IQ Engine v10.8.4 Release Notes

New Features, Fixes, and Known Issues

9039242-05 Rev AA
October 2025

Copyright © 2025 Extreme Networks, Inc. All rights reserved.

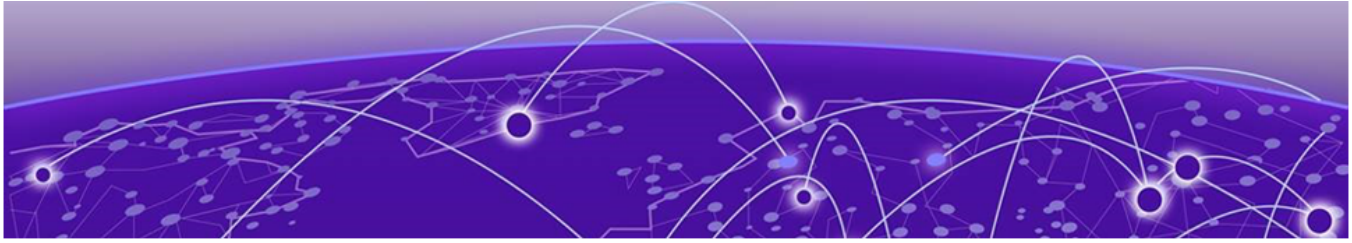


Table of Contents

Abstract iv
Help and Support v
Subscribe to Product Announcements v

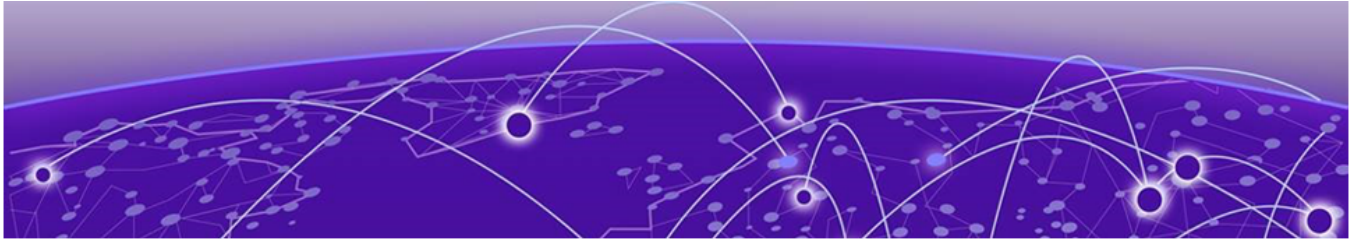
General Release Information for Release 10.8.4 7
Release Date 7
New Hardware Supported 7
Hardware Platforms Supported 7
Management Platforms Supported 8

