Extreme Platform ONE Networking v25.10.0-224 (Hotfix 1) Release Notes

New Features, Limitations, and Known Issues

9041098-01 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/

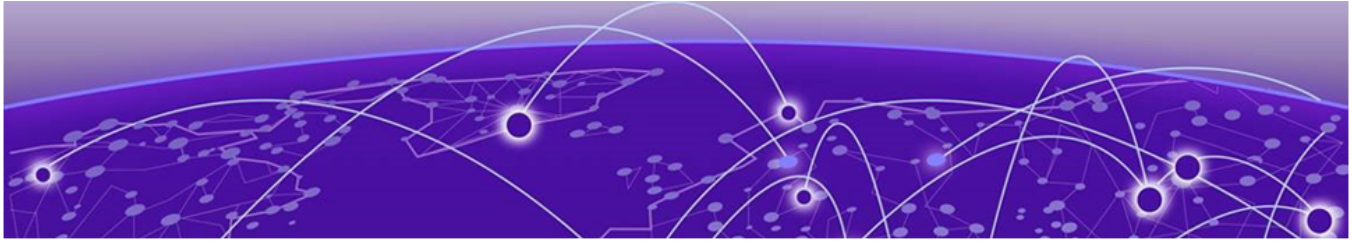
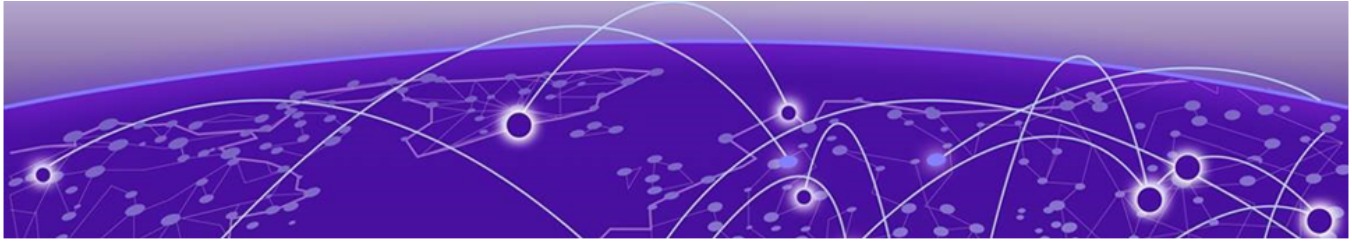


Table of Contents



Abstract

This release notes document for Extreme Platform ONE Networking version 25.10.0-224 (Hotfix 1) provides a technical overview of a cloud-based network management platform integrating ExtremeCloud IQ, SD-WAN, security, analytics, and third-party device management within a unified interface. It details core functionality such as centralized monitoring, inventory control, firmware lifecycle management, SSO-based access, AI-assisted diagnostics, alerting, and cross-domain topology visualization, with guidance for onboarding, configuration deployment, licensing, and large-scale operations. In this release, Extreme Platform ONE has made improvements to its Role-Based Access Control (RBAC) functionality. The document highlights new features including enhanced Third-Party Management Engine support, expanded Device 360 views, Fabric Attach visualization improvements, real-time troubleshooting for Wi-Fi 7 access points, RadSec-based secure authentication, automated configuration push, and expanded OS and firmware compatibility across EXOS, VOSS, and IQ Engine platforms. It summarizes addressed defects and known issues affecting APIs, RBAC, UI behavior, and topology accuracy, and outlines limitations in visualization, scalability, and unsupported topologies, along with firmware requirements, security considerations, and interoperability constraints for advanced administrators.

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

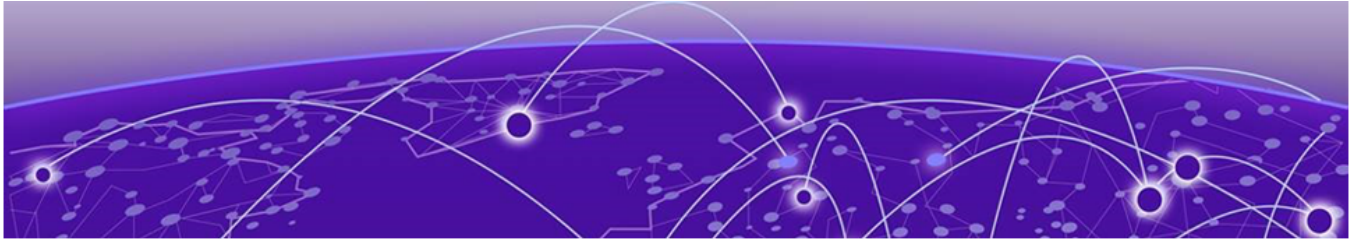
Subscribe to Product Announcements

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

Current Release: 25.10.0-224 (Hotfix 1)

May 2026

Extreme Platform ONE has made improvements to its Role-Based Access Control (RBAC) functionality.

Related Links

- Known Issues on page 26
- Device Support Information on page 35

Release: 25.10.0-224

May 2026

This release provides new features including enhanced Third-Party Management Engine support, expanded Device 360 views, Fabric Attach visualization improvements, real-time troubleshooting for Wi-Fi 7 access points, RadSec-based secure authentication, automated configuration push, and expanded OS and firmware compatibility across EXOS/Switch Engine, VOSS/Fabric Engine, and IQ Engine platforms.

This release provides support for a range of values for port range and IP Address range when configuring a Firewall rule. See Firewall Enhancement: Port and IP Address Range (CFD-17230) on page 10 for more information.

Related Links

- Known Issues on page 26
- Device Support Information on page 35

Introduction to Extreme Platform ONE Networking

The following are a few key features:

- Comprehensive UI: Provides access to alerts, licensing details, inventory, and firmware updates.
- Alerts and Notifications: Find and fix problems quickly. Real-time notifications ensure you receive prompt notifications about system updates and security notices.
- Contextual AI Support: Meet your AI Expert-your contextual helper. Powered by the latest in AI technology, AI Expert provides instant support and guidance, ensuring you have the answers you need, when you need them.
- Single Sign-On (SSO): Access Extreme Platform ONE Networking applications with a single sign-on, removes the need for multiple credentials.

Extreme Platform ONE Public IP Address Blocks

Data Center	IP Block	Addresses and Ports
Global Data Center (GDC)	44.234.22.92/30 18.194.95.0/28 34.253.190.192/26 3.234.248.0/27	
Australia (AUS)	13.210.3.192/28 18.98.198.80/28	Firewall Address and Port Information
Azure, Canada Central (ACA)	20.151.64.48/28	Firewall Address and Port Information
Azure, US East (AVA)	52.226.89.112/28	Firewall Address and Port Information
Brazil (BR)	18.228.70.16/28	Firewall Address and Port Information
Germany (FRA)	3.67.81.96/27 18.194.95.0/28	Firewall Address and Port Information
India (IN)	13.232.67.8/29 3.6.70.64/29	Firewall Address and Port Information
Ireland (IE)	34.253.190.192/26	Firewall Address and Port Information
Japan (JP)	18.176.203.112/29 13.231.6.232/29 57.181.58.0/28	Firewall Address and Port Information
Netherlands (NL-GCP)	34.91.82.64/27	Firewall Address and Port Information
Singapore (SG-GCP)	34.87.158.80/28	Firewall Address and Port Information
Spain (ES)	18.101.49.128/27	Firewall Address and Port Information
Sweden (SE)	13.48.186.224/29 13.48.4.184/29 13.48.4.240/28	Firewall Address and Port Information

Data Center	IP Block	Addresses and Ports
Switzerland (ACH)	51.107.1.192/28	Firewall Address and Port Information
United Arab Emirates (UAE)	3.28.159.128/28	Firewall Address and Port Information
United Kingdom (UK-AGB)	51.143.233.80/28	Firewall Address and Port Information
US East (VA)	34.202.197.0/26 44.192.245.0/26 3.234.248.0/27	Firewall Address and Port Information
US East 2 (VA2)	34.202.197.0/26 44.192.245.0/26 3.234.248.0/27	Firewall Address and Port Information
US-Iowa (IA-GCP)	34.67.130.64/27	Firewall Address and Port Information
US Ohio (OH)	3.145.235.64/26	Firewall Address and Port Information

Supported Applications

Extreme Platform ONE Networking eliminates the need to log in separately to the Extreme Networks multi-domain network management solutions by unifying them within a single user interface.

