Extreme Platform ONE Networking v25.9.2-1 (Patch 4) Release Notes

New Features, Limitations, and Known Issues

9041075-04 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/

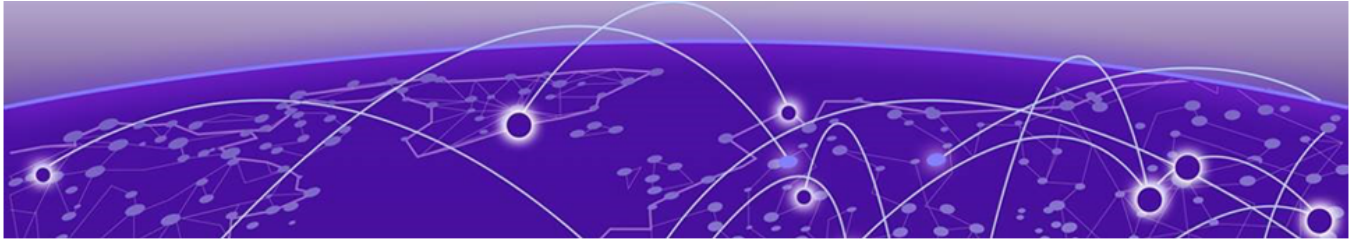
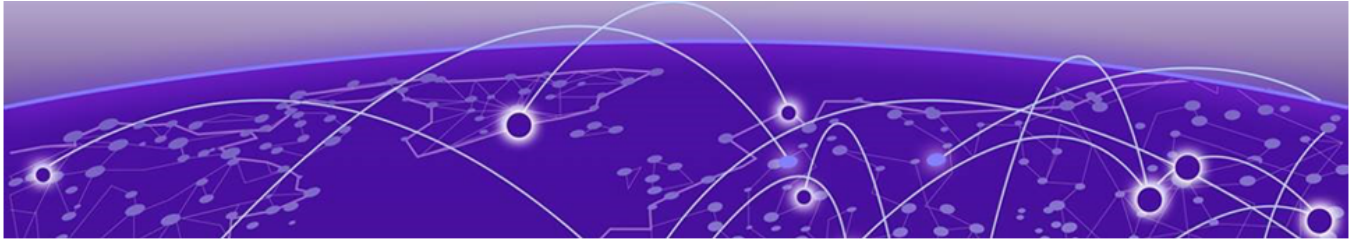
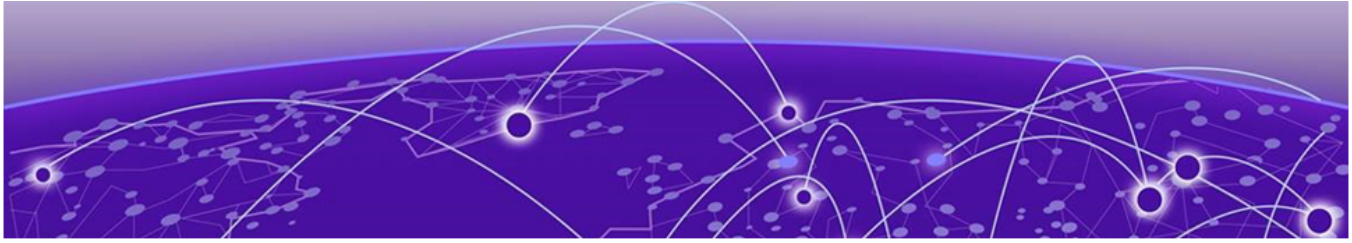


Table of Contents



Abstract

This release notes document for Extreme Platform ONE Networking version 25.9.2-1 (Patch 4) provides a technical overview of updates, fixes, and operational constraints for the unified cloud-based network management platform, targeting experienced IT administrators. It details core functionality including centralized device onboarding, monitoring, configuration, API integration, AI-assisted support, and unified access across ExtremeCloud IQ, SD-WAN, security, and analytics applications with SSO and browser-based interfaces. Patch update resolves an issue where users could experience intermittent slowness or unresponsiveness when interacting with Extreme Platform ONE Networking. The document outlines deployment prerequisites such as public cloud IP ranges and firmware thresholds, and addresses scalability considerations for large inventories. It also highlights known issues in APIs, RBAC enforcement, visualization accuracy, and bulk operations, and provides troubleshooting insights into onboarding failures, performance bottlenecks, and configuration inconsistencies.



