Extreme IQ Engine v10.9.2a (10.9.2.1) Release Notes

New Features, Fixes, and Known Issues

9041225-02 Rev AA
October 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/

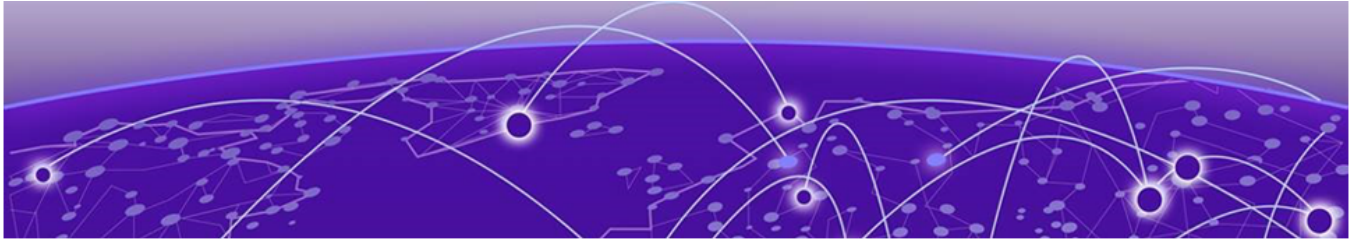


Table of Contents

Abstract iv
Help and Support v
Subscribe to Product Announcements v
Extreme Support Portal vi
Create an End Customer Extreme Support Portal Account vi
Create a Partner Extreme Support Portal Account vii

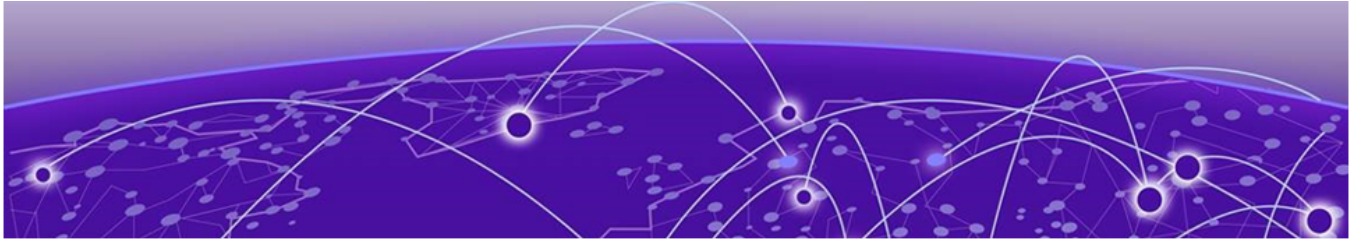
General Release Information for Release 10.9.2a (10.9.2.1) 8
Release Date 8
New Hardware Support 8
Hardware Platforms Support 8
Management Platforms Supported 9

New Features in Release 10.9.2a (10.9.2.1) 10

Addressed Issues in Release 10.9.2a (10.9.2.1) 11

Known Issues in Release 10.9.2a (10.9.2.1) 12

Earlier 10.9 Releases 13
Release 10.9.1 New Features and Addressed Issues 13
New Hardware Support 13
New Features in 10.9.1 13
Addressed Issues in 10.9.1 14
Release 10.9.2 New Features and Addressed Issues 15
New Hardware Support 15
New Features in 10.9.2 15
Addressed Issues in 10.9.2 15



Abstract

This release notes document for Extreme IQ Engine version 10.9.2a (10.9.2.1), dated October 2026, describes a security maintenance release for Extreme Networks access points, written for network administrators. The release adds no new hardware or features. It addresses one issue by upgrading the embedded PHP runtime to version 8.4.27, which resolves CVE-2026-109618 and CVE-2026-109619, vulnerabilities that could allow remote code execution through the web UI. This release requires ExtremeCloud IQ (Classic or New) or Extreme Platform ONE Networking 25.14.0 or later.

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.

Extreme Support Portal

The Extreme Networks Extreme Support Portal provides access to:

- License management
- Firmware downloads
- Case management
- GTAC Knowledge base
- And more

To access the portal, you must first create an account. The Extreme Support Portal provides separate registration forms for End Customers and Partners.