For example, if you subscribe to ExtremeCloud IQ, and have a site, you can view all connected sites and onboarded devices from ExtremeCloud IQ and Extreme Platform ONE Networking.

Note
The applications available when you log in are specific to the subscription licenses purchased by your organization. Access to applications might also be defined by the role assigned if your organization implements Single Sign-On.

Extreme Platform ONE Networking supports the following applications:

- ExtremeCloud IQ: Provides centralized configuration and network monitoring, reporting, alarms, and statistics for Extreme Networks devices.
- ExtremeCloud SD-WAN: Provides unified wired and wireless management through fabric services. You can enable a secure network, automate application performance management, and create a centralized management of applications with intuitive user experiences.
- Extreme Platform ONE Security: Provides network, application, and device access security within a single solution.
- Extreme Intuitive Insights: Provides cloud-based deployment and monitoring of Zebra hand-held devices.

Browser Support and Display Settings

Note
Extreme Platform ONE does not support 32-bit browsers.

Desktop Browsers

Extreme Platform ONE supports the latest 64-bit versions of the following desktop browsers:

- Chrome
- Edge
- Firefox
- Opera
- Safari

Microsoft Internet Explorer is not supported.

Display Settings

Extreme Platform ONE supports display resolutions of 1280 x 1024 or higher.

Firewall Enhancement: Port and IP Address Range (CFD-17230)

Extreme Platform One and ExtremeCloud IQ v25.10 support a range of values for port range and IP Address range when configuring a Firewall rule. This feature eliminates the need for multiple rules to cover a range of values.

Port Range

The Port Range feature behaves as designed. Range support is offered in the user interface and in IQ Engine, and it works as expected. Go to **Common Objects** > **Network** > **Network Services**.

IP Address Range

Configuring IP Address range is release 25.10 requires the following caveats:

- Range Support is offered in the user interface, but range support is not supported in IQ Engine.
- The current implementation uses legacy firewall CLI syntax, which forces a 64 object firewall entry limit.

Note
The IP Address range must not exceed 64 objects. This includes the aggregate value when configuring more than one firewall rule.
This translation adds back-end load and therefore, it can cause task-engine memory exhaustion.

Go to **Common Objects** > **Security** > **IP Firewall Policy**.

Configure User Profile Firewall Rule

Use this task to configure a port range and IP Address range in a firewall rule.

Note
Follow this workflow carefully. Practice creating the range objects described below.

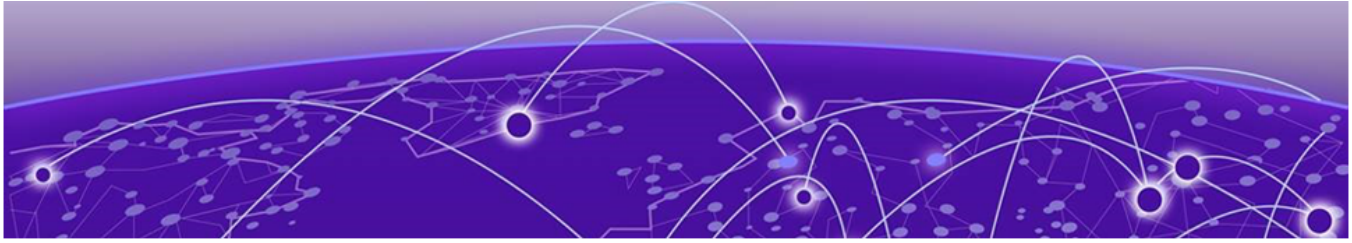
1. Create a User Profile and provide a Profile Name.
2. Enable the firewall and provide a Firewall Name.
3. Select **+** to create a new rule.
4. Select **+** to create a new Network Service.

Port Range

5. From the **Port Number** field, configure a port range. The full range is supported.
6. Save the object.

IP Address Range

7. Select and edit the firewall rule.
8. Create the **Source range** object and save.
9. Create the **Destination range** object and save.
10. Go back and edit the firewall rule.
11. From the drop-down menu, select the source and destination objects you created above to configure the source and destination ranges for the firewall rule.
12. Save the firewall rule.



New Features

Table 1 on page 13 lists the new features introduced in Extreme Platform ONE Networking release 25.10.0-224.

For more information about Extreme Platform ONE Networking features, see the Extreme Platform ONE Networking v25.10.0 User Guide.

Device OS Support

This release supports the following device operating systems.

- EXOS/Switch Engine:
  - IQAgent Version
    - EXOS/Switch Engine release < 31.7: upgrade to IQAgent version 0.9.32
    - EXOS/Switch Engine release >= 31.7 < 33.2 upgrade to IQAgent version 0.9.41
    - EXOS/Switch Engine release >= 33.2 upgrade to IQAgent version 1.9.41
  - 33.5.2.118-patch1-6 Latest Supported GA Patch

    Onboard, Monitor, Config, Image Mgmt, and Global Download Support
  - 33.6.1 Latest Supported GA Image

    Onboard, Monitor, Config, Image Mgmt, and Global Download Support
  - 32.7.3.15-patch1-33 Previous Supported GA Patch

    Onboard, Monitor, Config, Image Mgmt, and Global Download Support
  - 32.7.3.15-patch1-33 Previous Supported GA Image

    Onboard, Monitor, Config, Image Mgmt, and Global Download Support
- VOSS/Fabric Engine:
  - 0.9.41 IQ Agent Support
  - 9.4 Latest Supported GA Image

    Onboard, Monitor, Config, Image Mgmt, and Global Download Support
  - 9.2.3 Previous Supported GA Patch

    Onboard, Monitor, Config, Image Mgmt, and Global Download Support
  - 9.2.1.1 Previous Supported GA Image

    Onboard, Monitor, Config, Image Mgmt, and Global Download Support
- IQEngine Support:
  - IQEngine release 10.8.7

New Hardware Support

Extreme Platform ONE Networking now supports the following hardware:

- AP5022, AP5022FX, and AP5022S6D access points
- AP5060U and AP5060D access points

Table 1: New Features in release 25.10.0-224

Feature ID	Feature	Description
NVO-12980	Visualization Enhancements	Multiple enhancements are delivered to Visualization: (1) The Link Inspector for standard links displays a Mode property with Trunk/Access values; for link aggregation links, it displays a Trunk property with Tagged/Untagged values. (2) **Terminal** is renamed to **SSH Session**. (3) Visualization legends in **Access**, **Physical**, and **Fabric** views replace the Third-Party Management Engine (TPME) Managed Device entry with a link to the User Guide for all device icons. (4) Selected text color in the SSH Session light theme is improved. (5) The tooltip text Select Layers is updated to Select View or Layer(s).
NVO-13194	Tagging and Masking Operations for Third-Party Management Engine-Managed Devices	Third-Party Management Engine (TPME)-managed devices on Access and Physical visualization maps now support tagging and masking operations. The Add Tag, Copy Tag, Paste Tag, and Mask Device actions can be applied to TPME-managed devices. Mask Link and Unmask operations are also supported for links involving TPME-managed and discovered devices.
NVO-13383, NVO-13384	Configuration Enhancement for SNMP Timer	In the Edit Assignment and Assignment dialogs, **Location** now displays instead of **Site**, and the **Current Assignment** column is now visible.
NVO-15269	Discovered is Replaced with Detected	In Visualization, the term Discovered is replaced with Detected when referring to LLDP-discovered devices. The update applies to the **Access View Legend**, **Physical View Legend**, and **Fabric View Legend**.
NVO-15270	Initiate Discovery Renamed to Update Topology	The **Initiate Discovery** action in the **Visualization** section is renamed to **Update Topology** at both the Floor and Building levels. Related toast messages are updated to reflect the new terminology.