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.

General Release Information

Browser Support and Display Settings on page 11

Current Release: 25.9.2-1 (Patch 4)

May 2026

This release resolves an issue where users could experience intermittent slowness or unresponsiveness when interacting with Extreme Platform ONE Networking.

Related Links

- Known Issues on page 19
- Device Support Information on page 26

Release: 25.9.0-199 (Patch 3)

May 2026

This release addresses database connection inefficiencies, onboarding inconsistencies, RF statistics processing errors, UI/API defects, and adds support for the AP4060 and AP4060X universal access points.

Related Links

- Known Issues on page 19
- Device Support Information on page 26

Table 1: Release: 25.9.0-199 (Patch 3) Addressed Issues

Issue ID	Description
CFD-16926	Addressed the issue where VLAN and Auto-Sense values were not populated in the user interface during switch bulk onboarding through XLSX. The system now correctly applies configuration values from the XLSX file and automatically pushes the configuration to the device.
XCP-12320	Added onboard, monitor, and configuration support for the AP4060 and AP4060X universal access points.

Table 1: Release: 25.9.0-199 (Patch 3) Addressed Issues (continued)

Issue ID	Description
XCP-21215	Addressed the issue where pcs-wireless-service leaked idle-in-transaction database sessions on systemdb, causing DBLongTransaction alerts. The service now provides more predictable and stable wireless service performance without the gradual slowdowns that were occurring as leaked database connections accumulated and does not require manual CloudOps intervention to clean up stale sessions.
XCP-21218	Addressed the issue where PCS service enablement added approximately 500 new database connections with large connection pools to configdb, causing memory constraints. The system now provides more reliable platform operations without the resource contention that was impacting the configuration database's ability to handle normal workloads efficiently.

Release: 25.9.0-199 (Patch 2)

April 2026

Related Links

- Known Issues on page 19
- Device Support Information on page 26

Table 2: Release: 25.9.0-199 (Patch 2) Addressed Issues

Issue ID	Description
CFD-16838	Addressed an issue where incorrect or missing information was provided for port details on the Extreme Platform ONE Networking **Overview** page.
CFD-16989	Addressed an issue where affected switches displayed a "Configuration rollback" status without a rollback being performed.
NVO-10726, WS-3519	External users with the Bizops role have access to the **Visualization** page.
NVO-12227	Reverting a Fabric Engine 7830 device to template defaults does not correctly reset VIM port configuration. After the revert, only port 1/1 is restored to default; ports on VIM 2 and VIM 3 retain their previous VLAN and auto-sense settings. Unlocking the device does not restore access to VIM 2 and VIM 3 ports.

Table 2: Release: 25.9.0-199 (Patch 2) Addressed Issues (continued)

Issue ID	Description
XCP-20775	Addressed an issue where the `start` and `end` time fields returned by the `assets/v1/summary/history` API contained values whose data types did not match the declared schema.
XIQ-49108	Addressed an issue where launching Real Time Troubleshoot (RTTS) from the **Client Inventory Heat Map** view caused two RTTS pop-up windows to open simultaneously, with the **Start/Stop** controls hidden.
XIQ-49343	Addressed an issue where selecting a site row on the **Dashboard** did not automatically apply the site filter.
XIQ-49345	Addressed an issue where there was no visible indicator that a filter was active on the **Dashboard** and other pages. A visible indicator now appears when a site filter is active to prevent confusion from filtered views
XIQ-49347	Addressed an issue where the **Dashboard** displayed raw unformatted numbers without units or context. The **Dashboard** now displays all numeric values in a consistent, human-readable format. Large integers are abbreviated with K, M, or B suffixes; byte counts include appropriate units (KB, MB, GB, TB); and percentages are shown with a % symbol at the correct decimal precision.
XIQ-49357	Addressed an issue where the Extreme Platform ONE Networking **Dashboard** did not display key performance indicators (KPIs) for legacy and third-party devices alongside cloud-managed devices.
XIQ-49362	Addressed an issue where wireless access points were not appearing on the **Usage & Capacity** and **Device Health** pages after onboarding due to an RF statistics processing error.

