



Extreme Platform ONE Networking v25.7.2-184 (Patch 2) Release Notes

New Features, Limitations, and Known Issues

9041007-02 Rev AA
March 2026



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

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: <https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks>

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses.

End-user license agreements and open source declarations can be found at: <https://www.extremenetworks.com/support/policies/open-source-declaration/>

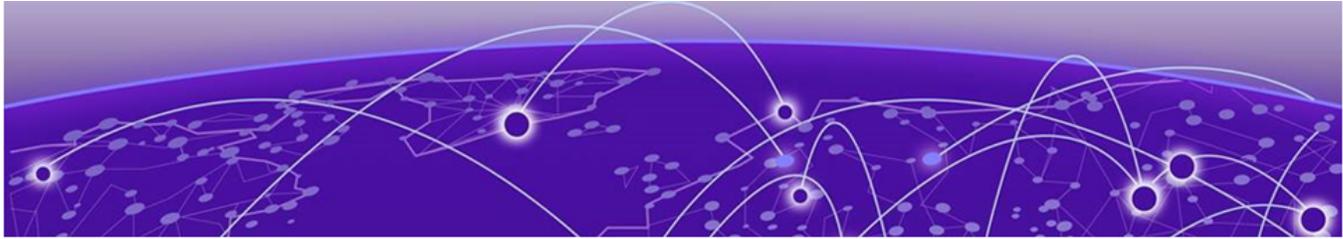
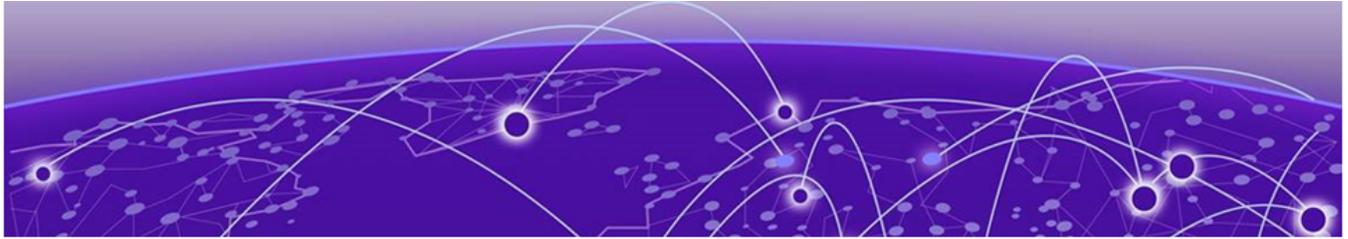


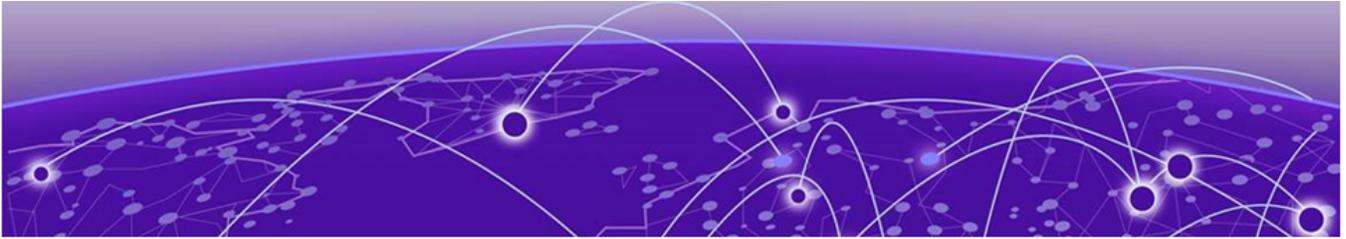
Table of Contents

Abstract.....	4
Help and Support.....	v
General Release Information.....	6
Current Release: 25.7.2-184 (Patch 2).....	6
Release: 25.7.2-184 (Patch 2) Addressed Issues.....	6
Release: 25.7.0-175 (Patch 1).....	7
Release: 25.7.0-175 (Patch 1) Addressed Issues.....	7
Introduction to Extreme Platform ONE Networking.....	7
Extreme Platform ONE Public IP Address Blocks.....	8
Supported Applications.....	9
Browser Support and Display Settings.....	9
Desktop Browsers.....	9
Display Settings.....	10
Previous Release.....	11
New Features.....	11
Addressed Issues.....	13
Known Issues.....	16
Limitations.....	20
Device Support Information.....	21
Universal Compute Platform.....	21
Access Points (Universal Hardware).....	21
Switches (Universal Hardware).....	23