Table 1: New Features in release 25.10.0-224 (continued)

Feature ID	Feature	Description
SEN-566	User Interface Enhancement	The Third-Party Management Engine (TPME) status command now provides clearer onboarding information after system restarts. Previously, the Last Onboard Time displayed `Never` after a reboot, which was misleading for devices that had been successfully onboarded before the restart. The enhanced status display now accurately reflects onboarding state by displaying `Not Onboarded Since Restart` and `No Healthcheck Since Restart` respectively until TPME reconnects to the platform.
XCP-6331	Search Capability for the Sites Page	Extreme Platform ONE Networking now includes a search capability for the **Sites** page. Users can search for site groups, sites, buildings, and floors. The search returns all matching occurrences and uses smart forward-typing search, consistent with ExtremeCloud IQ (Classic).
XCP-8304	Onboarding Using an XLSX File Support	Extreme Platform ONE Networking now supports bulk onboarding of locally managed (on-premises) devices using an XLSX file. The XLSX file includes an **Access Points** tab (Serial Number, Hostname, Static IP, Default Gateway) and a **Controller** tab for on-premises appliances (ExtremeCloud IQ-SE, Wing Controller, ExtremeCloud IQ-Controller). For the **Controller** tab, Serial Number and MAC address are mandatory.
XCP-14259	Onboarding of Locally Managed Devices for ExtremeCloud IQ Controller	Extreme Platform ONE Networking now supports onboarding of locally managed (ExtremeCloud IQ Controller-managed) devices via manual and bulk methods. Serial Number is the only mandatory field. No configuration such as location or network policy can be applied during onboarding. Serial number validation follows the same rules as Universal APs.
XCP-14449	Manual and Bulk Onboarding of the AP5022 Access Point	Extreme Platform ONE Networking now supports manual and bulk onboarding of the AP5022 family (AP5022, AP5022FX, and AP5022S6D) as locally managed devices. After onboarding, devices appear in **Network Devices** and **Inventory** with Managed By: Controller and OS Type: Controller Engine.
XCP-15124	Onboarding Flow Enhancement	The onboarding flow is updated with the following changes: the **Onboard** button is renamed to **+Add Devices**; the **Bulk** dropdown option is renamed to **Import** and **Manual** is renamed to **Manually**; the stepper is removed from the Import flow; a link to download the XLSX template file is added to the Import flow; and the Device Type dropdown option **Access Point** is renamed to **IQ Engine**.

Table 1: New Features in release 25.10.0-224 (continued)

Feature ID	Feature	Description
XCP-16600	Entire Location Tree Export Support	Extreme Platform ONE Networking now supports exporting the entire location tree from the top level. Previously, export was available only at the site group, site, and building levels. The complete location tree can be exported for migration to another account.
XCP-16607	AP5022 Access Point Support	Support is now offered for AP5022, AP5022FX, and AP5022S6D access points as cloud-managed devices. These devices can be onboarded manually or in bulk, with devices appearing in the **Network Devices** and **Inventory** pages as cloud-managed with the IQ Engine operating system type. While onboarding is blocked in ExtremeCloud IQ Classic, monitoring and statistics remain available in ExtremeCloud IQ Classic.
XCP-16608	AP5060 Access Point Support	Support is now offered for AP5060U and AP5060D access points as cloud-managed devices. These devices can be onboarded manually or in bulk, with devices appearing in **Network Devices** and **Inventory** pages as cloud-managed with the IQ Engine operating system type. While onboarding is blocked in ExtremeCloud IQ Classic, monitoring and statistics remain available in ExtremeCloud IQ Classic.
XCP-16609	Manual and Bulk Onboarding for the AP5060 Access Point	Support is now offered for manual and bulk onboarding of the AP5060 access point as a locally managed device. After onboarding, devices appear in **Network Devices** and **Inventory** with Managed By: Controller and OS Type: Controller Engine.
XCP-17335	Product Family-Filtered PSIRT List	PSIRT (Product Security Incident Response Team) advisories filtered by the customer's actual product inventory are now displayed instead of showing all PSIRTs across every Extreme Networks product family. This enhancement provides more relevant security information by limiting the PSIRT list to only those advisories applicable to products in the customer's environment. The filtered view ensures accurate PSIRT counts and eliminates irrelevant security advisories, improving the efficiency of security vulnerability management.
XCP-17874	Guest Management Role Support	A dedicated Guest Management role is now offered that provides exclusive access to guest management tasks and credential distribution. This role grants direct access to **Config** > **Network** > **Users** and **Config** > **Network** > **User Groups**, and includes SSO/IDP enhancements that allow administrators to map a primary role to Guest Management through attribute mapping. Guest Management users have a streamlined interface without the 9-dot app switcher or notification bell icon to maintain focus on guest-related tasks.

Table 1: New Features in release 25.10.0-224 (continued)

Feature ID	Feature	Description
XCP-19941	Third-Party Management Engine IPv4 Subnet Discovery Validation	The Third-Party Management Engine (TPME) now validates IPv4 subnet masks during SNMP discovery to prevent invalid configurations. The system now blocks discovery attempts using /31 or /32 subnet masks, as these configurations contain no valid host addresses for discovery (only network and broadcast addresses). Previously, discovery would appear to proceed but silently fail with no user feedback, potentially leaving discovery sessions in a stuck state. The enhanced validation provides immediate feedback to users, ensuring only valid subnet ranges are used for device discovery operations.
XCP-21326	Inventory Page Button Label Update	The **Inventory** page now features an **Add Device** button, replacing the previous **Onboard** label for improved clarity and consistency. This terminology change provides a more intuitive description of the action, and makes it clearer that devices are being added to the inventory.
XIQ-33345	IQ Engine Support for Port and IP Ranges in Firewall Rules	IQ Engine now supports port and IP ranges in firewall rule configuration, allowing administrators to define a range of ports in a single rule instead of entering each port individually.
XIQ-35549	IQ Engine Support	IQ Engine version 10.8.7 is now supported.
XIQ-44189	IEEE 802.3az Standard Support	The IEEE 802.3az standard (Energy Efficient Ethernet) is now supported on the AP305C/X, AP410C, AP460C, AP460S6C, AP460S12C, AP510C, and AP510X access points.
XIQ-45854	Client Mode Configuration Improvement	Client Mode configuration now includes a NAT enable/disable toggle in the device template and device configuration. When NAT is disabled, the default DHCP server and scope are also disabled, enabling use cases where devices on a Client Bridge require direct reachability from the uplink network.
XIQ-46616, XIQ-48967	Direct RadSec Tunnel Configuration Support	Extreme Platform ONE Networking and ExtremeCloud IQ now support direct RadSec tunnel configuration for ExtremeCloud Universal ZTNA (UZTNA) authentication on AP3000, AP5000, and Wi-Fi 7 access point series. Administrators can enable UZTNA on an SSID using the "Authentication with ExtremeCloud Universal ZTNA" toggle in the SSID settings. The UZTNA root CA, intermediate CA, and client certificate are automatically deployed to access points. This capability coexists with the existing IDM tunnel, enabling PPSK to continue functioning while UZTNA reduces authentication latency.