New Features in Release 10.8.4 9

Addressed Issues in Release 10.8.4 11

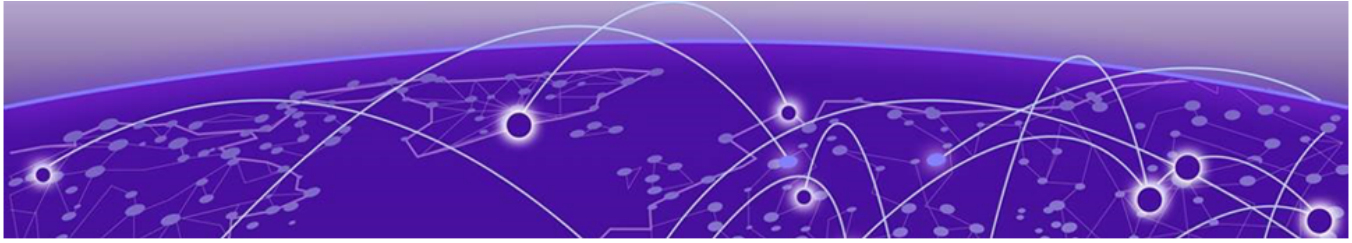
Known Issues in Release 10.8.4 12

Earlier 10.8 Releases 13
Release 10.8.1 New Features and Addressed Issues 13
Release Date 13
New Hardware Supported 13
New Features in Release 10.8.1 13
Addressed Issues in Release 10.8.1 14
Release 10.8.2 New Features and Addressed Issues 14
New Hardware Support 14
Release 10.8.2a New Features and Addressed Issues 16
New Hardware Support 16
New Features in Release 10.8.2a 17
Addressed Issues in Release 10.8.2a 17
Release 10.8.3 New Features and Addressed Issues 17
New Hardware Support 17
New features in 10.8.3 17
Addressed issues in 10.8.3 17



Abstract

This release notes document for IQ Engine version 10.8.4 provides technical updates, feature enhancements, and issue resolutions for wireless infrastructure managed via ExtremeCloud IQ version 25.5.0 and later. It introduces support for new hardware platforms AP4020FX, AP4060, and AP4060X, and expands functionality across Wi-Fi 6E/7 access points with features such as mesh bridging, Fabric Attach redundancy, OpenRoaming, and AFC support for indoor and outdoor deployments. The release also adds support for Hanshow and Solum dongles. Security improvements include updates to Curl and OpenSSH addressing CVEs, and recommendations for cryptographic key upgrades. The document outlines resolved issues affecting scan scheduling, interstation traffic control, CPU performance, RADIUS VLAN handling, and beacon protection enforcement. Known issues include boot failures with uncertified USB cables and spectrum analysis crashes on specific bands. Designed for technical readers, the document provides detailed feature IDs, platform compatibility, and configuration guidance to support enterprise wireless network operations.



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

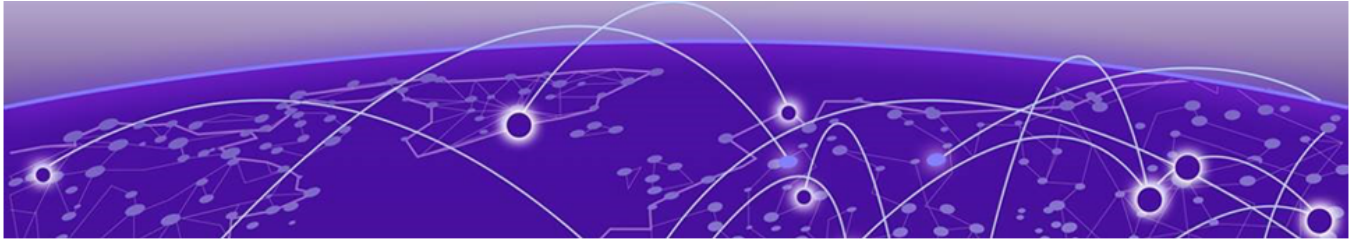
Subscribe to Product Announcements

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 10.8.4

Release Date

October 2025

New Hardware Supported

Release 10.8.4 introduces support for the following new hardware:

- AP4020FX
- AP4020X
- AP4060

Hardware Platforms Supported

- 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 25.5.0 and later

Related Links

New Features in Release 10.8.4 on page 9
Addressed Issues in Release 10.8.4 on page 11
Known Issues in Release 10.8.4 on page 12

New Features in Release 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.
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).

Feature ID	New feature	Description
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 Release 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**.
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.

Known Issues in Release 10.8.4

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.
HOS-22705	AP4020 devices running IQ Engine version 10.8.2 might experience a crash when Spectrum Intelligence is used on WiFi0 (2.4 GHz). **Note:** Spectrum Intelligence functions as expected on the 5 GHz band.

Earlier 10.8 Releases

Release 10.8.1 New Features and Addressed Issues on page 13
Release 10.8.2 New Features and Addressed Issues on page 14
Release 10.8.2a New Features and Addressed Issues on page 16
Release 10.8.3 New Features and Addressed Issues on page 17

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.
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.

Feature ID	New feature	Description
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.