Extreme Platform ONE Networking v25.4.3-113 Release Notes

New Features, Limitations, and Known Issues

9039330-03 Rev AA
August 2025

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 Networksand 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/

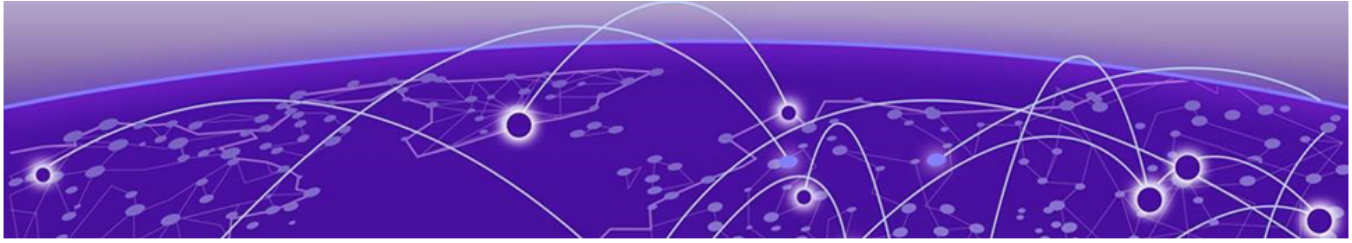
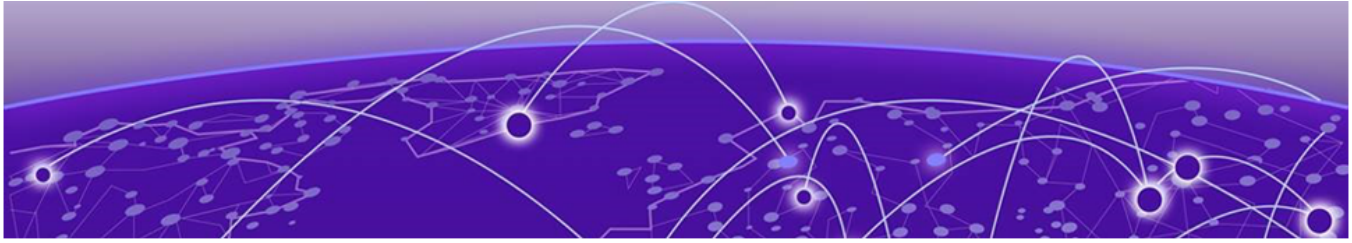
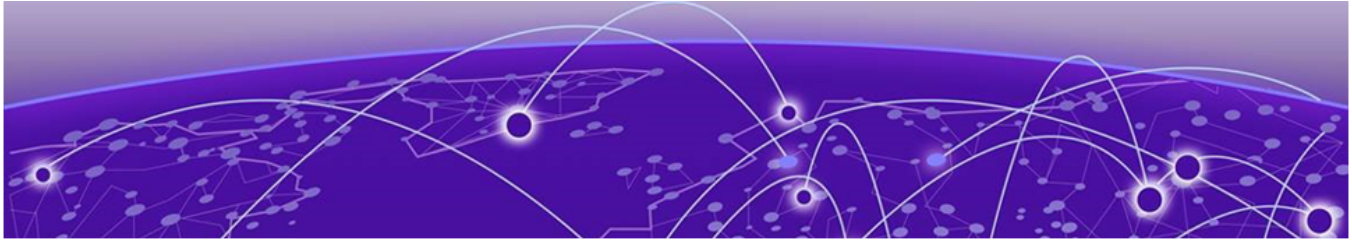