Table 1: New Features in release 25.10.0-224 (continued)

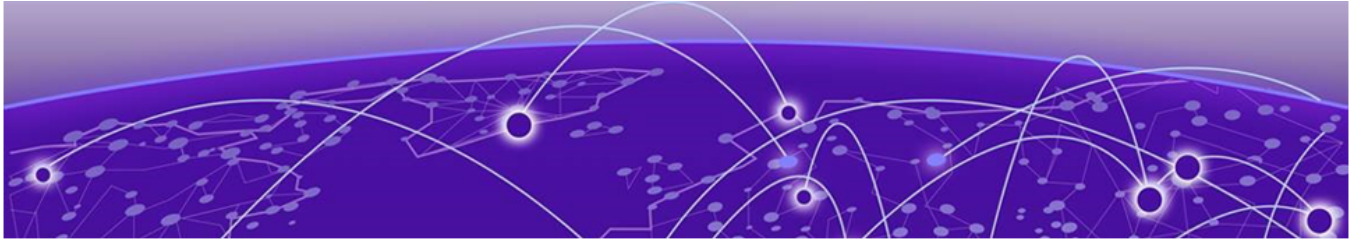
Feature ID	Feature	Description
XIQ-47128	Real-Time Troubleshoot Support	Real-Time Troubleshoot (RTTS) now supports the AP5020 and AP4020 series Wi-Fi 7 access points, expanding coverage beyond the previously supported AP3000, AP3000X, AP5010, AP5050U, and AP5050D platforms.
XIQ-47402	Power Profiles and Software Modes of Operation for AP5060	Power profiles and software modes of operation are now defined for the AP5060U-WW and AP5060D-WW access points. Both models share the same power profiles and support tri-radio scan software modes with 2.4 GHz, 5 GHz, and 6 GHz radio configurations under both 802.3bt and 802.3at power standards.
XIQ-47404	Power Profiles and Software Modes of Operation for AP5022	Power profiles and software modes of operation are now defined for the AP5022-WW, AP5022FX-WW, and AP5022S6D-WW access points. All three models share the same power profiles and support tri-radio scan software modes with 2.4 GHz, 5 GHz, and 6 GHz radio configurations under both 802.3bt and 802.3at power standards.
XIQ-47766	Automatic Configuration Push to Offline Devices Upon Reconnection	Support is now offered for automatic configuration push to offline devices upon reconnection. Administrators can enable or disable this feature at the VIQ level using the `Automatically apply the latest configuration to offline devices at reconnect` setting, which is off by default. When enabled, offline devices can be selected alongside online devices in **Manage** > **Devices** for a configuration update. Offline devices display a `Pending Config` status until they reconnect and receive the latest configuration. A public API is available for this functionality.
XIQ-47891	Client Lock Out Alert	Extreme Platform ONE Networking and ExtremeCloud IQ now generate an alert when a client is locked out. The `Client locked out` alert event integrates with the Alert Service and Notification Service, enabling delivery of lockout notifications to external systems through webhook or email. This feature applies to cloud PPSK users only. Local PPSK authentication is handled on-device and does not go through the cloud, so local PPSK clients are not in scope for lockout detection or alerting.

Table 1: New Features in release 25.10.0-224 (continued)

Feature ID	Feature	Description
XIQ-47810	VLAN Probe for Multiple Concurrent Devices	Support is now offered for VLAN Probe for multiple devices simultaneously. Previously limited to single device operations, the VLAN Probe diagnostics can now be executed across multiple selected devices at the same time. This enhancement streamlines network troubleshooting by allowing administrators to validate VLAN configurations and connectivity across multiple switches or access points in a single operation.
XIQ-48204	Client Density Map Type	A new Client Density map type is available, that displays current and historical client density across floor areas. The map divides floors into color-coded squares representing four configurable density ranges, with default thresholds that can be customized to match the environment. Hovering over any square displays the exact client count in that area, and can access historical density data for up to 90 days in one-day increments with animated playback similar to weather radar maps. This feature is available only when Client Location is enabled.
XIQ-48205	Client Path Tracking and Last Known Location Visualization	Support is now offered for client path tracking and last known location visualization. Client Path action can be accessed from the **Inventory** > **Clients** to view a client's movement over the last 24 hours by default, with the ability to view historical paths for up to 90 days in one-day increments. The feature supports both connected clients (displayed by default) and disconnected clients (accessible through a separate tab with search functionality requiring at least two characters of the MAC or hostname). Last known location information is retained and displayed on maps for up to 90 days, with search results limited to 20 matching records before requiring refinement.
XIQ-48334	Indoor Automated Frequency Coordination Support	Indoor Automated Frequency Coordination (AFC) is now supported on the AP5022, AP5022FX, and AP5022S6D access points.
XIQ-48811	Multi-Link Operation (MLO) with Enterprise Security mode Support	Extreme Platform ONE Networking and ExtremeCloud IQ now support enabling Multi-Link Operation (MLO) with Enterprise security mode for the AP4020 access point. The MLO enable/disable configuration option is now available when Enterprise security mode is selected.
XIQ-49278	Enable ExtremeGuest Essentials Renamed	In **Open SSIDs**, the toggle previously labeled **Enable ExtremeGuest Essentials** is renamed to **Enable Guest Access** and is now always visible, even when Guest Access is not enabled in **Global** > **Service Management.**.

Table 1: New Features in release 25.10.0-224 (continued)

Feature ID	Feature	Description
XIQ-49396	Maps Support for AP5022	Maps now support the AP5022 family (AP5022, AP5022FX, AP5022S6D) and the AP5060 family (AP5060D, AP5060U). Antenna pattern support for these families is not included.
XIQ-49990	Legacy/Third Party Tab Renamed	In **Clients**, the **Legacy/Third Party** tab is renamed to **Discovered**.
XIQ-47935	VOSS/Fabric Engine Support	Support is now offered for Fabric Engine/VOSS 9.4 for onboarding, monitoring, configuration management, and image drag-and-drop on supported Universal Switches, VSP7400, and VSP4900 platforms. Users can downgrade to a previous image, including the IQAgent image, without GTAC engagement.
XIQ-47949	EXOS/Switch Engine 33.6 GA Download Support	Support is now offered for global image download for EXOS/Switch Engine 33.6 for all supported EXOS/Switch Engine SKUs, both single and stacked. The following images are available in the download dropdown: 31.7.4.2-patch1-7, 32.7.3.15-patch1-33, 33.5.2.118-patch1-6, and the latest 33.6. No other images are available.
XIQ-49264	EXOS/Switch Engine 32.7.3.15-patch1-54 GA Download Support	Support is now offered for global image download for EXOS/Switch Engine 32.7.3.15-patch1-66 for all supported EXOS/Switch Engine SKUs, both single and stacked. The following images are available in the download dropdown: 31.7.4.2-patch1-7, 32.7.3.15-patch1-33, 33.5.2.118-patch1-6, and 33.5.2. No other images are available.



Addressed Issues

Table 2 lists Addressed Issues in Extreme Platform ONE Networking release 25.10.0-224.

Table 2: Addressed Issues in release 25.10.0-224

Issue ID	Description
9-dot Menu	
XCP-3475	Addressed the issue where the 9-dot menu switcher returned 401 **no access** errors when redirecting to SD-WAN, UZTNA, and Extreme Intuitive Insight applications, despite the tenant having valid licenses for all applications.
Account Management	
WS-4174	Addressed the issue where switching to or directly logging in to an account displayed a blank screen instead of loading the account.
API	
XCP-17277	Addressed the issue where file downloads exceeding 1 GB failed when using the common-api-gateway URL.
XCP-17607	Addressed the issue where the Start Discovery API returned an incorrect error response when the request payload contained more than 10 individual IP addresses. The API now returns a clear error message indicating the maximum limit of 10 IP addresses per request.
XCP-17687	Addressed the issue where the Add Discovered Devices API returned an incorrect response schema when mandatory fields were missing. The API now returns a proper 400 validation error instead of accepting invalid data with a 200 response.
XCP-19541	Addressed the issue where DLCS APIs returned 403 Forbidden errors for users with Observer and NetSecOps roles, which have read-only access permissions.
XCP-20577	Addressed the issue where the List Buildings API response payload did not match the OpenAPI specification.
XCP-20615	Addressed the issue where the listDevices API returned inconsistent fields across different items in the same response payload.
Browser Issues	

Table 2: Addressed Issues in release 25.10.0-224 (continued)