Before you begin, gather the following: A valid corporate email address — required to receive the appropriate level of portal access. Your company details: company name, address, phone number (include country code if outside the US), job title, and job role. At least one supporting identifier: Sold-to number, serial number, contract number, or Purchase Order (PO) number.

Create an End Customer Extreme Support Portal Account

The Extreme Support Portal provides separate registration forms for End Customers and Partners. Use this task to create an End Customer account.



Note
If you are adding a new user to an existing account, the new user must complete and be vetted through the same registration process.

The portal registration page is at https://extreme-networks.my.site.com/.

1. Go to the Extreme Support Portal and select **Login or Signup** on the login page.
2. On the login page, select **Create a new Extreme Customer Portal Account** .
3. Complete all required fields (marked *). Use your corporate email address to ensure the appropriate access level.



Important
Do not register with a personal email address.

4. Read the Support Portal Terms of Use and select the acknowledgment check box to accept.



Important
You must accept the Terms of Use before you can submit the form. You can adjust or withdraw consent at any time through the Email Preference Center.

5. Select **Register**.

   A confirmation message appears on the page and a password setup email is sent to your corporate email address.
6. Open the password setup email and follow the instructions to create your portal password.

   Tip
   If the email does not appear in your inbox within a few minutes, check your spam or junk mail folder.

7. To log in to the support portal go to: https://extremesaas.my.site.com/.

Create a Partner Extreme Support Portal Account

The Extreme Support Portal provides separate registration forms for End Customers and Partners. Use this task to create a Partner account.

The portal registration page is at https://extreme-networks.my.site.com/.

1. Go to the Extreme Support Portal and select **Login or Signup** on the login page.
2. On the login page, select **Create a new Extreme Partner Portal Account**.
3. Complete all required fields (marked *). Use your corporate email address to ensure the appropriate access level.

   Important
   Do not register with a personal email address.

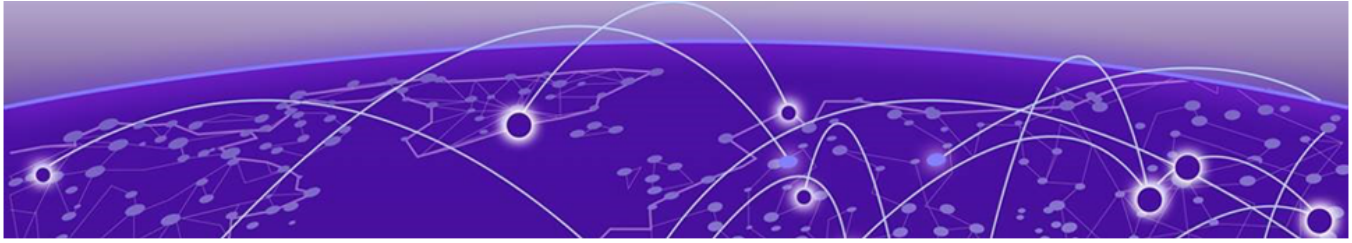
4. Read the following terms and select the required check boxes:
   - Support Portal Terms of Use
   - Extreme Networks Standard Reseller Terms and Conditions
   - Trade Compliance Terms and Conditions

   You can adjust or withdraw consent at any time through the Email Preference Center.
5. Select **Register**.

   A confirmation message appears on the page and a password setup email is sent to your corporate email address.
6. Open the password setup email and follow the instructions to create your portal password.

   Tip
   If the email does not appear in your inbox within a few minutes, check your spam or junk mail folder.

7. To log in to the support portal go to: https://extremesaas.my.site.com/.



General Release Information for Release 10.9.2a (10.9.2.1)

Release Date

October 2026

New Hardware Support

There is no new hardware supported for Release 10.9.2a (10.9.2.1).

Hardware Platforms Support

- AP302W
- AP305C
- AP305CX
- AP305C-1
- AP410C
- AP410C-1
- AP460C
- AP460S6C
- AP460S12C
- AP510C
- AP510CX
- AP650
- AP650X
- AP3000
- AP3000X
- AP3020W
- AP3060
- AP4000
- AP4000-1
- AP4020
- AP4020FX
- AP4020X
- AP4060