Release: 25.9.0-199 (Patch 1)

April 2026

This release addresses Third-Party Management Engine user interface text translation issues, AP5010 device disconnection issues, and OWE SSID configuration push issues.

Related Links

- Known Issues on page 19
- Device Support Information on page 26

Table 3: Release: 25.9.0-199 (Patch 1) Addressed Issues

Issue ID	Description
CFD-16594	Addressed an issue where an OWE SSID was not assigned after two complete configuration pushes or when using S-CLI with transition mode enabled.
CFD-16829	Addressed an issue where many AP5010 devices appeared as "capwap disconnected" on ExtremeCloud IQ after upgrading to version 25.8.1, even though they were connected.
CFD-16882	Resolved an issue where some Third-Party Management Engine user interface text was not translated correctly.

Release: 25.9.0-199

April 2026

This release introduces third-party device support, enhanced Device 360 visibility, improved topology and Fabric Attach visualization, updated OS and firmware compatibility, and diagnostics such as RTT and 6 GHz FTM, while also documenting resolved defects, known issues, and operational limitations relevant to large-scale enterprise deployments.

Related Links

- Known Issues on page 19
- Device Support Information on page 26

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
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

Data Center	IP Block	Addresses and Ports
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

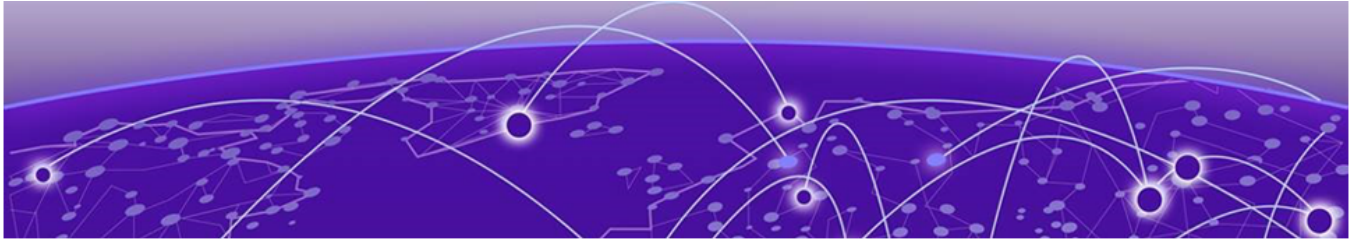
Extreme Platform ONE supports the latest 64-bit versions of the following desktop browsers:

- 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.



Previous Release

This section lists the new features, addressed issues, and known issues for the previous release.

New Features

Table 4 on page 14 lists the new features introduced in Extreme Platform ONE Networking release 25.9.0-199.

For more information about Extreme Platform ONE Networking features, see the Extreme Platform ONE Networking v25.9.0 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
  - 9.3.2 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 10.8.6

New Hardware Support

No new hardware in this release.