Issue ID	Description
XIQ-44593	Addressed the issue where the **AFC Status** and **GEO Location** widgets in the **AFC Wireless** View displayed graphical artifacts when viewed on MacBook Pro using Safari browser.
Device Management	
SEN-538	Addressed the issue where the Third-Party Management Engine (TPME) rebooted ungracefully when the redirector URL was reconfigured while TPME was actively connected to a different URL. TPME no longer triggers an OS-level reboot when the redirector URL is changed within a 10-minute window.
SEN-608	Addressed the issue where the CLI `device` command output incorrectly prepended a "TPME-" prefix to the serial numbers of Third-Party Management Engine-managed devices, while the `show support` command displayed the correct serial numbers without the prefix. The `device` command now displays serial numbers consistently without the "TPME-" prefix.
XCP-19598	Addressed the issue where editing a deployment at the device level did not exclude the device from the site-level schedule, causing the device to deploy at both the site-level and the device-level scheduled times.
XCP-19734	Addressed the issue where a device configured with an invalid or incompatible access profile did not transition to the disconnected state and remained in the connected state.
XCP-20907	Addressed the issue where importing a site group using an XML file failed with a **Country code missing** error.
XCP-21280	Addressed the issue where Third-Party Management Engine (TPME) devices discovered via the SNMPv2c profile were not added to the device list in the CLI or UI, despite discovery reporting as successful in the TPME-Agent pod logs.
Inventory	
XCP-18800	Addressed the issue where a managed device's status was not updated in the inventory when it reconnected after being disconnected. The inventory now reflects the correct device status upon reconnection.
Licensing	
WS-4079	Addressed the issue where newly registered customers could not navigate to the main page after linking their license.
XCP-8478	Addressed the issue where a 4-device stack displayed 2 devices as Active CoPilot and 2 devices in Grace Period instead of placing all 4 devices in Grace Period when the available CoPilot licenses were insufficient to cover the entire stack.
XCP-19376	Addressed the issue where certificate notification behavior was inconsistent with the **Days Remaining** value shown on the **Workspace** page. Certificates showing 2 days remaining now correctly trigger a notification.

Table 2: Addressed Issues in release 25.10.0-224 (continued)

Issue ID	Description
XCP-20014	Addressed the issue where SNMP Discovery with more devices than available licenses resulted in no devices being onboarded. Devices up to the available license count are now onboarded, and excess devices are added as UnManaged.
XCP-20691	Addressed the issue where Guest Management users received a "No license" page upon login despite the tenant having a valid active license.
XCP-21483	Addressed the issue where devices onboarded from ExtremeCloud IQ-SE without sufficient licenses displayed a status of **Managed** and **Not Required** instead of **Unmanaged** and **Not Licensed**.
XCP-21672	Addressed the issue where the Device Common Connector service did not push the Extreme Platform ONE Networking standard license to VOSS Wired switches running 9.4.0.0.GA. The capabilities and URLs transmitted by the switch exceeded the buffer limit, preventing the license patch command from being sent.
Logs	
XCP-16345	Addressed the issue where the audit log sequence for firmware upgrade events was incorrect. The firmware initiate message appeared before the processed log entry. The processed log entry now appears before the initiate message.
Onboarding	
SEN-568	Addressed the issue where the Third-Party Management Engine (TPME) operating system rebooted when the TPME container restarted twice within 10 minutes due to configuration changes such as hostname or redirector URL updates. After the OS reboot, onboarding failed due to a DNS resolution error caused by the container's `resolve.conf` file not being updated. TPME no longer triggers an OS-level reboot under this condition.
Roles	
WS-4095	Addressed the issue where several navigation menu items — including **Inventory**, **Subscriptions & Licensing**, and **Contracts** — were not visible to users assigned the BizOps role.
WS-4124	Addressed the issue where clicking the ExtremeCloudIQ logo caused screen flickering for BizOps role users instead of loading the Network Devices page.
XCP-19151	Addressed the issue where the NetSecOps role could create sites when the **All Sites Permitted By Role** permission was enabled. Site creation behavior for the NetSecOps role is now consistent with the intended design.
XCP-21152	Addressed the issue where Observer role users received a 403 error when navigating to the **Visualise** page despite having read-only view access.
Troubleshooting	

Table 2: Addressed Issues in release 25.10.0-224 (continued)

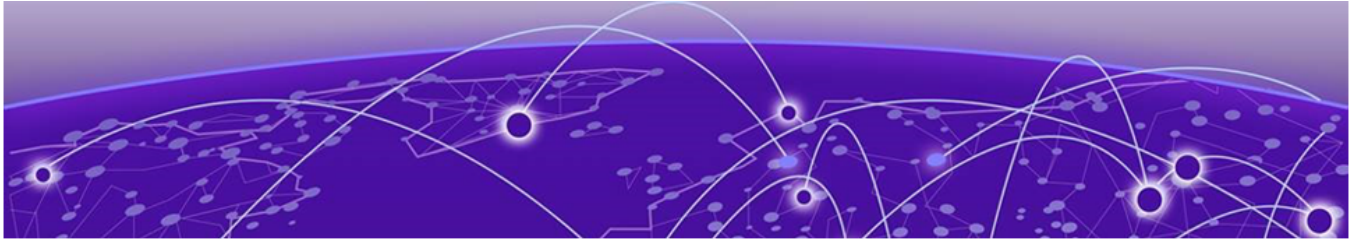
Issue ID	Description
SEN-520	Addressed the issue where the `show tpme proxy` command did not display the proxy password in masked format, leaving users unable to confirm that a password was configured. The password field now displays with masked characters (asterisks) when a proxy password is set.
SEN-616	Addressed the issue where the HTTP proxy configuration set via the CLI was not persisted after the session ended. Although the CLI displayed a `HTTP proxy configured successfully` message, the `show tpme proxy` command subsequently reported `No proxy configured`. The proxy configuration is now correctly retained and displayed after setup.
Upgrading	
XCP-17406	Addressed the issue where the Firmware Upgrade History and Download XLSX Template endpoints returned errors for users with the Observer role. Observer role users can now access these endpoints with read-only permissions.
User Interface	
WS-4021, WS-4022, WS-4024	Addressed the issue where the **Integration**, Third-Party Management, and Reports page failed to load in the ExtremeCloud IQ platform.
XCP-18627	Addressed the issue where the **Schedule Deploy** window allowed selection of times less than 1 hour ahead or dates more than 7 days in the future. The schedule time selection now enforces a minimum of 1 hour and a maximum of 7 days from the current time.
XCP-18697	Addressed the issue where the Third-Party Management Engine (TPME) operating system version was not displayed on the Device 360 page despite the API response containing the correct firmware version information.
XCP-18925	Addressed the issue where the total device count was not displayed in the **Delete Access Profile** confirmation window, even though the window listed all devices assigned to the profile.
XCP-18982	Addressed the issue where the displayed device selection count did not match the actual number of selected devices when devices were selected across multiple pages.
XCP-19116	Addressed the issue where a modal on the **Device 360** page displayed an unnecessary vertical scroll bar despite sufficient empty space being available below the table content.
XCP-19182	Addressed the issue where Link In/Out statistics displayed as zero for links between Third-Party Management Engine-managed switches and cloud-managed access points, despite correct statistics being available through SNMP.

Table 2: Addressed Issues in release 25.10.0-224 (continued)

Issue ID	Description
XCP-19330	Addressed the issue where no validation message was displayed in the user interface when saving CLI Credentials with a duplicate name, even though the API returned a proper error response.
XCP-19572	Addressed the issue where the **Link Type** field displayed as "Unknown" in topology view for links involving Third-Party Management Engine-managed devices. The **Link Type** field is no longer displayed for links that include Third-Party Management Engine-managed devices.
XCP-19443	Addressed the issue where **System Uptime** displayed as 0 for Third-Party Management Engine-managed Cisco switches in the visualization object inspector, despite the correct uptime value being available through SNMP.
XCP-19706	Addressed the issue where the **Profile Assignment** table displayed outside its container boundary, and the device assignment view flickered between the assigned device list and the **View Rules** text.
XCP-19995	Addressed the issue where navigation from a Third-Party Management Engine-managed device's Device 360 page to the Third-Party Management Engine Device 360 page failed to load on the first attempt.
XCP-20010	Addressed the issue where the **Device 360** page for an unmanaged Third-Party Management Engine (TPME) device displayed a "No device found" error. Unmanaging a TPME device no longer causes TPME-managed devices to become unmanaged or clears inferred device entries.
XCP-20196	Addressed the issue where the Access Management page failed to load.
XCP-20649	Addressed the issue where the industry selection made during user registration was not displayed in the summary section of the registration form.
XCP-20949	Addressed the issue where location-based search did not return results in the Access Profile assign and assigned views.
XCP-21111	Addressed the issue where the user interface did not display updated assignment details after an SNMP Timers assignment action. The user interface now retrieves the latest assignment status after the action completes.
XCP-21235	Addressed the issue where switch devices appeared in the Profile Assignment table when they should be excluded. Profile assignment and deployment are not supported for switch devices.
XIQ-48575	Addressed the issue where the **VLAN Override** option was incorrectly displayed on the **PPSK User** page when the Local (AP) database was selected. The **VLAN Override** option is supported only for Cloud PPSK and is no longer visible on the **Local** user page.