Table of Contents



Abstract

The release notes for Extreme Platform ONE Networking version 25.4.3.113 details centralized orchestration enhancements across ExtremeCloud IQ, SD-WAN, Intuitive Insights, and Platform ONE Security, with role-based access control. Technical updates include device-level configuration for EXOS and Fabric Engine platforms, supporting channelized ports, VLAN/ISID mapping, PoE control, static routing, and Excel-based onboarding with automated provisioning. Visualization modules enable hierarchical topology mapping, multi-area IS-IS overlays, VLAN/L2/L3 service correlation, RF heat maps, and diagnostics for CPU, memory, and port-level metrics. The AI Expert module introduces retrieval-augmented generation (RAG) for documentation summarization, contextual multi-modal responses, and persistent chat history. Firmware prerequisites include EXOS 33.3 and Fabric Engine 9.2.1.0. Issues from previous versions have been addressed, and known limitations remain in areas such as onboarding, visualization fidelity, and wireless mesh support. The content is intended for IT administrators and network engineers managing enterprise-scale, cloud-managed deployments.



Release Notes

Introduction to Extreme Platform ONE Networking

Extreme Platform ONE Networking is a central management platform that simplifies the user experience and provides automation at scale.

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 are always aware of system updates or 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, removing 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	Firewall Address and Port Information
Azure, Canada Central (ACA)	20.151.64.48/28	Firewall Address and Port Information

Data Center	IP Block	Addresses and Ports
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
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.

Note
The applications visible when you log on 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 cloud-enabled 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.
- **Universal ZTNA**: Provides network, application, and device access security within a single solution.

  Note
  As part of the Extreme Platform ONE rollout, Universal ZTNA is now accessible under the label **Extreme Platform ONE Security** in both ExtremeCloud IQ and Extreme Platform ONE. The nine-dot menu label has changed accordingly.

  Once you have selected this option, the Universal ZTNA experience remains unchanged and delivers the same capabilities as expected.

- **Extreme Intuitive Insights**: Provides cloud-based deployment and monitoring of Zebra hand-held devices.

Supported Devices and OS Versions

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 9.1.0.1 or later.
- EXOS or Switch Engine must be 33.3 or later.

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

Device Family	Version	Devices
Switch Engine (single/ stacked)	33.3	• 4120 • 4220 • 5120 • 5320 • 5420 • 5520 • 5720 • 7520 • 7720
EXOS	33.3	• 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

Device Family	Version	Devices
Fabric Engine	9.2.1.0	• 4120 • 4220 • 5120 • 5320 • 5420 • 5520 • 5720 • 7520 • 7720
VOSS	9.2.1.0	• VSP7432CQ • VSP7400-48Y • VSP4900-48P • VSP4900-24XE • VSP4900-24S • VSP4900-12MXU-12XE
IQ Engine Access Point	10.8.3	• AP302W • AP305C • AP305CX • AP3000 • AP3000X • AP4000 • AP4020 • AP410C • AP460C • AP460S6C • AP460S12C • AP5010 • AP5020 • AP5050U • AP5050D • AP510C/CX • AP630 • AP650 • AP650X
ExtremeCloud Edge (UCP)	v5.11.01	• 1130C • 2130C • 3150C • 3160C • 4120C

New Features

Extreme Platform ONE Networking introduces the following features in the 25.4.0 release.

For more information about Extreme Platform ONE Networking features, see the 25.4.0 User Guide.

Table 1: Extreme Platform ONE Networking Features

Feature	Description
Workspace	Serves as the central landing page upon login, offering a unified view of network, security, and subscription insights. It is designed to help users quickly identify critical issues and prioritize actions.
Role-Based Access	Access to Extreme Platform ONE Networking features is governed by user roles. • Administrator: Users with full control over the system • NetSecOps: Users managing network and security operations • Observer: Users with read-only access for monitoring • BizOps: Business users focused on operational insights and subscriptions
Backup & Restore	Manual backup and restore for the Extreme Platform ONE account instance.
Subscriptions & Licensing	View subscriptions and licenses for all cloud-based applications in one place.
Trial Subscription	Request trial subscriptions for Extreme Platform ONE Networking and Universal ZTNA customers who do not have any subscriptions.
Alerts	Add new site policies, detect, record, and report details of events and evaluate performance metrics.
Network Devices	Provides detailed insights into the performance, health, and usage of each device, helping you maintain optimal network functionality.
Network Policy	A network policy is a combination of configuration settings that can be applied to multiple APs, switches, and routers that share a common characteristic, such as being located at the same site or working together to connect multiple remote sites through VPN tunnels.
Inventory	Track critical devices within your site and raise alert notifications in case of abnormalities with the asset.
Theme	Choose between light or dark themes for the user interface.
Logs	Use specific log types to narrow the focus area and streamline troubleshooting.

