



Extreme IQ Engine v10.9.1 Release Notes

New Features, Fixes, and Known Issues

9041225-00 Rev AA
August 2026



Copyright © 2026 Extreme Networks, Inc. All rights reserved.

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/>

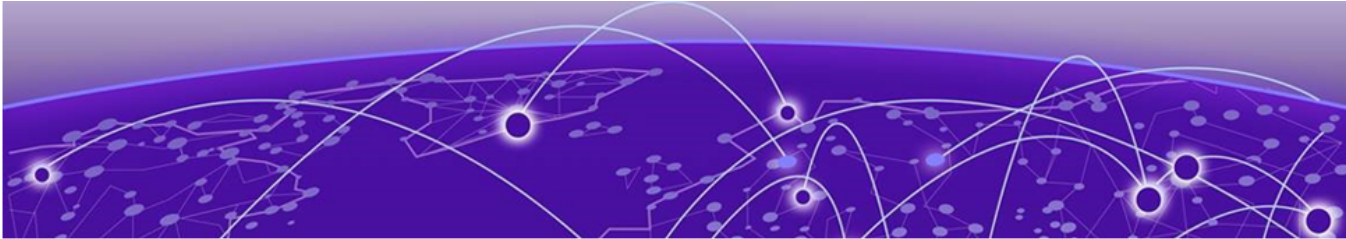


Table of Contents

Abstract..... iv

Help and Support..... v

 Subscribe to Product Announcements..... v

General Release Information for Release 10.9.1..... 7

 Release Date..... 7

 New Hardware Support..... 7

 Hardware Platforms Support..... 7

 Management Platforms Supported..... 8

New Features in Release 10.9.1..... 9

Addressed Issues in Release 10.9.1.....10

Known Issues in Release 10.9.1..... 12



Abstract

This release notes document for Extreme IQ Engine version 10.9.1 covers new features, addressed issues, and known issues for Extreme Networks access points managed via ExtremeCloud IQ 25.13.0 or later. Released August 2026, this version introduces no new hardware but delivers key security and interoperability enhancements across a broad range of AP platforms, including the AP3000, AP4000, AP4020, AP5020, and AP5022 series. A notable security update (HOS-25681) deprecates SHA-1 cryptographic algorithms for SSH access, enforcing SHA-2 (minimum SHA-256) for host key algorithms, key exchange methods, and MACs across numerous supported AP models. Electronic Shelf Label (ESL) support is extended via Solum and Hanshow dongles on AP3020, AP3020X, and AP3020W platforms. Addressed issues resolve MLO SSID beaconing failures, 802.1X PEAP authentication on 802.11ax APs, CWP redirect failures on AP5020, AP4000 kernel panics, TLS 1.3 incompatibility affecting AFS server connectivity, and WPA3-Enterprise PMKID reassociation handling. One known issue documents boot failures on AP5010, AP5050D, and AP5050U when non-Extreme-certified micro-USB console cables are connected.



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

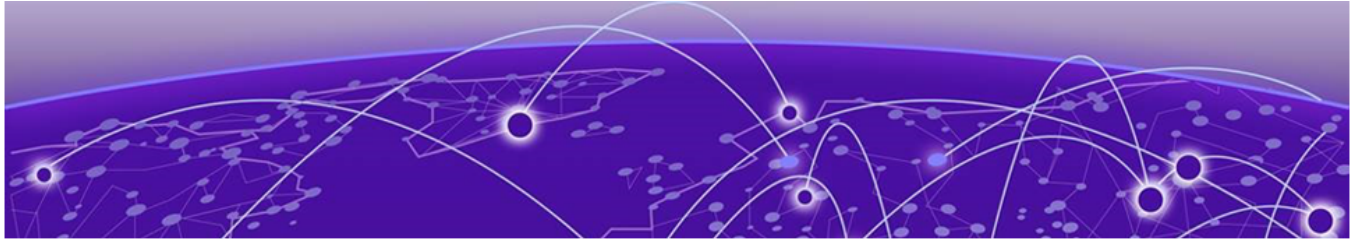
Subscribe to Product Announcements

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 10.9.1

Release Date

August 2026

New Hardware Support

There is no new hardware supported for Release 10.9.1.