- AP4060X
- AP5000
- AP5010
- AP5020
- AP5022
- AP5022FX
- AP5022S6D
- AP5050D
- AP5050U
- AP5060D
- AP5060U

Management Platforms Supported

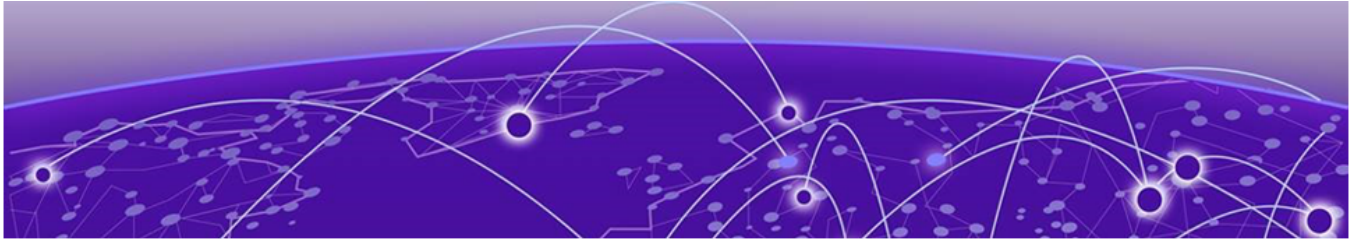
ExtremeCloud IQ and Extreme Platform ONE™ Networking 25.14.0 and later



Note
Instances of ExtremeCloud IQ refer to ExtremeCloud IQ (Classic) and ExtremeCloud IQ (New).

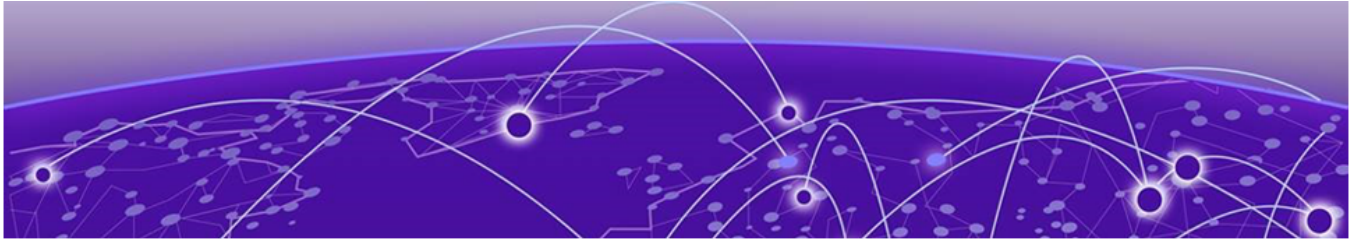
Related Links

New Features in Release 10.9.2a (10.9.2.1) on page 10
Addressed Issues in Release 10.9.2a (10.9.2.1) on page 11
Known Issues in Release 10.9.2a (10.9.2.1) on page 12



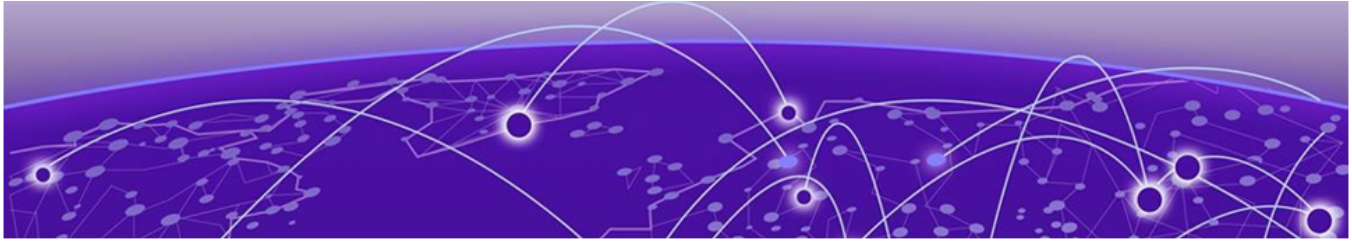
New Features in Release 10.9.2a (10.9.2.1)

There are no new features in this release.