Abstract

This release notes document for Extreme Platform ONE Networking version 25.7.2-184 (Patch 2) provides a technical overview of targeted software fixes, platform enhancements, and operational refinements across unified network management workflows. It details corrections to visualization accuracy, MFA login stability, AP5010 zero-touch provisioning, 6 GHz radio setup, dashboard data integrity, and health-visibility metrics. Key usage scenarios include multi-domain device onboarding, remote configuration, firmware lifecycle operations, and cross-application SSO access. Known issues and limitations address API metric inaccuracies, browser-specific UI defects, regulatory-driven AP constraints, and scalability limits for bulk operations. This document is intended for experienced network administrators and technical practitioners requiring precise, platform-specific operational guidance.



Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

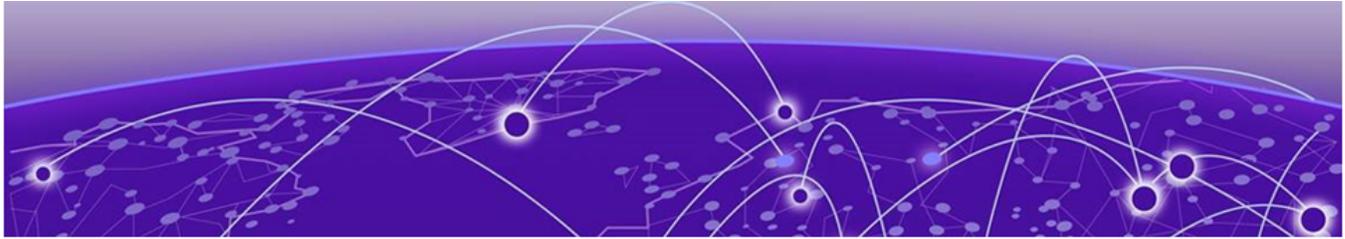
Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

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 9

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

Current Release: 25.7.2-184 (Patch 2)

March 2026

This release provides corrections to visualizations affecting heatmaps and client visibility. It also provides improvements to Multi-Factor Authentication (MFA) login for customers with strict security policies. AP5010 zero-touch provisioning and 6GHz radio configuration setup is improved. This release also provides data integrity improvements to dashboard accuracy and customer health visibility.

Related Links

- [Known Issues](#) on page 16
- [Device Support Information](#) on page 21

Release: 25.7.2-184 (Patch 2) Addressed Issues

Issue ID	Description
XIQ-48406	Addressed the issue where RDCs that have not upgraded to release 25.7 experience broken heatmaps, client visibility, and scheduled reporting due to a MFE/API version mismatch.
XIQ-47715	Fixed the issue where newly deployed AP5010 devices fail to auto-configure the commissioner function, which requires manual CLI intervention.
XCP-17558	Addressed the issue where wired client session records have incorrect disconnect timestamps, which causes stale 'active' sessions to persist in analytics.
CFD-16354	Fixed the issue where ExtremeCloud IQ login fails after Multi-Factor Authentication due to a security block on an external CDN (cdn.jsdelivr.net).

Release: 25.7.0-175 (Patch 1)

February 2026

This release addresses several device display issues, including incorrect LLDP neighbor data after configuration push, observer-role users errors, and client statistics failing to load properly. This release addresses multiple AP display and configuration issues including missing data for ExtremeCloud IQ Controller-managed AP5060 models. This release also addresses multiple Tunnel Concentrator configuration issues including displaying policy changes, delta configuration pushes, and location-based SSID classifications.