Table 2: Addressed Issues in release 25.10.0-224 (continued)

Issue ID	Description
XIQ-49108	Addressed the issue where launching Real-Time Troubleshoot from the **Client Inventory Heat Map** opened two simultaneous UI pop-up windows instead of one and hid the Start/Stop controls.
XIQ-49126	Addressed the issue where the **Action** drop-down in **Manage** > **Devices** remained disabled for Third-Party Management Engine (TPME) devices onboarded through Extreme Platform ONE Networking, preventing users from performing **Manage** or **Unmanage** actions.
Visualize	
NVO-15096	Addressed the issue where the Assign Location pop-up failed to display when selected from the Object Inspector for a TPME managed device in the Visualization page. The page displayed a loading indicator instead of the pop-up.
NVO-15628	Addressed the issue where a configuration push for a VLAN attribute failed when a VLAN with the same ID (but a different name) already existed on the switch. The VLAN is now successfully renamed to the name specified in the configuration profile, consistent with the default override behavior.



Known Issues

Table 3 lists the Known Issues in Extreme Platform ONE Networking release 25.10.0-224 (Hotfix 1).

Table 3: Known Issues in release 25.10.0-224 (Hotfix 1)

Issue ID	Description
CFD	
CFD-16439	IQ Engine v10.8.7 upgrade at the GDC is not supported at the RDC until full upgrade to Extreme Platform One v25.10. This issue will be addressed in a future release.
9-dot Menu	
XCP-10803, XCP-11090	Accessing applications from the 9-dot menu fails with Internal Server Errors.
API	
SEN-555	The state/system API returns a negative sysUpTime value for third-party devices with a system uptime exceeding approximately 248 days. This occurs due to a 32-bit integer overflow in the sysUpTime field. The Third-Party Management Engine (TPME) currently caps the reported sysUpTime at the maximum int32 value (2,147,483,647) to prevent negative values from being reported.
XCP-19243	The PerfMon API returns inconsistent and non-deterministic data schemas for legacy device types. Each legacy device type returns a different set of fields, and a unified schema mapping for legacy devices has not been established.
XCP-20428	Null values are returned for client IP address fields (client_ip and ipv4) in the wired client API response, even when an IP address is assigned and visible in ExtremeCloud IQ.
XCP-20647	The listDevice API returns the field "is_locally_managed" in the response payload, which is not defined in the API output specification.
XCP-20770	The asset summary/history API specification does not mark the request body as required in the OpenAPI specification.
XCP-20819	The ClientStats service sends the bwUsage field as an object containing avg, max, and min values instead of the required int64 format as defined in the specification.

Table 3: Known Issues in release 25.10.0-224 (Hotfix 1) (continued)

Issue ID	Description
XIQ-39330	The packet loss metric is incorrectly reported as a raw packet count rather than a percentage in both the API response and the user interface.
XIQ-48097	The Third-Party Management Engine (TPME) devices API accepts search queries with fewer than three characters and returns results instead of returning a 400 BAD_REQUEST response. The existing DLCM List device API enforces a three-character minimum for search queries. Additionally, the toast message for this validation is not displayed correctly.
XIQ-49961	The POST /ng-reports/scheduled/custom API returns a generic 400 BAD_REQUEST response without providing actionable validation details. The response does not identify which field failed validation, why the request was rejected, or what corrective action is required, making it difficult for API consumers to correct their requests.
Browser Issues	
WS-3841	Pages flicker when using Safari browser version 26.2 on macOS with an external monitor.
XCP-8507	An issue exists where the login button remains disabled even when the username and password fields are pre-filled.
Device Management	
XCP-5227, XCP-5268	Incorrect `Managed_by` value for locally managed devices.
XCP-12743	Bulk delete operations are limited to approximately 250-287 devices due to ExtremeCloud IQ API path parameter constraints. Larger bulk operations will require event-based design implementation for proper scaling.
XCP-13202	Security vulnerabilities are not displayed in the firmware upgrade flow for locally managed switches. Currently, locally managed devices are not in scope for PSIRTS vulnerability reporting.
XCP-16986	The end of sales and service dates are missing from the exported file when exporting stack details.
XCP-18164	Third-Party Management Engine device discovery is available even if no Configuration Profile is assigned. The Configuration Profile assignment is mandatory for the Third-Party Management Engine.
XCP-18640	The **Retry** action is disabled after the configuration deployment fails for the Third-Party Management Engine.
XCP-19055	The Reset VIQ action does not clear the configuration for the Third-Party Management Engine.
XIQ-19320	WiFi interface transmission power values may not update correctly in **Managed Device** page after bulk edit operations.
XCP-20011	Feature assignment is lost when the Third-Party Management Engine state is changed from managed to unmanaged. The features must be reassigned after the state change.

Table 3: Known Issues in release 25.10.0-224 (Hotfix 1) (continued)

Issue ID	Description
XCP-21131	The user-modified default Access Profile is not deployed to the Third-Party Management Engine in some situations.
XCP-21261	The Sites XML import functionality does not properly validate site hierarchy, allowing invalid XML files to be imported. Specifically, the import process accepts XML structures where a GENERIC location contains both SITE and BUILDING types as direct children, which violates the expected site hierarchy.
XCP-21263	When attempting to upgrade devices and filtering to show only locally managed devices, the device type field displays as empty and no devices are returned. This occurs even when locally managed devices exist and are onboarded in the system.
XIQ-19368	User interface overrides Supplemental CLI option incorrectly pushes Supplemental CLI configuration instead of UI configuration for multicast rate limit settings.
XIQ-19498	Changing transmission type for eth0 interface on AP5010 incorrectly generates delta CLI for speed configuration.
XIQ-19509	Configuring eth0 interface with minimum speed and half duplex transmission type causes AP to go offline.
XIQ-21339	ExtremeCloud IQ does not display error message when aggregation is enabled with rate-limit configuration, but configuration fails.
XIQ-33498	An issue exists where client mode and backhaul mesh link options need to be disabled on AP5050U/D 6GHz FCC configurations to ensure proper regulatory compliance.
XIQ-34724	An issue exists where delta configuration push fails for AP5020 Wifi0 with dual 5G mode when 5G-Low channels are not supported in countries like Pakistan.
XIQ-46182	An issue exists where the EXOS and Switch Engine 31.7.4.2-patch1-7 cannot be onboarded, monitored, or configured through drag-and-drop image management for all EXOS and Switch Engine ExtremeCloud IQ supported SKUs.
XIQ-46735	Auto configuration toggle in VIQ causes devices with audit match status to incorrectly move to audit mismatch state.
XIQ-46795	Stack hostname changes made in device CLI are not reflected in ExtremeCloud IQ interface.
XIQ-47278	AP5010 and AP5020 do not support 6 GHz in the Indonesia region.
XIQ-47962	Tunnel Concentrator retains the old IP address of an AP after the configuration is updated with a new IP address.
XIQ-47986	Location based SSID classification adds unnecessary AP information to Tunnel Concentrator configuration.
XIQ-49244	When creating an auto-provisioning policy for AP5060 access points, the IoT radio is enabled by default, which causes a "missing iot profile" error if no IoT profile is configured.
Inventory	

Table 3: Known Issues in release 25.10.0-224 (Hotfix 1) (continued)