Addressed Issues in Release 10.9.2a (10.9.2.1)

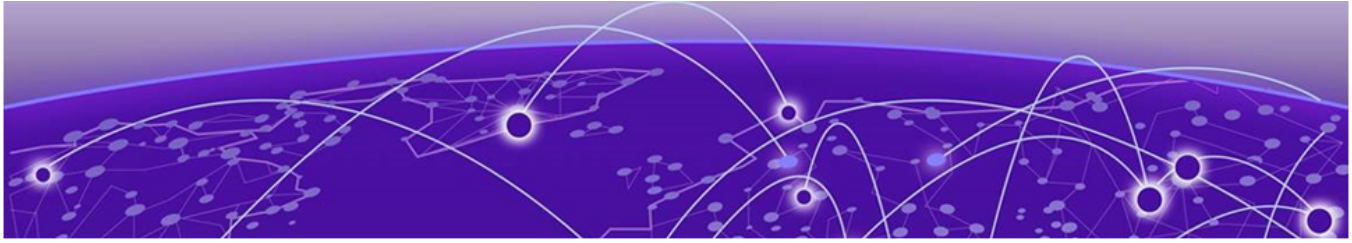
Release 10.9.2a (10.9.2.1) upgrades the embedded PHP runtime to version 8.4.27 to address CVE-2026-109618 and CVE-2026-109619, which could allow remote code execution through the web UI.



Known Issues in Release 10.9.2a (10.9.2.1)

Table 1: Known issues

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 10.9 Releases

Release 10.9.1 New Features and Addressed Issues on page 13
Release 10.9.2 New Features and Addressed Issues on page 15

The following sections provide information about changes for earlier IQ Engine 10.9 releases.

Release 10.9.1 New Features and Addressed Issues

New Hardware Support

Release 10.9.1 adds support for the AP3020W.

New Features in 10.9.1

Table 2: New features

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/AP5022S6D.
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 10.9.1

Table 3: Addressed issues

Issue ID	Description
CFD-17330 (03273228)	Addressed the issue where the `show interface wifi` 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 `show station` 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.
HOS-25465	Addressed the issue where the log message `ah_dcd_show_fa_map_db: get fa map db on iotgw failed` 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.

Table 3: Addressed issues (continued)

Issue ID	Description
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.

Release 10.9.2 New Features and Addressed Issues

New Hardware Support

There is no new hardware supported for Release 10.9.2.

New Features in 10.9.2

Feature ID	Description
HOS-25885	The 5 GHz radio of an AP5020 access point retrieves 6 GHz neighbor information from the Reduced Neighbor Report (RNR) element during background scanning and includes this information in its own RNR.
HOS-23945	A client IP address pool configuration option, previously available for VPN Gateway Virtual Appliance (VGVA) deployments, is available for use with Tunnel Concentrator and access point deployments.
HOS-23931	MTU detection between an access point and the Tunnel Concentrator uses ICMP-based keep-alive messages to verify configured MTU sizes for GRE and GRE over IPsec tunnels. The access point performs detection in the data plane before IP assembly, and reports detected MTU mismatches.
HOS-20322	A cloud-managed access point forwards RADIUS and other authentication traffic to the Tunnel Concentrator over standard GRE or GRE over IPsec tunnels. Administrators define a Client Tunnel IP address range, consistent with VPN Gateway Virtual Appliance (VGVA) deployments, for use as the source IP address of RADIUS requests sent through an IPsec tunnel.

Addressed Issues in 10.9.2

Issue ID	Description
CFD-17958 (03262604)	Addressed the issue where the 6 GHz radio of an AP5020 access point ran out of memory, causing the AP to stop accepting new client associations.
CFD-17940 (03302215)	Addressed the issue where an access point continued to use a cached DNS resolution for a RADIUS server hostname after a DNS failover changed the server's IP address, causing RADIUS authentication to fail until the AP was rebooted.

Issue ID	Description
CFD-17931 (03301989)	Addressed the issue where the **ML Insight** > **Network** page displayed network usage significantly higher than actual traffic for AP4020, AP5010, and AP5020 access points running IQ Engine 10.8.5 or later.
CFD-17809 (03297377)	Addressed the issue where an AP4060 access point experienced a kernel panic and rebooted during a 6 GHz scan while running IQ Engine 10.8.5.4.
CFD-17385 (03281486)	Addressed the issue where the client count displayed in ExtremeCloud IQ and Extreme Platform ONE Networking was incorrect for AP5020 access points when the username of a connected client included a domain separator, such as `domain\username`.
CFD-16657 (03246632)	Addressed the issue where ExtremeCloud IQ displayed the channel and power settings for all AP3000 access points as AUTO instead of the actual values.