Table 2: Visualize Features

Feature	Description
Hierarchical Device Locations	You can position devices into a hierarchical location structure which have individual visualization attributes.

Table 2: Visualize Features (continued)

Feature	Description
	Device locations are structured into Site Groups/Sites/ Buildings and Floors.
Different visualization Views	**Abstract View**: Visualize the network in an abstract manner where device interconnect links are normalized. **List View:** Lists the devices in a table view
Dashboard	Overview of the network performance
Geographic View	Sites and buildings are displayed based on address or GPS coordinates.
Physical View	Cloud managed and neighboring devices are positioned on an infinite canvas. The physical view allows device position changes on demand and is shared among all users.
Access View	Access view shows cameras, VoIP phones, and switches along with their connection points. Access View is limited to a single building, with a focused display of one floor at a time.
Fabric View	Fabric View shows the complete network with fabric context, including Fabric Attach, Fabric Connect, and Fabric Extend. Fabric View enables correlation between the Fabric network and both physical and service views.
Service View	Service view shows network services in the context of VLANs, L2 Services, L3 Services. Service view enables correlation of services with both the physical and fabric views. An optional end-to-end service view shows the service path through the network infrastructure.
Floor Plan View	Devices are placed on the floor plan.
Aggregate LLDP Devices	In Physical and Fabric views, all LLDP devices of the same type are grouped as a single LLDP device, marked with the total number of LLDP devices.
Inspector Panel	Inspector Panel provides information about the selected nodes or links in context of the selected views.
Quick Navigation Panel	A quick navigation panel enables fast navigation through the topology by bringing the selected sites/building/ floors into focus.
Per User Save options	You can save Visualize attributes.
Search Infrastructure	A search infrastructure allows to locate any managed device on the list or map.
Tagging Infrastructure	A comprehensive tagging infrastructure enables automatic tags as well as manual tags which enable a wide range of functionality including topology highlights of tagged elements.

Table 2: Visualize Features (continued)

Feature	Description
Alert Visualization	Overlay of alerts on Topology Views and Inspector panel.
Service Definition and Visualization (verbose and non-verbose views)	The following Display Global or Per Device Service View is supported: • L2 Services (L2 ISID and L2 ISID to device/UNI membership) • L3 Services (L3 ISID and L3 ISID to device membership) • VLAN Services (VLANs and VLAN to device/port membership)
Service Tagging	The following features are supported in Service Tagging: • Default tags created for L2/L3/VLAN services • Auto association or dissociation of default service tags with the services, that is, self-tagging • Auto association or dissociation of default service tags with the devices • Policy based service tags
Service Visualization and IS-IS Multi-Area functionality	General Service Visualization is supported across multiple IS-IS areas.
Visualization of one or more services on top of the Topology View	General Service Visualization to visualize one or more network services based on Physical or Fabric View is supported.
Radio Frequency (RF) Network Heat Map	Shows real-time device signal strength across a building floor plan using a color spectrum.
Device 360°	Offers a detailed overview of the selected device, including specifications and status. • Device 360 view for wired devices provides detailed device information, port statistics, client connectivity, services/VLANs, routing tables, and system health monitoring. • The enhanced interface includes interactive port diagrams, real-time statistics, and device management capabilities for both standalone switches and stacks.
Wired Client Health	Provides comprehensive visibility into wired client device health issues. The page displays client connectivity problems, port errors, congestion, and traffic anomalies with actionable workflows for quick issue identification and resolution.
Wired Device Health	Provides comprehensive visibility into switch hardware health including CPU utilization, memory usage, temperature monitoring, PoE utilization, fan status, and power supply health. The page enables quick identification of switches experiencing hardware issues with detailed health metrics and status indicators.