Table 4: New Features in release 25.9.0-199

Feature ID	Feature	Description
NVO-5277	Visualization Support for Third-Party and Legacy Devices	Extreme Platform ONE Networking supports visualization for third-party and legacy devices managed through the Third-Party Management Engine. The topology and access maps display these devices using a dedicated icon, with limited features including LLDP-based neighbor linking, port names on links, and link statistics.
NVO-10257	Object Inspector panel for Third-Party Managed Devices	Extreme Platform ONE Networking provides an **Object Inspector** panel for devices managed through the Third-Party Management Engine. The panel displays connection status, device health, system name, IP address, location, model, OS version, system MAC, serial number, system description, and port operational status, with a link to the associated Third-Party Management Engine.
NVO-11474	Device Details (D360) for Third-Party Managed Devices	Extreme Platform ONE Networking now offers Device Details (D360) for third-party managed devices through the Third-Party Management Engine. The view is accessible from the **Object Inspector** and **Network Devices**, and displays connection status, device health, CPU and memory usage, resource utilization, temperature, port statistics, and port silk screen data, matching the look and feel of wired device details.
NVO-11475	Device Details (D360) for Third-Party Management Engine	Extreme Platform ONE Networking now offers Device Details (D360) for the Third-Party Management Engine itself. The view displays connection status, system information, discovery status, backup and firmware upgrade progress, SNMP timer properties, scheduled jobs, and an inventory table of all devices owned by the Third-Party Management Engine.

Table 4: New Features in release 25.9.0-199 (continued)

Feature ID	Feature	Description
NVO-11513	New Configuration Model Support for the Third-Party Management Engine	Extreme Platform ONE Networking now offers New Configuration Model support for the Third-Party Management Engine itself, including New Configuration Model profile and profile assignment, SNMP Timer configuration, Management Profile settings, and a global configuration and deploy flow for the Third-Party Management Engine.
NVO-11514	New Configuration Model Support for Third-Party Managed Devices	Extreme Platform ONE Networking now offers New Configuration Model support for third-party devices managed by the Third-Party Management Engine, including Managed Profile (hostname and device family), Access Profile, SNMP Credentials, and CLI Credentials configuration.
NVO-11517	Display of Fabric Attach (FA) links between MLAG clusters in both the **Physical** and **Fabric** topology layers	Extreme Platform ONE Networking now offers correct display of Fabric Attach (FA) links between MLAG clusters in both the **Physical** and **Fabric** topology layers, including support for configurations where EXOS/Switch Engine switches act as FA Proxies and VOSS/Fabric Engine switches act as FA Servers.
NVO-12731	**Device Details** (D360) for Third-Party Managed Devices	Extreme Platform ONE Networking now offers **Device Details** (D360) for third-party managed devices through the Third-Party Management Engine, displaying device health, CPU and memory usage, resource utilization, temperature, fan and power status, port statistics (utilization, throughput, in/out counters, errors), and LLDP neighbor information. The view is accessible from the **Object Inspector** and **Network Devices**.
XCP-12658	Licensing Support for the Third-Party Management Engine and Devices Onboarded	Extreme Platform ONE Networking now offers licensing support for the Third-Party Management Engine and devices onboarded through it. The Third-Party Management Engine requires a minimum Tier A (EP1-STD) license, while managed devices require an EP1-STD-T3RD (third-party) license. An unmanaged Third-Party Management Engine provides no device statistics. The implementation includes generic licensing support, subscription requests, and license violation handling, with Navigator and Pilot licenses remaining incompatible with Third-Party Management Engine and EP1-compatible buildings.

Table 4: New Features in release 25.9.0-199 (continued)

