform Support	Introduced IQ Engine support for the AP4060 access point platform, including indoor and outdoor mode configurations.
HOS-21554	AP4060X IQ Engine Platform Support	Introduced IQ Engine support for the AP4060X access point platform with external antenna capability.

Addressed Issues in 10.8.5

Issue ID	Description
HOS-23697	Fixed an issue where AP5020 access points were missing power configurations for radios A, AN-HT20, and AC-VT80 in the Isle of Man (IM) country code. The compliance table has been updated to include the correct power settings for this region.
HOS-21883	Addressed the issue where AP5020, AP5000, AP4000, AP5050, and AP4060 access points exhibited low antenna power output when increasing transmit power settings. This affected multiple channel bandwidths (20MHz, 40MHz, and 80MHz) on the 5GHz band, where certain antennas showed significantly reduced power levels at higher configured power settings.

Release 10.8.5b New Features and Addressed Issues

Note
ExtremeCloud IQ Engine Release 10.8.5b is the alternative to 10.8.6 for deployments that do not require support for the Multi-Link Operation (MLO) feature.

New Hardware Support

There is no new hardware supported for Release 10.8.5b.

New Features in 10.8.5b

Feature ID	New Feature	Description
HOS-19952	Support for Packet Capture on Thread interface —AP5010	The Packet Capture tool supports the Thread Interface on the AP5010.
HOS-23474	Thread: Refactor commissioner start and stop	When the Thread Commissioner Start or Stop function is used, the commissioning operation applies at the building level rather than targeting individual device IDs. This change improves device onboarding in scenarios where the Thread network has become segmented, resulting in multiple isolated Thread network partitions.
HOS-23898	IQ Engine to Add MD4 for Legacy Supplicant Authentication	We added the MD4 cryptographic module back into IQ Engine to support backwards compatibility for legacy authentication, such as PEAP-MSCHAPv2, for both wired and wireless. This update resolves CFD-14824.

Addressed Issues in 10.8.5b

Issue ID	Description
CFD-15141 (03169486)	Fixed an issue where the 6th- and 9th-generation Apple iPad (MR7F2LL/A) failed to connect to a WPA3 SSID with 802.11r enabled on AP5010 running IQ Engine 10.8.3. The AP incorrectly processed iPad association requests, treating the WPA IE version as WPA2 and rejecting the RSN information element when 802.11r mobility domain information was present.
CFD-15234 (03176342)	Fixed an issue where the client snapshot report on AP5020 displayed SSID names as unrecognizable or corrupted symbols. The SSID name field in the DCD stats snapshot incorrectly populated with garbage values instead of the actual SSID string upon client association.

Issue ID	Description
CFD-15356 (03177352)	Addressed the issue where AP5020 units running IQ Engine 10.8.2a reported a gradual increase in memory utilization from approximately 48% after reboot to up to 70% over the course of a week, along with FWTRAP-related reboots. The memory usage increase and FW trap crashes are resolved in IQ Engine 10.8.3a and later.
CFD-15385 (03172946, 03218917, 03225560)	Fixed an issue where Wi-Fi sub-interfaces were missing from the authentication host access point daemon (HAPD) interface list after an SSID un-bind and re-bind sequence or following a power outage. This caused security SSIDs to broadcast as Open SSIDs, or prevented Open SSIDs from assigning IP addresses to clients.
CFD-15554 (03192730)	Fixed an issue where AP5020 and AP4020 units running IQ Engine 10.8.4 or 10.8.5 crashed with a kernel panic triggered by a NULL pointer dereference in the Broadcom Wi-Fi driver key management receive path (wlc_keymgmt_recvdata). The crash also occurred in the ADSP sensor receive path (ah_adsp_sensor_rx) under IQ Engine 10.8.5.
CFD-15607 (03193484, 03237962)	Fixed an issue where AP4020 units running IQ Engine 10.8.3a or 10.8.4 rebooted randomly because an attempt to read from an unreadable memory address in the wlc_keymgmt_recvdata path of the Broadcom WLAN driver cause a kernel panic.
CFD-15648 (03175771)	Fixed an issue where Zebra MC3300x and WT6000 handheld scanners periodically disconnected from AP510CX. The ARP requests from the scanners were held in the AP beyond the tolerance threshold of the client before being forwarded, causing the client to interpret the lack of response as a connectivity failure and disconnect.
CFD-15695 (03201360)	Fixed an issue where AP5010 units running IQ Engine 10.8.3a rebooted frequently with a kernel panic triggered by a NULL pointer dereference in the wipsk (WIPS) module during ADSP air termination processing. The crash occurred in the Fpm_ThreadFunc path when the ADSP sensor transmitted deauthentication frames to rogue clients.
CFD-15764 (03190727)	Fixed an issue where the lighttpd web server process on AP5020 units running IQ Engine 10.8.2a and 10.8.5 failed to restart automatically after a crash, causing the Guest Essentials captive portal to stop functioning. TCP traffic interception was also disrupted due to TCP RST packets. A factory reset was required to restore portal functionality.
CFD-15804 (03209689)	Fixed an issue where AP410C-1 units running IQ Engine 10.8.4 and 10.8.5 crashed with a kernel panic in the ah_cwp_vector function within the forwarding engine (fe) module. The crash occurred during ingress packet processing and affected multiple APs across deployments.
CFD-15819 (03208411)	Fixed an issue where AP5020 units did not apply the configured 2.4 GHz minimum basic rate (MBR) after any type of reboot, including factory reset. The AP broadcasted legacy 802.11b rates (1, 2, 5.5, 11 Mbps) despite the running configuration reflecting the correct MBR settings. A Delta update or CLI push was required to enforce the correct rates in the current boot cycle.