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
- AP5022
- AP5022FX
- AP5022S6D
- AP5050D
- AP5050U
- AP5060D
- AP5060U

Management Platforms Supported

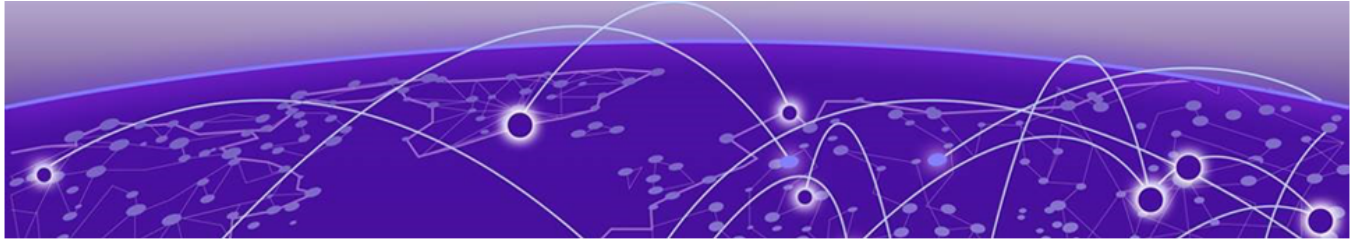
ExtremeCloud IQ 25.13.0 and later

Related Links

[New Features in Release 10.9.1](#) on page 9

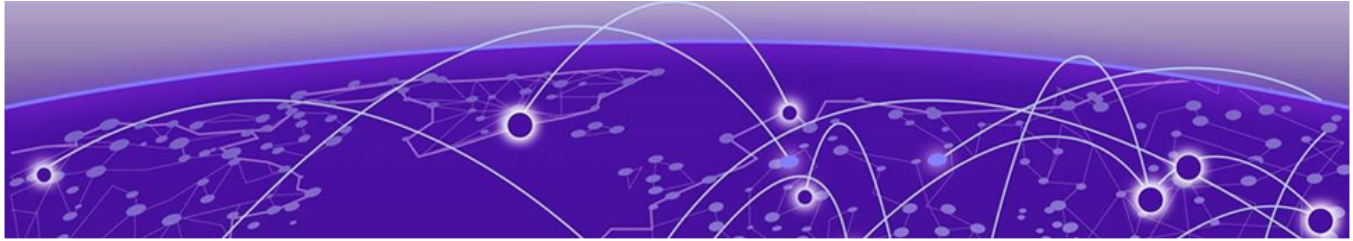
[Addressed Issues in Release 10.9.1](#) on page 10

[Known Issues in Release 10.9.1](#) on page 12



New Features in Release 10.9.1

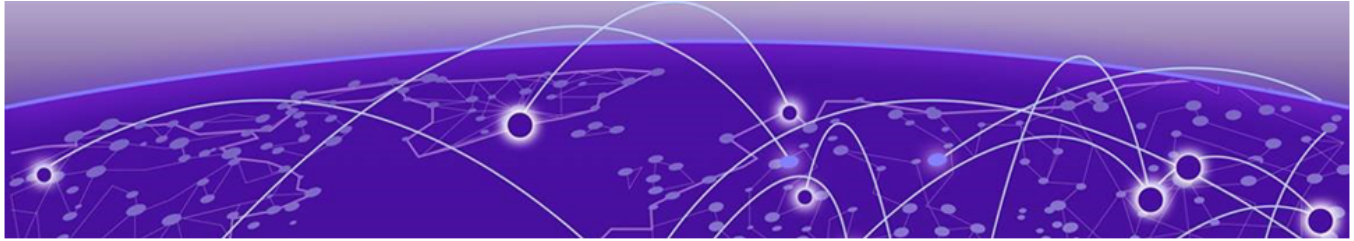
Issue ID	Description
HOS-25681	IQ Engine deprecates SHA-1-based cryptographic algorithms for SSH client access and enforces SHA-2 (minimum SHA-256) or stronger alternatives for host key algorithms, key exchange methods, and MACs on the following AP models: AP305C/AP305CX, AP410C/AP410CX, AP460C/AP460CX, AP510C/AP510CX/AP510X, AP650/AP650X, AP3000/AP3000X, AP4000, AP5010, AP5050U/AP5050D, AP3020/AP3020X/AP3020W, AP3060, AP4020, AP5020, and AP5022/AP5022FX/AP5022SD6.
HOS-25408	IQ Engine supports the Hanshow dongle for Electronic Shelf Label (ESL) functionality on the AP3020W.
HOS-25406	IQ Engine supports the Solum dongle for Electronic Shelf Label (ESL) functionality on the AP3020 and AP3020X.
HOS-25405	IQ Engine supports the Solum dongle for Electronic Shelf Label (ESL) functionality on the AP3020W.