Table 2: Visualize Features (continued)

Feature	Description
Wired Usage and Capacity	Provides comprehensive visibility into wired network performance including bandwidth utilization, throughput metrics, and congestion monitoring. The page displays aggregated switch performance data with detailed port statistics to help identify network bottlenecks and capacity issues.
Switch Engine (EXOS) Device Configuration	Added comprehensive Switch Engine (EXOS) device configuration capabilities to Extreme Platform ONE Networking including network policies, common objects, switch templates, port types, and device-level configuration.
Wireless Device Configuration	Added comprehensive wireless device configuration capabilities to Extreme Platform ONE Networking including network policies, common objects, wireless profiles, radio configurations, and device-level settings.

Table 2: Visualize Features (continued)

Feature	Description
Fabric Engine (VOSS) Device Configuration	• Expanded device-level configuration capabilities for Fabric Engine (VOSS) devices within Extreme Platform ONE Networking. Users can configure Fabric Engine devices directly with comprehensive control over port configuration, LAG, loop prevention, VLAN management, STP settings, PoE control, IP Interface, Static Routing, VLAN/ISID, and Layer 2 switching features. • Applies to existing SKUs and includes support for the 7x20 series (7520 and 7720) with channelized port capabilities. These enhancements provide flexibility in designing high-density networks. • Extended support to the 4K/5K series SKUs (4220, 5320-XT, 5520, and 5720). Users can manage these mid-range switch platforms including port configuration, LAG, loop prevention, VLAN management, STP settings, PoE control, IP Interface, Static Routing, VLAN/ISID, and Layer 2 switching features. • Added lightweight Excel-based onboarding support for Fabric Engine devices with automated configuration provisioning including management settings, fabric parameters, and auto-sense configurations. Users can now streamline fabric device deployment through bulk configuration upload and automated provisioning workflows.
Fabric Engine (VOSS) Fabric-Specific Configuration	Added simplified Shortest Path Bridging MAC (SBPM) Fabric and auto-sense configuration support for Fabric Engine and VOSS SKUs running software version 9.2.1.0 or higher, targeting small-scale, cloud-managed deployments.

Table 3: Extreme AI Expert Features

Feature	Description
AI conversational interface	The AI-powered conversational interface supports the following capabilities: • Streaming responses to user queries, including questions about the network such as locations, devices, clients, applications, alerts, copilot anomalies, and copilot connectivity experience. • Contextual responses. AI will remember the context of previously asked questions • Responses include reference links under the **Learn More** section • Automatic conversation title generation • Interactions support the ability to copy responses, delete a response, and options to provide detailed feedback

Table 3: Extreme AI Expert Features (continued)

Feature	Description
	• Conversation history support the ability to download conversations, delete conversations, delete all conversations, and edit conversation titles • Ability to minimize and restore the interface • Ability to provide multi-modal answers, including text, tables, and charts, about the network.
Documentation summarization (RAG)	Extreme AI Expert provides accurate and summarized responses to documentation-based questions. Responses are sourced from documents included in Extreme AI Expert Knowledge Base.
AI suggested questions	For new conversations, questions are matched to the characters in the input field. For ongoing conversations, questions are matched to the topic of the most recent interaction.
Out of Scope responses	Extreme AI Expert responds with a templated response when the user questions are outside of scope for Extreme AI Expert.
New chat	Initiates a new chat.
Settings	Provides access to the following Extreme AI Expert settings: • Impersonation • Developer Info

Addressed Issues

The following tables list Addressed Issues for Extreme Platform ONE Networking release 25.4.3-113 .

9-Dot Menu

Issue ID	Description
XCP-11590	Fixed an issue where users received unauthorized errors when switching accounts from the 9-Dot menu after navigating to it a second time in a different tab.

API

Issues related to Application Programming Interface (API) functionality and responses.

Issue ID	Description
XCP-11136	Fixed an issue where the App Catalog API did not reflect the customer's RDC deployment status by enhancing it to automatically hide applications that are not deployed at the customer's RDC.