Issue ID	Description
CFD-15880 (000131745)	Fixed an issue where the SNMP process on AP5020 units running IQ Engine 10.8.2a failed and generated core dumps within hours of a complete configuration push. Rebooting the AP temporarily restored SNMP functionality, but the process continued to fail intermittently.
CFD-15948 (03202131)	Addressed the issue where Windows clients failed to connect to a WPA3 SSID on AP410C running IQ Engine 10.8.5, while macOS clients connected successfully. The issue persisted even with 802.11r disabled and with updated Windows Wi-Fi drivers. Enabling WPA2 as a workaround restored client connectivity.
CFD-15960 (03220254)	Fixed an issue where AP5020 units running IQ Engine 10.8.4 and 10.8.5 rebooted due to firmware (FW) trap events, primarily TRAP type 0x7, and non-maskable interrupt (NMI)-triggered hardware watchdog resets. The issue affected approximately 6 out of 100 APs in the deployment.
CFD-16013 (03223115, 03231632)	Fixed an issue where Windows 11 clients failed to authenticate to an 802.1x SSID when the AP acting as the RADIUS server ran IQ Engine 10.8.5. The client connected successfully on IQ Engine 10.8.3 and 10.8.4. Other client operating systems such as Android and iOS were unaffected.
CFD-16064 (03223727)	Fixed an issue where Wi-Fi clients intermittently failed to obtain a DHCP IP address when connecting to a Guest Essentials SSID on AP5020 running IQ Engine 10.8.5. The forwarding engine dropped DHCP Discover packets with a "dhcp: blocked, drop pak" error. The issue did not occur on IQ Engine 10.8.2a.
CFD-16085 (03225809)	Addressed the issue where the active client count displayed in XIQ under **Manage** > **Devices** did not match the actual client count reported by the AP CLI. The discrepancy occurred randomly across APs in environments with mixed XIQ-SE and standard AP data sources.
CFD-16150 (03227182)	Fixed an issue where the weak SNR probe request suppression feature did not function on AP5020 running IQ Engine 10.7r5 and later, including 10.8.3 and 10.8.5. Clients with an SNR below the configured suppression threshold were still permitted to associate. The feature worked correctly on IQ Engine 10.7.3. The root cause is related to a conflict with the dynamic capture function.
CFD-16261 (03234068)	Fixed an issue where AP5020 units continued to broadcast beacon and probe response frames for SSIDs that were in a shutdown state during the ACSP channel selection process. Clients associated with the shut-down SSID received an IP address of 0.0.0.0 and could not complete the connection process.
HOS-22918	Fixed an issue where iPhone 16 failed to roam with WPA3 FT-SAE+beacon protection (5ghz/6ghz) configured on AP5020 and AP4020 APs.
HOS-24087	Fixed an issue where AP3000 and AP5000 series clients failed to connect to the AD server.