Feature ID	Feature	Description
XIQ-43244	Improved Communication of Round Trip Time (RTT) Platform Support	Extreme Platform ONE Networking now offers improved communication of Round Trip Time (RTT) platform support in the client view. Clients eligible for RTT testing are now visually distinguished, and users receive an informative error message when RTT is unavailable for a given client's associated access point.
XIQ-49305	Automatic Ap to AP 802.11mc FTM Ranging is Automatically Enabled	Automatic Ap to AP 802.11mc FTM ranging is automatically enabled when SSID configuration requires 6 GHz and 6 GHz, when AP model supports 6 GHz and when the country of operation is USA or Canada.
XCP-17589	VOSS/ Fabric Engine Support	Support is now offered for Fabric Engine 9.2.3 and 9.3.2 to enable onboarding, monitoring, configuration, and drag- and-drop image management for VOSS/Fabric Engine ExtremeCloud supported SKUs including Universal switches, 7830, VSP7400, and VSP4900.
XIQ-48693	EXOS/ Switch Engine 33.5.2.118-patch1-11 Patch Support	Support is now offered for EXOS/Switch Engine 33.5.2.118-patch1-11 patch for onboarding, monitoring, and configuration for all ExtremeCloud-supported SKUs through download image support.
XIQ-48694	EXOS/ Switch Engine 33.5.2.118-patch1-11 Patch Support	Support is now offered for image download for EXOS/Switch Engine version 33.5.2.118-patch1-11 for all supported single and stacked EXOS/ Switch Engine SKUs. The available images in the global download dropdown are 31.7.4.2-patch1-7, 32.7.3.15-patch1-33, 33.5.2.118-patch-11, and 33.5.2 (latest).
XIQ-47948	EXOS/ Switch Engine 33.6 GA Support	Support is now offered for image download for EXOS/Switch Engine 33.6 GA for all ExtremeCloud-supported SKUs, making it available as the latest image in the download dropdown.
XIQ-47949	EXOS/ Switch Engine 33.6 Download Support	Support is now offered for image download for EXOS/Switch Engine 33.6 GA for all ExtremeCloud-supported SKUs.
XCP-17622	EXOS/ Switch Engine 33.6.1 GA support	Support is now offered for onboarding, monitoring, and configuring all ExtremeCloud IQ-supported EXOSSwitch Engine SKUs running version 33.6.1, including drag-and-drop local image management support.

Addressed Issues

lists Addressed Issues in Extreme Platform ONE Networking release 25.9.0-199.

Table 5: Addressed Issues in release 25.9.0-199

Issue ID	Description
Alerts	
XCP-12847	Addressed the issue where an alert was not generated when a device is detected with an unsupported firmware version.
XCP-12964	Addressed the issue to update the alert formatting.
Device Management	
XCP-19003	Addressed the issue where attempting to unmanage an already-unmanaged device in the **Network Devices** view displayed an invalid subscription error. The fix corrects the subscription status display to show Not Applicable for unmanaged devices.
XCP-19210	Addressed the issue where the internal user list in **Access Management** displayed no users when the pagination count was set to 500.
XCP-19571	Addressed the issue where deleting a stack from ExtremeCloud IQ-SE correctly removed the stack member from the Extreme Platform ONE Networking Inventory but left the parent Stack entry behind.
XIQ-47663	Addressed the issue where a Switch Engine device did not transition to a disconnected state after being flipped to a Fabric Engine persona.
Inventory	
XCP-14922	Addressed the issue where the **Firmware Status** page returned no data and generated a 504 timeout error when the inventory contained approximately 30,000 or more devices.
XCP-18242	Addressed the issue where device location assignments applied in bulk using multi-select did not reflect consistently between the **Network Devices** and **Inventory** views, causing some devices to display as Unassigned in **Inventory** while correctly showing the location in **Network Devices**.
Licensing	
WS-4019	Addressed the issue where an erroneous "Error linking account" toast appeared when linking a VIQ to a Partner license account using a correct CUID, even though the link completed successfully.
XCP-17735	Addressed the issue where users with active Legacy Entitlement Keys (LEKs) did not receive a warning upon login to the ExtremeCloud IQ Classic user interface when the VIQ is not linked.
XCP-19249	Addressed the issue where the NG-IAM integration with the licensing system failed due to an incorrectly configured linkage request parameter in the license API, causing IAM services to enter a CrashLoopBackOff state.

Table 5: Addressed Issues in release 25.9.0-199 (continued)