Issue ID	Description
WS-2433	Inventory displays an SD-WAN appliance as Disconnected, but Orchestrator shows it as Connected. Also, Extreme Platform ONE Networking does not display the firmware of the SD-WAN devices.
XCP-10933	EOS/EOM details for wireless devices do not update in the device model mouse-over display and the Hardware Lifecycle widget. The widget shows no updates needed despite EOS/EOM devices being present in the inventory.
XCP-14975	Unassigned folders are displayed for non-admin users (NetSecOps, BizOps, or Observer roles) on the **Inventory** page when the site filter is selected.
XCP-17825	The Inventory is not immediately refreshed for the **Manage/ Unmanage** actions.
XCP-18242	A location assigned to multiple devices simultaneously is correctly reflected in the **Network Devices** table but not in the Inventory page, which continues to show the location as Unassigned for some devices.
XCP-19029	In **Configuration | Third-Party Management**, the Third-Party Management Engine is listed as assigned to the site even if the site was already deleted.
Licensing	
XCP-20454	When more Third-Party Management Engine devices are discovered than available licenses allow, the devices initially activate the available licenses but then transition to an unmanaged state. The activated licenses remain consumed in the backend even though the devices are in an unmanaged state.
Logs	
XCP-11224	The **Audit Log** displays API denied error log entries, which are not relevant.
XCP-16530	Audit logs are generated out of sequence when exporting a device.
XIQ-47371	Multiple logs are generated for both single and bulk device deletions.
MSP	
XCP-11254	Changing a user role from MSP Super Admin to MSP Admin removes their ExtremeCloud IQ Admin role.
XCP-11278	In the MSP view for the U.S. region, the **Switch Tenant** panel remains open and cannot be dismissed.
XCP-18891	The **Enterprise** view is displayed instead of the expected MSP tenant view when a user switches to or logs in as a tenant that has a linked legacy license account.
Onboarding	
WS-3579	A toast notification splits into two separate messages when a user performs a navigation action while a toast is active, such as during onboarding or device deletion operations.

Table 3: Known Issues in release 25.10.0-224 (Hotfix 1) (continued)

Issue ID	Description
XCP-17215	The failure toast "Device Failed to Onboard" disappears automatically after 10 seconds when a device onboarding attempt fails.
Roles	
CFD-16351, XCP-11511	An issue exists where Extreme Platform ONE Networking does not restrict admin visibility based on location, affecting only the Observer and the Operator roles.
XCP-10308	**Manage** or **Unmanage** actions are not performed for the NetSecOps role.
XCP-20938	BizOps users can successfully add a VOSS/Fabric Engine device on the **Network Devices** page but cannot see the added device on that page. The device only appears on the **Inventory** page.
XCP-21028	Creating both internal and external BizOps users is not possible when the RDC is running release 25.9.0 and the region is on release 25.10.0. The release difference between the RDC and region causes BizOps user creation to fail.
XCP-21032	BizOps users are unable to view Third-Party Management Engine (TPME) device details in the Device 360 (D360) page. When attempting to access the D360 page for TPME-managed devices, the page opens but displays no device data.
XCP-21282	SSO users with the Guest Management role cannot successfully create PPSK users and receive an `Access Denied` error when attempting to create accounts in user groups. This issue occurs when an SSO user is added to Credential Groups and then attempts to manage PPSK credentials.
XCP-21347	Users cannot create Guest Management role users in an RDC running release 25.9 after role mapping changes introduced in the 25.10 release. The role mapping changes are not backward compatible when the RDC remains on a lower build.
XCP-21527	An external user with the ExtremeCloud IQ Installer role is mapped to the Observer role in Extreme Platform ONE Networking instead of retaining the Installer role privileges.
XIQ-45333	Manage/unmanage actions are not working for Extreme Platform ONE Networking BizOps role users, showing "something went wrong" error.
XIQ-45477	An issue exists where Extreme Platform ONE Networking NetSecOps role users with Write access to inventory cannot perform Manage/Unmanage actions, resulting in permission errors.
SSO	
XCP-8507	The login button does not activate for certain SSO-enabled user login instances.
Troubleshooting	
XIQ-48210	Downloading the AFC Geolocation report produced a corrupt file that was not in the expected CSV format, making it unusable for troubleshooting.

Table 3: Known Issues in release 25.10.0-224 (Hotfix 1) (continued)

Issue ID	Description
Upgrading	
XCP-12063, XCP-12064, XCP-16651	An audit log is not generated for a scheduled a firmware upgrade, when a firmware upgrade successfully completes, or when a firmware upgrade fails.
XCP-12707	Individual level upgrade firmware screen does not display data properly once CVEs are expanded in the UI. This is dependent on EC1 team fixes for proper chip overflow behavior.
XCP-13051	While a firmware upgrade is in progress for a device in Extreme Platform ONE Networking it is deleted in ExtremeCloud IQ.
XCP-14211	The **Firmware Version** dropdown is not visible during a firmware upgrade when multiple APs are selected and the last device in the list is reviewed on high-resolution displays.
XCP-17804	After upgrading to 25R7, the schema registry service encounters 409 errors for the hm-device-stats-value and xiq-client-events-value topics. The affected schemas must be deleted before the registry service calls can succeed.
User Interface	
NVO-15001	Port Description in Link & Port details for devices managed by Third-Party Management Engine contain incorrect values.
WS-3923	The breadcrumb on the **Network Profile** page displays **Network Configuration / Network Policies** instead of only **Network Policies**, causing an inconsistency with the left navigation.
XCP-4999	Currently, when filtering on a switch stack, when a a search matches any child device, the entire stack is displayed instead of individual devices.
XCP-5065	**Search** and **Filter** does not filter the appliance cluster.
XCP-13806	Switching to the HomeVIQ tenant view causes most APIs, including the myaccount API, to fail with a 403 Forbidden error.
XCP-16957	The **Firmware Upgrade History** page displays a maximum of two filtered columns.
XCP-17326	Tables in the user interface refresh slowly when the pagination is set for 500.
XCP-18901	Sorting tables based on location results in incorrect results and error messages.
XCP-18963	The three-dots action icon is not visible by default in the **Network Devices** table and displays inconsistently across different device tabs.
XCP-19002	Fabric Attach links display as operationally down in the visualization even when they are operationally up. This issue affects Switch Engine downstream and SMLT Cluster upstream configurations that use Fabric Attach without authentication.

Table 3: Known Issues in release 25.10.0-224 (Hotfix 1) (continued)

Issue ID	Description
XCP-19039	**Device 360** page does not open if the same S/N is managed in the same RDC, but a different VIQ. Configuration assignment does not show the device in the selection if the same S/N is managed in the same RDC but a different VIQ.
XCP-19300, XCP-19301	"Uptime" and "Connected For" data is not available for devices managed by the Third-Party Management Engine in Network Devices.
XCP-18722	The error message is not formatted properly when a duplicate Access Profile is created.
XCP-18944	The Unknown tag can be assigned to a device managed by the Third-Party Management Engine in some cases.
XCP-19865	No failure details are displayed in the user interface when a Third-Party Management Engine configuration deployment fails. The deployment API response confirms a failed status but does not include a failure reason, and no corresponding audit log entry is generated.
XCP-20134	The filter chip for the Extreme Platform ONE Networking selection in the Application Access column filter in **Access Management** is not displayed, preventing confirmation that the filter has been applied.
XCP-20852	The Global Sites filter does not return sites in alphabetical order. Sites are currently sorted by creation time instead of alphabetically. Site Groups and search results within the filter are also not sorted alphabetically.
XIQ-42050	An issue exists where FIPS enabled filter in **Manage Application** page displays all applications instead of filtering to show only FIPS-enabled applications.
XIQ-42051	An issue exists where FIPS enabled filter in **Manage Summary** widget shows inaccurate data for **Top Application Groups**, **Top Usage**, and **Total Application Usage** metrics.
XIQ-46203	On the **Monitoring** > **Clients** > **Users** tab, the Source value displays Other instead of Others.
XIQ-47575	A new location does not appear in the **Users** page after a site is updated and filtering by the newly assigned site does not return the entry.
XIQ-47622	The Users grid XAPI request times out when the Status=Connected filter is applied to a dataset of approximately 148,000 user records.
XIQ-47708	The summary widgets on the Users page fail to load when the page contains approximately 500,000 user records.
XIQ-47942	DPcap events are not appearing on the **Client Monitor Diagnosis** page.
XIQ-48389	The user type count and connected users count do not match the total users count on the **Users** page.
XIQ-48217	The export option is unavailable in the **Other Devices** tab on the **Network Devices** page for Third-Party Management Engine-managed devices in the user interface.