Browser Issues

Issues related to the browser.

Issue ID	Description
XCP-11362	Fixed an issue where users were unable to log out of the Workspace application when using Chrome Incognito browser, as the application automatically logged back in.
CFD-14697	Fixed an issue where login to ExtremeCloud IQ failed when using the latest version of Firefox, causing a redirect loop back to the login page.

Device Issues

Issues related to device visibility, device information display, and device management functionality.

Issue ID	Description
XCP-9897	Fixed an issue where sites became empty when editing external users in the device management interface.

Inventory

Issues related to Inventory.

Issue ID	Description
NVO-9576	Fixed an issue where switches were not getting deleted from the NVO database in scaled setups, even after being deleted from ExtremeCloud IQ.

Licensing

Issues related to license management and contract handling.

Issue ID	Description
XCP-7725	Fixed an issue where license allocation logic did not trigger when there were expired Legacy Entitlement Keys after MSP switched CUID by implementing periodic deletion of expired LEKs.
XCP-11860	Fixed an issue related to license expiry events by re-enabling VIQ notifications for active activations and improving synchronization between GDC and license services.
WS-3259	Fixed an issue where the CUID banner popup was not loading when unlinking licenses in the WS2N environment.

Logs

Issues related to audit logs, security logs, and logging functionality.

Issue ID	Description
XCP-11288	Fixed an issue by implementing unified logout IAM support to ensure all applications log out when a user logs out from any application in multiple tabs.

MSP

Issues related to Managed Service Provider (MSP) functionality and roles.

Issue ID	Description
XCP-11684	The Help Center icon is not visible for users with MSP Super Admin and MSP Admin roles.
XCP-11575	Fixed an issue where API failures occurred when switching tenants within the same region in MSP environments.
WS-3323	Fixed an issue where MSP Admin home and tenant switch buttons were missing after logging into MSP Admin accounts.

Roles

Issues related to role-based access control and user permissions.

Issue ID	Description
XIQ-43835	As designed, users with the Netsecops role do not have permissions to Import/Export/Reset VIQ for Extreme Platform ONE Networking or ExtremeCloud IQ (New).

SSO

Issues related to Single Sign-On (SSO) functionality and authentication.

Issue ID	Description
WS-3313	Fixed an issue where ExtremeCloud IQ (Classic) logout routine in staging appeared different than in production by addressing unified logout experience implementation.

User Interface

Issues related to general user interface components and interactions.

Issue ID	Description
WS-3305	Fixed an issue where logging out from ExtremeCloud IQ did not automatically log out Extreme Platform ONE Networking in unified logout scenarios.
WS-3306	Fixed an issue where Extreme Platform ONE Networking application opened in two tabs did not log out the other tab upon logout in one tab.
WS-3307	Fixed an issue where the logout popup was not loading when users logged out, preventing proper redirect to the login page.
WS-3211, WS-3252	Fixed an issue where clearing cache was required every time before login to CITn/Extreme Platform ONE Networking environments.
WS-3322	Fixed an issue where the login page was not loading after logout, redirecting users to localhost instead of the proper login page.

Visualize

Issues related to network visualization, topology display, and visualization features.

Issue ID	Description
NVO-9468	Fixed an issue where changing network policy on devices did not work properly, with policy changes not persisting after configuration updates.
NVO-9695	Fixed an issue where a 502 Bad Gateway error appeared when scrolling through filters in the NVO physical view.
NVO-9733	Fixed an issue where a collection not complete error appeared when a CDP Neighbor Versions was greater than 255 characters.
NVO-9747	Fixed an issue where changing address in Extreme Platform ONE Networking compatible site locations resulted in locations going from Extreme Platform ONE Networking compatible to limited platform features.
NVO-9756	Fixed an issue where the delta configuration for auto-negotiation enable on transceiver ports that have been pre-configured was adjusted. Explicit port speeds can be configured.
NVO-9810	Fixed an issue where users with Observer role received Access Denied (403 Forbidden) error when saving settings in Visualize.