Release 10.8.5c New Features and Addressed Issues

New Hardware Support

There is no new hardware supported for Release 10.8.5c.

New Features in 10.8.5c

There are no new features for Release 10.8.5c.

Addressed Issues in 10..8.5c

Issue ID	Description
CFD-15343 (03178845)	Fixed an issue where user profile/VLAN assignment could remain incorrect after a username change (user versus machine authentication) by redoing reassignment instead of using stale roaming-cache data.
CFD-16019 (03213922)	Fixed ECWP fallback roaming where the AP could send a disassociation during client reassociation by removing vendor driver logic that initiated disassociation during TX validation (multicast L3 roaming scenarios).
CFD-16175 (03230588)	Fixed AP5020 upstream QoS rate limiting not being enforced by ensuring the FE correctly detects QoS-flagged packets and applies the configured per-client limit.
CFD-16508 (03220996, 03243636)	Fixed wired 802.1X supplicant authentication failures (EAP-TLS) after an OpenSSL upgrade by loading/parsing the private key in the application and attaching it directly to the SSL object.
HOS-23531	Fixed a defect with 802.11w/MFP mode configuration.
HOS-23898	Fixed a backwards compatibility issue for legacy authentication (such as PEAP-MSCHAPv2) for both wired and wireless (related: CFD-14824) by adding the MD4 cryptographic module back into IQ Engine.

Release 10.8.6 New Features and Addressed Issues

New Hardware Support

There is no new hardware supported for Release 10.8.6.

New Features in 10.8.6

Feature ID	New Feature	Description
HOS-19952	Support for Packet Capture on Thread interface—AP5010	The Packet Capture tool supports the Thread Interface on the AP5010.
HOS-21760	RTTS: Enable RTTS on other WiFi7 platforms—AP4020	The AP4020/X/FX model access points support Real-Time Troubleshooting (RTTS).
HOS-21894	RadSec Proxy AP Election Improvements (OpenRoaming)	We made improvements to better handle the RadSec election process when an intermix of APs running older firmware alongside APs with newer firmware exists in the same network.
HOS-23139	Indoor SP without AFC spectrum confirmation: radio behavior—LPI	When a 6 GHz radio that is configured for the Standard Power (SP) does not receive spectrum from the AFC server, the access point will fall back to LPI (Low Power Indoor) mode.
HOS-23172	HOS—Update AVC Signature to the latest version for 32/64-bit platforms—All platforms	The IQ Engine AVC (Application Visibility & Control) Signature library has been updated.
HOS-23474	Thread: Refactor commissioner start and stop	The Thread Commissioner Start/Stop function applies at the building level rather than targeting individual device IDs. Commissioning across the entire building improves device onboarding in scenarios where the Thread network has become segmented into multiple isolated Thread network partitions.

Addressed Issues in 10.8.6

Issue ID	Description
CFD-14784 (03147164, 03155257, 03189433)	Addressed the issue where APs did not refresh the connection after VLAN reassignment was completed successfully with Extreme Control. After a user switched accounts triggering reauthentication with a different VLAN assignment, the AP assigned the correct user profile and VLAN but the client retained the old IP address until manually disconnecting and reconnecting.
CFD-15187 (03173839)	Addressed the issue where AP5010 experienced performance degradation caused by high CPU utilization. The system CPU exceeded 60 seconds of busy time, leading to core dump file generation and RadSec AP election problems.
CFD-15282 (03086326)	Addressed the issue where Apple CNA (Captive Network Assistant) was popping up on iOS 18 and newer devices when the Prevent Apple CNA option was enabled. The AP returned HTTP 200 with an HTML <body>, which triggered the CNA popup caused by changed behavior in iOS 18.