Related Links

- [Known Issues](#) on page 16
- [Device Support Information](#) on page 21

Release: 25.7.0-175 (Patch 1) Addressed Issues

Issue ID	Description
CFD-16414	Addressed the issue where SSO login was not visible on the ExtremeCloud IQ login page for some users.
CFD-16235	Addressed the issue where customer stacks went unmanaged, disrupting switch management and licensing.

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

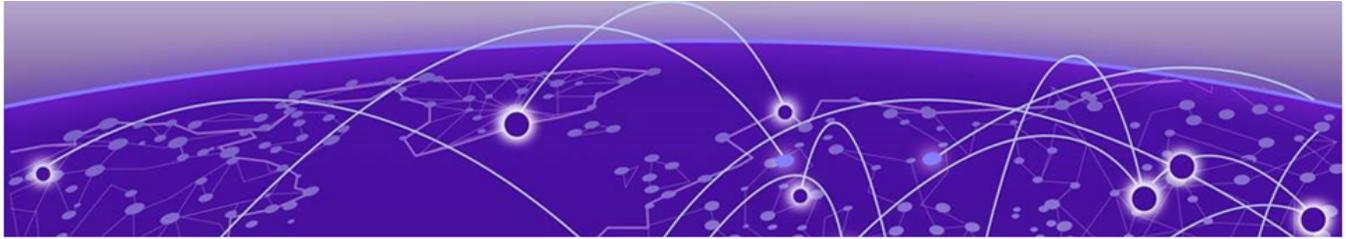
Extreme Platform ONE supports the latest 64-bit versions of the following desktop browsers:

- 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

[New Features](#) on page 11

[Addressed Issues](#) on page 13

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

New Features

[Table 1](#) on page 12 lists the new features introduced in Extreme Platform ONE Networking release 25.7.0-175.

For more information about Extreme Platform ONE Networking features, see the Extreme Platform ONE Networking v25.7.0 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 0.9.40
 - EXOS/Switch Engine release >= 33.2 upgrade to IQAgent version 1.9.40
- 33.5.2.118-patch1-6 Latest Supported GA Patch

Onboard, Monitor, Config, Image Mgmt, and Global Download Support

- 33.5.1.6 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:**

- 0.9.31 IQ Agent Support
- 9.3.1 Latest Supported GA Image

Onboard, Monitor, Config, Image Mgmt, and Global Download Support

- 9.2.2 Previous Supported GA Patch

- Onboard, Monitor, Config, Image Mgmt, and Global Download Support
 - 9.1.3 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 1: New Features in release 25.7.0-175

Feature ID	Feature	Description
NVO-10901	New Zoom Functionality	Added double-click and shift + double-click zoom functionality in the Physical and Fabric layer views.
NVO-13263	Visualization Feature Compatibility	Compatibility and testing for NVO 24.8 visualization features requires minimum versions: Switch Engine/EXOS 33.5, Fabric Engine/VOSS 9.3, and IQ Engine 10.8r4.
XIQ-27415	Packet Capture on IOT Interface	Added packet capture support on the IOT interface for AP5010 access points.
XIQ-29193	New Filter for Network Devices	A new filter allows you to draw a shape around a collection of devices from the heat map and use that filter to focus only on the highlighted devices in the Network Devices tab.
XIQ-35548	IQ Engine 10.8.6 Support	Added support for the IQ Engine 10.8.6 software version.
XIQ-35666	Real-Time Troubleshooting (RTTS) for Wi-Fi 7 Access Points	Enhanced RTTS functionality to include Wi-Fi 7 access points on the AP5020 and the AP4020 series platforms.
XIQ-35720	Text Objects and Labels for Floor Maps	Added the ability to add text objects and labels to floor maps for better understanding of floor areas.
XIQ-38523	VLAN per Private Pre-Shared Key Functionality	Implemented VLAN per Private Pre-Shared Key functionality for hospitality environments with individual room isolation.
XIQ-41384	Multiple Network Profiles for Tunnel Concentrator	A Tunnel Concentrator may now be used in multiple network policies.
XIQ-44768	Email Report Delivery Support	Email delivery of reports is now supported.