Issue ID	Description
Logs	
CFD-16719	Addressed an issue where AP events were not being logged.
SSO	
WS-3868	Addressed the issue where switching to an external SSO account immediately after navigating from an internal account failed on the first click.
Upgrading	
CFD-16883	Addressed the issue where all existing certificate authority information was deleted from Extreme Platform ONE Security, and Extreme Managed Certificate could not be generated, after upgrade.
XCP-18110	Addressed the issue where the firmware upgrade scheduler saves the change in scheduled date or time without selecting **Done**.
User Interface	
WS-3120	Addressed the issue where users occasionally encountered a white screen with incomplete application loading upon login to the Extreme Platform ONE Networking.
XCP-19062	Addressed the issue where the column header in the Monitoring network devices view was displayed as OS instead of the full column header of Operating System.
XCP-19369	Addressed the issue where the client health statistics table returned no data because the analytics client table was not populating the client_health_stats table correctly.
XCP-19805	Addressed the issue where an uploaded floor image did not load correctly when editing an existing floor in the **Sites** module, even though the image was saved successfully during floor creation.
XIQ-46735	Addressed the issue where toggling the Auto Config setting in VIQ Management caused devices with a current audit match status (green icon) to incorrectly change to audit mismatch status (yellow icon) in the **Network Devices** view.
XIQ-47190	Addressed the issue where the notification service failed to send emails to addresses containing an apostrophe, even though the user interface allowed such addresses to be saved.
Visualize	
NVO-6837	Addressed the issue where device icons in the **Physical** topology view were not centered in their circles when using the Firefox browser, causing icons for APs and stacks to appear cut off at the top. This issue did not occur in Chrome.
NVO-10726	Addressed the issue where external users with the BizOps role could access the **Network Visualization** page without authorization.

Known Issues

Table 6 lists the Known Issues in Extreme Platform ONE Networking release 25.9.2-1 (Patch 4).

Table 6: Known Issues in release 25.9.2-1 (Patch 4)

Issue ID	Description
9-dot Menu	
XCP-3475, XCP-10803, XCP-11090	Accessing applications from the 9-dot menu fails with Internal Server Errors.
API	
XCP-17687	If the user interface has a different schema it might not show the toast message from the 400 json data.
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. The root cause is a data sync gap between XIQ and the Common Ignite and HM Ignite cache tables.
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-47766	Automatic configuration application to offline devices is not supported.
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.
XIQ-44593	An issue exists where **AFC Status** and **GEO Location** widgets display visual artifacts when viewed on MacBook Pro using Safari browser.
Device Management	
SEN-538	The VM restarts if there are two environmental changes in a ten minute period, such as a change to the HTTP proxy and a hostname change.

Table 6: Known Issues in release 25.9.2-1 (Patch 4) (continued)

Issue ID	Description
NVO-12227	Reverting a Fabric Engine 7830 device to template defaults does not correctly reset the auto-sense and VLAN configuration on ports located on VIM 2 and VIM 3. After a revert, VIM 2 and VIM 3 ports remain inaccessible in the configuration page.
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-19598	The deployment schedule on the device level cannot be edited after the site deployment is scheduled.
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.
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.

Table 6: Known Issues in release 25.9.2-1 (Patch 4) (continued)

Issue ID	Description
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.
Inventory	
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.
XIQ-47622	The Users grid XAPI request times out when a filter such as Status=Connected is applied to an inventory containing approximately 148,000 user records.
Licensing	
XCP-20014	Third-Party Management Engine discovered devices are not onboarded to Extreme Platform ONE Networking if there are not enough licenses for all discovered devices.
Logs	
XCP-11224	The **Audit Log** displays API denied error log entries, which are not relevant.

Table 6: Known Issues in release 25.9.2-1 (Patch 4) (continued)

Issue ID	Description
XCP-16345, XCP-16530	Audit logs are generated out of sequence when upgrading firmware or 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	
SEN-568	If the VM reboots during the onboarding process the next onboarding attempt fails.
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.
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.
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	
SEN-616	The `show tpme proxy` command does not display the configured value.
XIQ-48210	Downloading the AFC Geolocation report produced a corrupt file that was not in the expected CSV format, making it unusable for troubleshooting.
Upgrading	

Table 6: Known Issues in release 25.9.2-1 (Patch 4) (continued)

Issue ID	Description
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.
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-18982	EP1, New XIQ: The displayed selection count does not match the actual number of selected devices when devices are selected across multiple pages.
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-19182	Link statistics for devices managed by Third-Party Management Engine are displayed as 0.
XCP-19300	"Uptime" and "Connected For" data is not available for devices managed by the Third-Party Management Engine in Network Devices.