Issue ID	Description
CFD-15343 (03178845)	Addressed the issue where roaming clients incorrectly used cached UPID values even when associating with different usernames or user groups, leading to incorrect VLAN and profile assignments.
CFD-15385 (03172946, 03218917, 03225560)	Addressed the issue where WiFi sub-interfaces were missing in the show auth list, causing authentication interfaces to fail initialization. Security SSIDs changed to Open or Open SSIDs failed to provide IP addresses to clients.
CFD-15554 (03192730)	Addressed the issue where Access Points experienced system crashes in the ADSP module. The kernel panic was caused by invalid memory access during Wi-Fi driver stack processing.
CFD-15607 (03193484)	Addressed the issue where AP4020 access points were rebooting from kernel panics. The APs experienced unreadable memory errors at random intervals affecting multiple devices.
CFD-15648 (03175771)	Addressed an issue with ARP handling where some devices experienced periodic Wi-Fi disconnections.
CFD-15695 (03201360)	Addressed an issue where an AP5010 was frequently rebooting with the "Kernel panic - not syncing: Fatal exception" message.
CFD-15764 (03190727)	Addressed an issue where the AP5020 Webserver kept restarting and causing Guest Essentials to stop working.
CFD-15819 (03208411)	Addressed the issue where AP5020 and AP4020X WiFi0 interface did not follow configured data rates after a reboot. The AP broadcast beacon and probe frames were using legacy b rates, even though these rates were disabled in the configuration.
CFD-15960 (03220254)	Addressed the issue where the AP5020 experienced firmware traps and NMI-triggered reboots. The access points encountered watchdog timer expiration and firmware trap type 0x7 errors.
HOS-23966	Addressed an issue where the outdoor 6GHz txbf power is too low for the AP4060X.
HOS-24087	Addressed an issue where clients failed to connect to the Active Directory server on AP3000 and AP5000 platforms when trunk configuration was used.

Release 10.8.6a New Features and Addressed Issues

New Hardware Support

There is no new hardware supported for Release 10.8.6a.

Note
Release 10.8.6a corresponds with Release 10.8.6.1.

New Features in 10.8.6a

There are no new features for Release 10.8.6.a.

Addressed Issues in 10.8.6a

Issue ID	Description
CFD-15234 (03176342)	Addressed the issue where SSID names displayed as unrecognizable symbols or malformed values in the device monitoring interface. The AP5020 reported incorrect SSID names with all "Z" characters instead of the actual configured SSID names.
CFD-16064 (03223727)	Addressed the issue where WiFi clients intermittently failed to obtain DHCP IP addresses when connecting to Guest Essentials SSIDs on AP5020 running IQE version 10.8.5. The forwarding engine blocked DHCP packets, preventing clients from completing the connection process.
CFD-16150 (03227182)	Addressed the issue where the weak signal probe request suppression feature was not functioning on AP5020 models. Stations with SNR below the configured threshold were not suppressed from connecting, and no weak-snr-suppress log entries were generated when clients connected below the threshold value.
CFD-16261 (03234068)	Addressed the issue where the AP5020 continued to broadcast beacons for SSIDs after they were shut down during Auto Channel Selection Process (ACSP). When an SSID was disabled, the radio interface showed down status, but beacon frames continued transmitting, causing clients to connect and receive invalid IP addresses (0.0.0.0).
HOS-22916	Addressed the issue where iPhone 16 failed to roam with FT and WPA3 enterprise with beacon protection enabled on 5GHz. Reassociation failed, requiring clients to re-associate completely rather than roaming successfully.
HOS-22918	Addressed the issue where iPhone 16 failed to roam with WPA3 FT-SAE and beacon protection enabled on 5GHz/6GHz. Reassociation failed, causing clients to re-associate from scratch instead of performing a seamless roam.
HOS-24617	Addressed the issue where AP4060 in the UK (country code 826) did not show wifi0 or wifi1 interfaces when running firmware 10.8.5. The APs failed to broadcast networks and rejected commands related to wireless interfaces, stating "Interface has no available channels," despite being certified for UK operation.
HOS-24651	Addressed the issue where AP4020 RvR 6GHz single client throughput degraded more than 50% compared to 10.8.5. The performance regression affected wireless throughput measurements in the 6GHz band.
HOS-24693	Addressed the issue where clients failed to connect to MLO SSIDs on AP4020 when MLO was down in mixed MLO and non-MLO SSID configurations. The AP dropped authentication requests with "cfg sync not complete" errors, preventing both MLO and non-MLO clients from connecting.