Table 1: New Features in release 25.7.0-175 (continued)

Feature ID	Feature	Description
XIQ-44794	Multi-line Graphs for Reports "By OS" Support	Multi-line graphs now supported for "By OS" reports.
XIQ-46617	AP5020 MLO Support	Added MLO (Multi-Link Operation) support on an AP5020, including AP MLD (Multi-Link Device) operating with a non-AP MLD that supports EMLSR (Enhanced Multi-Link Single Radio).
XIQ-46682	EXOS/Switch Engine 33.5.2 GA Support	Added EXOS/Switch Engine 33.5.2 GA download image support for all ExtremeCloud IQ-supported SKUs, making it available as the latest image in the download dropdown.
XIQ-46919	EXOS/Switch Engine 32.7.3.15-patch1-33 Patch Support	Added EXOS/Switch Engine 32.7.3.15-patch1-33 patch support for onboarding, monitoring, and configuration for all ExtremeCloud IQ-supported SKUs through download image support.
XIQ-46920	EXOS/Switch Engine 32.7.3.15-patch1-33 GA Support	Added EXOS/Switch Engine 32.7.3.15-patch1-33 GA download image support for all ExtremeCloud IQ-supported SKUs.
XIQ-47382	EXOS/Switch Engine 33.5.2.118-patch1-6 GA Support	Added EXOS/Switch Engine 33.5.2.118-patch1-6 GA download image support for all ExtremeCloud IQ-supported SKUs.

Addressed Issues

Table 2 lists Addressed Issues in Extreme Platform ONE Networking release 25.7.0-175.

Table 2: Addressed Issues in release 25.7.0-175

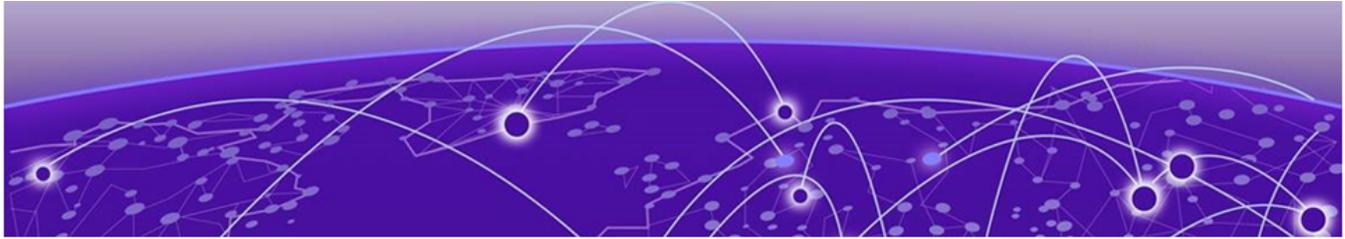
Issue ID	Description
Account Management	
WS-775	Addressed the issue where the Verify Email option in the Account Lockout Notification email takes you to the ExtremeCloud IQ application.
WS-1916	Addressed the issue where users with multiple accounts are unable to switch accounts or VIQs.
WS-3625	Addressed the issue where the account is listed incorrectly when switching from ExtremeCloud IQ to Extreme Platform ONE Networking.
XIQ-46551	Addressed the issue where updating user group in Credential Distribution Group threw an error indicating CDG already exists.

Table 2: Addressed Issues in release 25.7.0-175 (continued)