Known Issues

Table 4 lists the Known Issues in Extreme Platform ONE Networking release 25.4.3-113.

Table 4: Known Issues in release 25.4.3-113

Issue ID	Description
9-dot Menu	
XCP-10803, XCP-11090, XCP-3475	Accessing applications from the 9-dot menu fails with Internal Server Errors.
Account Management	
WS-1916	Users with multiple accounts are unable to switch accounts or VIQs.
WS-3238	Restricted screen is visible to an External VIQ user when switching from an Internal VIQ screen.
WS-775	The Verify Email option in the Account Lockout Notification email takes you to the ExtremeCloud IQ application.
XCP-11212	The External VIQ continues to appear in the Switcher menu even when the access start date is set to a future date.
XCP-11288	Logout from one application does not terminate sessions in other open applications by implementing unified logout functionality across Extreme Platform ONE Networking, ExtremeCloud IQ, SD-WAN, EII, and Extreme Platform ONE Networking Security applications.
XCP-11301	Extreme Platform ONE Networking logout does not support a unified logout URL by implementing support for single logout URL functionality.
Alerts	
CFD-14520	When selecting a cluster of APs connected to a switch, the Alerts tab in the Device Inspector panel does not display the alert count for the associated switch. However, if the Device Inspector is closed and the switch is selected directly (outside the AP cluster view), the correct alert count is shown.
API	
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.
Browser Issues	
NVO-1308	Unable to add or delete tags in Safari browser as pop-ups are not working.
NVO-6837	When using Foxfire, the device icons are misaligned in the Physical View.
WS-2718	When attempting to log out of Extreme Platform ONE Networking while using an Incognito browser window, the application automatically logs back in.
XCP-9905	When accessing the ExtremeCloud IQ URL (https://ws2.qa.xcloudiq.com/) or the SD-WAN URL (https://extremecloudiq.com/discovery-apps), users are redirected to the existing login pages instead of the Extreme Platform ONE Networking login page.

Table 4: Known Issues in release 25.4.3-113 (continued)

Issue ID	Description
Contracts	
CFD-14518	Canceled contracts are displayed as active in the Contracts view.
Device Management	
XIQ-44031	The number of client issues displayed on the Client List page does not match the count shown on the **C360** > **Troubleshooting** > **Client Issues** .
XCP-5268, XCP-5227	Incorrect "Managed_by" value for locally managed devices.
NVO-6878	The Device Inspector does not display the Client tab for some devices.
XCP-10812	Device managed by Site Engine cannot be changed from Managed to Unmanaged and Unmanaged to Managed in Extreme Platform ONE Networking. Use ExtremeCloud IQ to perform such actions.
Inventory	
XCP-7215	The Inventory page takes more time to load and filter API calls are added twice upon reloading.
XCP-10667	On the Inventory page, the Unlock Full Features option is currently disabled.
XCP-10805	When the number of devices is large, filters applied in the Inventory page do not persist after a page refresh.
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.
WS-978	Global search in the Inventory menu is non functional when using Status, Site, and Service Contract criteria.
Licensing	
XCP-10232	The system allocates Extreme Platform ONE Networking licenses to devices even when sufficient licenses are not available, leading to license violation banner in ExtremeCloud IQ (Classic).
WS-3204	Users with Legacy Entitlement Keys (LEK) are redirected to Extreme Platform ONE Networking instead of ExtremeCloud IQ Classic after login.
WS-3195	The "Application Tour" pop-up appears for new users even before a license is linked to their accounts.
WS-3189	The CUID Banner experiences a noticeable delay in loading after a license is unlinked from Extreme Platform ONE Networking.
XCP-11270	A user account with both Extreme Platform ONE Networking and ExtremeCloud IQ licenses is redirected to the ExtremeCloud IQ login page after login, instead of the expected Extreme Platform ONE Networking login page.
XCP-11193	Linking a portal account with Extreme Platform ONE Networking only licenses fails to redirect users from ExtremeCloud IQ to Extreme Platform ONE Networking.