Table 3: Known Issues in release 25.10.0-224 (Hotfix 1) (continued)

Issue ID	Description
XIQ-48218	Selecting **Configure** from **Network Devices** displays **Third Party Management** instead of **Configuration Profile**.
Visualize	
NVO-14730	Model for a device managed by the Third-Party Management Engine is Unknown in the Object Inspector.
NVO-14810	Devices that are managed by the Third-Party Management Engine can be displayed twice in **Visualization** when there is link aggregation between Cloud Native devices and Third-Party Management Engine managed devices.
NVO-14854	Devices that are managed by the Third-Party Management Engine can be displayed on the map as both a managed device and an LLDP discovered device at the same time.
NVO-14880	Data is unavailable for the Operational Ports in Object Inspector in **Visualization** for some devices that are managed by the Third-Party Management Engine.
NVO-15025	LLDP devices discovered through the Third-Party Management Engine do not support tagging.
NVO-15117	**Unmanage** causes inconsistency in the device count and topology display in Visualization for devices that are managed by the Third-Party Management Engine.
NVO-15250	Some devices that are managed by the Third-Party Management Engine have Partially Connected status in Visualization due to LLDP data discovery issues.
NVO-15304	Pushing an ISPP port change from Extreme Platform ONE Networking causes an unintended AAA RADIUS server reconfiguration on EXOS/Switch Engine 33.5 and later. For devices running EXOS/Switch Engine 32.7 using the HAC workflow, disabling the "Perform delta configuration update and resolve local device configuration which is out of sync with ExtremeCloud IQ" option is the current workaround.
NVO-15492	When a new LACP Link Aggregation Group (LAG) is created between two EXOS devices, the websocket connection does not automatically detect and display the new LAG on the network visualization canvas. The LAG configuration is correctly established on both devices with LLDP neighbors present, but the canvas continues to show the individual ports as down connections rather than displaying the aggregated link bundle.
NVO-15501	When a port is removed from an EXOS LACP Link Aggregation Group (LAG), the websocket connection does not detect the configuration change and the Inspector panel continues to display the original port count. After performing an **Update Topology** operation, the LAG status changes to *degraded* but the **Inspector** panel still incorrectly shows all original ports rather than reflecting the reduced port membership.

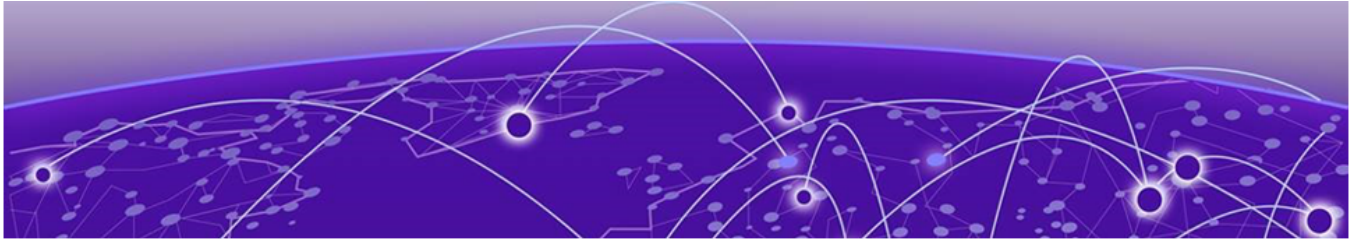
Table 3: Known Issues in release 25.10.0-224 (Hotfix 1) (continued)

Issue ID	Description
NVO-15660	A Link Aggregation Group (LAG) configured between an EXOS/ Switch Engine switch and an Access Point intermittently loses its LAG visualization on the network canvas and displays as a single link instead. The LAG configuration is correctly shown on both the EXOS/ Switch Engine device and the AP, but the visualization canvas fails to consistently represent the aggregated link bundle.
NVO-15689	The network visualization canvas does not automatically update to reflect the deletion of a Link Aggregation Group (LAG) between EXOS/Switch Engine devices. The LAG link continues to display on the canvas even after deletion and associated port disablement. Clicking on the orphaned LAG link generates a "unable to fetch physical link details" error message.

Limitations

Note the following caveats for this release of Extreme Platform ONE Networking.

- Trial Subscriptions are only available for Extreme Platform ONE Networking, Extreme Platform ONE Security, and ExtremeCloud SD-WAN.
- Support for Site-Engine managed devices that are connected to ExtremeCloud IQ is currently limited only to **Inventory**.
- Intermittent issue - the topology gets distorted while changing any node position.
- If all member ports are not in admin UP state, Visualize does not display LAG or MLT.
- Devices discovered through LLDP by Access Points (APs) are not displayed on the canvas in the Physical, Fabric, or Service views. However, they are visible in the Object Inspector.
- Wireless Mesh topology is not supported in the Physical, Access, or Fabric layer views.
- Outdoor sites are not supported in Visualization.



Device Support Information

Visualize does not show devices on topology maps if they do not meet the minimum firmware version requirement:

- VOSS or Fabric Engine devices must be 9.2.1.0 or later.
- EXOS or Switch Engine must be 33.3 or later.
- IQ Engine must be 10.8.2 or later.

Firmware compatibility is critical for feature functionality. New features may require specific firmware versions to operate as intended. The following tables list the minimum firmware versions required for the new features introduced in this release:

Universal Compute Platform

Table 4: Required Firmware Versions for Universal Compute Platform

Device Model	Latest Supported Release	Comments
ExtremeCloud Edge (UCP)	10.13.01	Supported hardware models: 1130C 2130C 3150C 3160C 4120C

Access Points (Universal Hardware)

Table 5: Required Firmware Versions for Universal Hardware Access Points

Device Model	Latest Supported Release	Recommended Minimum Release
AP302W	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP305C	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2

Table 5: Required Firmware Versions for Universal Hardware Access Points (continued)

Device Model	Latest Supported Release	Recommended Minimum Release
AP305C-1	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP305CX	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP3000	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP3000X	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP4000	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP4000-1	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP4020	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP410C	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP410C-1	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP460C	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP460S6C	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP460S12C	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP5010	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP5020	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP5022/FX/S6D	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP5050U/D	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP5060U/D	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2
AP510C/CX	IQ Engine 10.8.7 AP 10.18.1	IQ Engine 10.8.2

Switches (Universal Hardware)

Table 6: Required Firmware Versions for Switches

Device Family	Version	Devices
Switch Engine (single/ stacked)	33.6	• 4120 • 4220 • 5120 • 5320 • 5420 • 5520 • 5720 • 7520 • 7720
EXOS	33.6	• X435-8P-2T-W • X435-24T-4S • X435-24P-4S • X435-8T-4S • X435-8P-4S • X440-G2-12p-10GE4 • X440-G2-12t-10GE4 • X440-G2-24p-10GE4 • X440-G2-24t-10GE4 • X440-G2-48p-10GE4 • X440-G2-48t-10GE4 • X450-G2-24p-GE4 • X450-G2-24p-10GE4 • X450-G2-48p-10GE4 • X460-G2-16mp-32p-10GE4 • X460-G2-24p-10GE4 • X460-G2-24p-GE4 • X460-G2-24p-24hp-10GE4 • X460-G2-24t-10GE4 • X460-G2-24t-GE4 • X460-G2-24t-24ht-10GE4 • X460-G2-24x-10GE4 • X460-G2-48p-10GE4 • X460-G2-48t-10GE4 • X460-G2-48t-GE4 • X460-G2-48x-10GE4 • X465-24W • X465-48W • X465-24MU • X465-48P • X465-24MU-24W

Table 6: Required Firmware Versions for Switches (continued)

Device Family	Version	Devices
Fabric Engine	9.4.0.0	• 4220 • 5320 • 5420 • 5520 • 5720 • 7520 • 7720
VOSS	9.4.0.0	• VSP7432CQ • VSP7400-48Y • VSP4900-48P • VSP4900-24XE • VSP4900-24S • VSP4900-12MXU-12XE
Third-Party Management Engine	26.5.0	Model: TPME-S