Issue ID	Description
Device Management	
XIQ-19379	Addressed the issue where APs were not deleted from ExtremeCloud IQ when released to cloud in managed case scenarios.
XIQ-46116	Addressed the issue where VLAN Probe status incorrectly showed Completed instead of Stopped when probe was manually stopped.
XIQ-46978	Addressed the issue where certain hostnames were not being imported from Ekahau during map import.
Onboarding	
CFD-16137	Addressed a licensing issue that prevented onboarding additional devices.
XIQ-44411	Addressed the issue by refactoring Thread Commissioner start and stop functionality to support multiple partitions and improve network recovery.
SSO	
WS-3831	Addressed the issue where the Other Organization section was hidden in the SSO account switcher popup when users switched to internal accounts. The section now displays properly after switching to an internal organization.
Troubleshooting	
XIQ-44023	Addressed the issue by updating AVC signature to the latest version for 32-bit and 64-bit platforms.
XIQ-47719	Addressed the issue where a schema change in hm_dev_license_type table broke AVRO debezium replication.
Upgrading	
XIQ-46736	Addressed the issue to set delta update as the default selection when updating device configurations.
XIQ-47339	Addressed the issue where the uns_notifier_email_app table DDL was different between configdb1 and configdb2.
User Interface	
WS-3733	Addressed the issue where External VIQ users could access restricted screens when switching from Internal VIQ screens they did not have access to.
XIQ-46206	Addressed the issue where the session duration filter in the Users monitoring page was not functioning correctly, displaying all users regardless of the selected filter criteria.
XIQ-46279	Addressed the issue where data usage for users was inconsistent with ExtremeCloud IQ after client reconnection.
XIQ-46400	Addressed the issue where user type pie chart count was displaying incorrect values.

Table 2: Addressed Issues in release 25.7.0-175 (continued)

Issue ID	Description
XIQ-46418	Addressed the issue where filtering users based on site selection in Monitor > Users page was not working correctly, returning zero results when individual sites were selected.
XIQ-46469	Addressed the issue where sorting on the Source column in the Monitor > Users page was not functioning as expected.
XIQ-46474	Addressed the issue where the sort functionality on the Session Duration column is not working as expected on the Users page.
XIQ-46511	Addressed the issue where the Custom Time Filter is not displaying proper results. It displays incorrect user entries on the Users page.
XIQ-46588	Addressed the issue where the where Users page was restricted to only 200 entries despite having more users in the system.
XIQ-46612	Addressed the issue where last page navigation icon was not clickable due to overlapping resource center icon.
XIQ-46637	Addressed the issue where the Users page returned a 400 error when no active clients were connected and only historic clients older than one day were present.
Visualize	
NVO-6936	Addressed the issue where users could not define MSTP region and revision values for EXOS and Switch Engine devices within the network policy switching section.
NVO-7309	Addressed the issue where no IP address associated with a VLAN displayed "No rows to show" message. The message now displays "No Additional Details" for better clarity.
NVO-9398	Addressed the issue where wireless floor plans failed to load for users with the Observer role.
NVO-10488	Addressed the issue where LLDP discovered devices without hostname displayed MAC address. The system now displays 'N/A' as a placeholder in link labels, tooltips, and Link Inspector.
NVO-10584	Addressed the issue where SSH launch option was not available for managed cloud-onboarded Fabric Engine devices.
NVO-11684	Addressed the issue where devices with Limited Features license could not be properly managed in visualization. Enhanced mixed mode to display all compatible devices on canvas and allow unlock full features option.
NVO-12343	Addressed the issue where SSH terminal feature had usability problems including disabled terminal for disconnected devices and keyboard navigation issues.
NVO-12410	Addressed the issue where subsequent configuration push failed for FE7830-32CE-8DE with LACP/LAG default trunk port type configuration.
NVO-13476	Addressed the issue where the user interface displayed devices as Limited Features even when Extreme Platform ONE licenses were assigned to the devices.



Known Issues

Table 3 lists the Known Issues in Extreme Platform ONE Networking release 25.7.2-184 (Patch 2).

Table 3: Known Issues in release 25.7.2-184 (Patch 2)

Issue ID	Description
9-dot Menu	
XCP-3475, XCP-10803, XCP-11090	Accessing applications from the 9-dot menu fails with Internal Server Errors.
Account Management	
WS-3868	When switching to an external account immediately after navigating from an internal account, the switch may not work on the first click in STAGING environment.
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.
XCP-9613	DevX runtime performance dashboard development for API utilization, notifications, and ITSM sync.
XCP-12725	Internal Grafana-based runtime performance dashboard development for API and notification monitoring.
XCP-12727	API rate limiting implementation needed for customer accounts, users, and tokens with appropriate KPI tracking.
XCP-13136	External release type and release notes information is missing for cloud managed device upgrade/firmware versions API. This requires dependency resolution with IT services for complete implementation.
XIQ-47766	Automatic configuration application to offline devices is not supported.
Browser Issues	
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	