Table 4: Known Issues in release 25.4.3-113 (continued)

Issue ID	Description
Logs	
XCP-10467	During onboarding failures, the Audit Log incorrectly records the status as "Success".
XCP-11224	The Audit Log displays API denied error log entries, which are not relevant.
MSP	
XCP-10605	MSP Super Admin and MSP Admin users are unable to access the Clone Building and Clone Floor functionalities.
XCP-11278	In the MSP view for the U.S. region, the Switch Tenant panel remains open and cannot be dismissed.
XCP-11254	Changing a user role from MSP Super Admin to MSP Admin removes their ExtremeCloud IQ Admin role.
Onboarding	
XCP-6924	The general device onboarding failed toast messages must include reason for failure.
XCP-10407	The DLCS service returns inconsistent schema structures for HTTP 400 errors across different onboarding interfaces.
XCP-10371	Wired and Wireless onboarding processes onboard more than 10 devices, exceeding the intended limit.
XCP-10317, XCP-10324	Wired and Wireless AP serial numbers are not validated during onboarding, and the expected HTTP 400 error code is not returned.
Roles	
XCP-10308	Manage or Unmanage actions are not performed for the NetSecOps Role.
XCP-10865	Users with the NetSecOps Role scoped to specific sites are able to create new site groups successfully, but unable to view new groups after creating them.
WS-3030	The eligibility banner ("Connect Eligible and Not Eligible") is displayed incorrectly when accessing the application using a role-based account.
SSO	
XCP-8507	The login button does not activate for certain SSO-enabled user login instances.
Troubleshooting	
XCP-11234	The number of client issues displayed on the Client List page does not match the count on the **C360** > **Troubleshooting** > **Client Issues**.
User Interface	
XCP-5065	Search and Filter does not filter the appliance cluster.
XCP-5043	UCP appliance is misaligned in the table under **Asset** > **Appliance**.

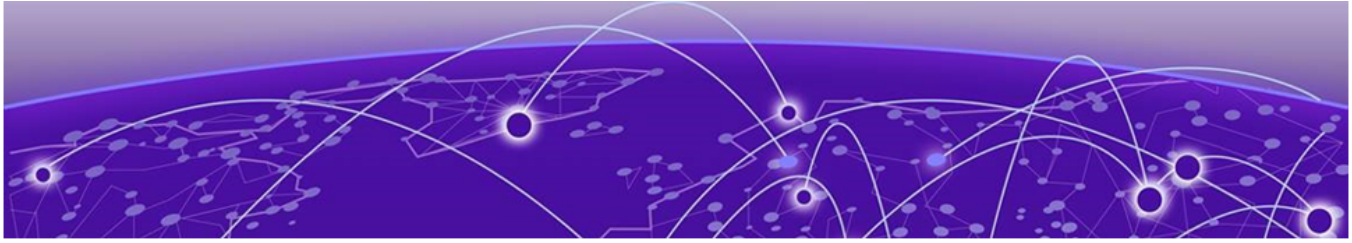
Table 4: Known Issues in release 25.4.3-113 (continued)

Issue ID	Description
XCP-6945	Table alignment for the child devices is not aligned under **All** > **Switch** > **Appliance**.
WS-2894	The Terms & Conditions pop-up briefly appears after login but disappears without user interaction.
XCP-10793, WS-2708	Extreme Platform ONE Networking does not apply the selected language to the following elements: • Dashboard title and menu name • Sub text of the tiles • Table column header
Visualize	
NVO-8908	Node custom positions in topology are not retained on browser refresh.
NVO-7586	Fabric links may not appear in the Fabric Layer View when devices use the default ISIS area ID 1515.fee1.900d.1515.fee1.900d and are running Visualization version 24.5 or older.

Limitations

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

- Trial Subscriptions are only available for Extreme Platform ONE Networking and Universal ZTNA.
- Site-Engine managed devices that are connected to ExtremeCloud IQ are unsupported.
- 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.



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.