Addressed Issues in Release 10.9.1

Issue ID	Description
CFD-17330 (03273228)	Addressed the issue where the <code>show interface wifi</code> command on AP5020 displayed inaccurate running average TX/RX channel utilization percentages when the interference map was enabled in the radio profile.
CFD-17265 (03275875)	Addressed the issue where the AP4000 did not respond to directed probe requests for hidden SSIDs on the Wi-Fi 6E (6 GHz) band.
CFD-17183 (03243636)	Addressed the issue where port-based 802.1X authentication using PEAP was not functional on 802.11ax APs running IQ Engine 10.8.5 and later.
CFD-17065 (03264578)	Addressed the issue where AP4000 devices running IQ Engine 10.8.5 and later failed to download captive web portal (CWP) files, complete configurations, and firmware images from the AFS server in network environments that did not permit TLS 1.3 connections.
CFD-17040 (03261495)	Addressed the issue where the Monitor > Clients view for an AP in ExtremeCloud IQ showed no client connection records when a time range beyond one day was selected.
CFD-17017 (03263775, 03240101, 03245697, 03271580, 03289423)	Addressed the issue where captive web portal (CWP) redirects did not occur on AP5020 when external CWP was configured through NAC.
CFD-16073 (03224570)	Addressed the issue where AP4000 devices experienced intermittent kernel panics, causing unexpected restarts.
HOS-25573	Addressed the issue where AP4020 devices with Winbond flash could not be downgraded from IQ Engine 10.8.7 to IQ Engine 10.8.5d.
HOS-25546	Addressed the issue where the <code>show station</code> command on the AP5020 displayed a positive RSSI value instead of a negative value for wireless clients connected to the wifi0 dual 6 GHz radio.
HOS-25474	Addressed the issue where Thread network dataset comparisons between DCD configuration and OTBR stored values triggered an unnecessary factory reset. Network key values no longer appear in error logs.
HOS-25466	Addressed the issue where, after disabling the wifi2 radio on an AP4020 with multiple MLO SSIDs configured, all MLO SSIDs stopped beaconing and only non-MLO SSIDs remained visible on-air.

Issue ID	Description
HOS-25465	Addressed the issue where the log message <code>ah_dcd_show_fa_map_db: get fa map db on iotgw failed</code> appeared unnecessarily in AP logs.
HOS-25453	Addressed the issue where clients connected through the eth1 port of an AP4020 or AP5020 operating in client mode with NAT/DHCP disabled received an IP address but could not communicate with the client mode AP.
HOS-24525	Addressed the issue where disabling an MLO radio by shutting down its associated SSID on AP4020 and AP5020 caused the MLO session to go down completely instead of reconfiguring in dual-band mode.
HOS-23886	Addressed the issue where, on a WPA3-Enterprise Suite B 192-bit SSID, the AP initiated a full EAP authentication exchange on reassociation even when the client provided a valid PMKID in the reassociation request.



Known Issues in Release 10.9.1

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.