Table 6: Known Issues in release 25.9.2-1 (Patch 4) (continued)

Issue ID	Description
XCP-19330, XCP-18722	The error message is not formatted properly when a duplicate CLI Credential or a duplicate Access Profile is created.
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-19995	The **Device-360** view of a Third-party Management Engine is not displayed from within the **Device-360** view of a device managed by the Third-Party Management Engine for the first time. Workaround: Close Device-360 and open it again.
XCP-20010	**Device 360** view displays an error for the devices managed by the Third-Party Management Engine if those devices are Unmanaged.
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.
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-48218	Selecting **Configure** from **Network Devices** displays **Third Party Management** instead of **Configuration Profile**.
Visualize	
NVO-12227	Reverting a Fabric Engine 7830 device to template defaults does not correctly reset VIM port configuration. After the revert, only port 1/1 is restored to default; ports on VIM 2 and VIM 3 retain their previous VLAN and auto-sense settings. Unlocking the device does not restore access to VIM 2 and VIM 3 ports.

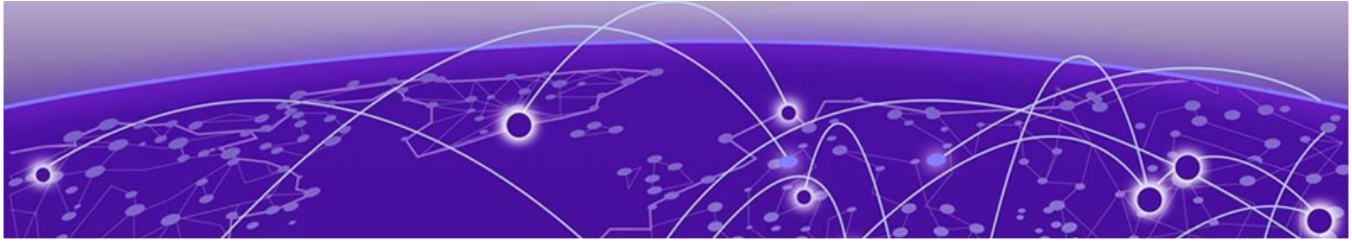
Table 6: Known Issues in release 25.9.2-1 (Patch 4) (continued)

Issue ID	Description
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.
XCP-18944	The Unknown tag can be assigned to a device managed by the Third-Party Management Engine in some cases.

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 7: 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 8: Required Firmware Versions for Universal Hardware Access Points

Device Model	Latest Supported Release	Recommended Minimum Release
AP302W	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2
AP305C	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2

Table 8: Required Firmware Versions for Universal Hardware Access Points (continued)

Device Model	Latest Supported Release	Recommended Minimum Release
AP305C-1	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2
AP305CX	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2
AP3000	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2
AP3000X	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2
AP4000	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2
AP4000-1	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2
AP4020	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2
AP410C	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2
AP410C-1	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2
AP460C	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2
AP460S6C	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2
AP460S12C	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2
AP5010	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2
AP5020	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2
AP5050U	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2
AP5050D	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2
AP510C/CX	IQ Engine 10.8.6 AP 10.18.1	IQ Engine 10.8.2

Switches (Universal Hardware)

Table 9: Required Firmware Versions for Switches

Device Family	Version	Devices
Switch Engine (single/ stacked)	33.5	• 4120 • 4220 • 5120 • 5320 • 5420 • 5520 • 5720 • 7520 • 7720
EXOS	33.5	• 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 9: Required Firmware Versions for Switches (continued)

Device Family	Version	Devices
Fabric Engine	9.3.0.0	• 4120 • 4220 • 5120 • 5320 • 5420 • 5520 • 5720 • 7520 • 7720
VOSS	9.3.0.0	• VSP7432CQ • VSP7400-48Y • VSP4900-48P • VSP4900-24XE • VSP4900-24S • VSP4900-12MXU-12XE