Table 3: Known Issues in release 25.7.2-184 (Patch 2) (continued)

Issue ID	Description
XCP-5227, XCP-5268	Incorrect <code>Managed_by</code> 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.
XIQ-19320	WiFi interface transmission power values may not update correctly in Managed Device page after bulk edit operations.
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.
Inventory	

Table 3: Known Issues in release 25.7.2-184 (Patch 2) (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-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-17215	The failure toast "Device Failed to Onboard" disappears automatically after 10 seconds when a device onboarding attempt fails.
Licensing	
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.
Logs	
XCP-11224	The Audit Log displays API denied error log entries, which are not relevant.
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.
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.
WS-3519	External users with the Bizops role have access to the Visualization page.
XCP-10308	Manage or Unmanage actions are not performed for the NetSecOps role.
XCP-13153	Existing Monitor and Observer roles are converted to tenant admin post GDC upgrade on staging environment.
NVO-10726	An issue exists where external users with BizOps role have unauthorized access to the Visualization page despite role restrictions.
XIQ-45333	Manage/unmanage actions are not working for Extreme Platform ONE Networking BizOps role users, showing "something went wrong" error.

Table 3: Known Issues in release 25.7.2-184 (Patch 2) (continued)

Issue ID	Description
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.
Upgrading	
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-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-13051	While a firmware upgrade is in progress for a device in Extreme Platform ONE Networking it is deleted in ExtremeCloud IQ.
User Interface	
WS-3120	Intermittent logins receive a white screen with an incomplete load of the application.
WS-3873	The Workspace page is not displayed after logging in even if Extreme AI Expert is enabled.
XCP-5065	Search and Filter does not filter the appliance cluster.
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.
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-47931	Onboard, monitor, config, and drag-drop image operations are not supported in Fabric Engine and VOSS 9.3.2.
XIQ-47942	DPCap events are not appearing on the Client Monitor Diagnosis page.
Visualize	

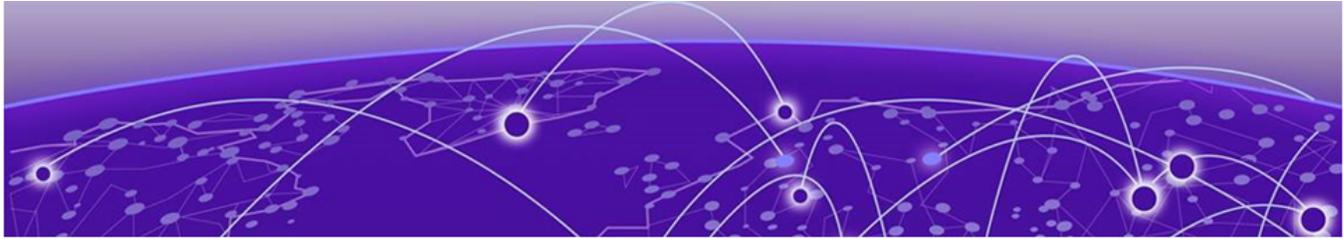
Table 3: Known Issues in release 25.7.2-184 (Patch 2) (continued)

Issue ID	Description
NVO-7899	Device action Configure Fabric needs to be restricted to Extreme Platform ONE Networking compatible buildings only.
NVO-8908	Node custom positions in topology are not retained on browser refresh.
NVO-13692	Onboarded devices may not appear in the Visualize page inspector panel.
NVO-10726, WS-3519	External users with the Bizops role have access to the Visualization page.

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

- [Universal Compute Platform](#) on page 21
- [Access Points \(Universal Hardware\)](#) on page 21
- [Switches \(Universal Hardware\)](#) on page 23

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 10.8.6 AP 10.17.1	IQ Engine 10.8.2
AP305C	IQ Engine 10.8.6 AP 10.17.1	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 10.8.6 AP 10.17.1	IQ Engine 10.8.2
AP305CX	IQ Engine 10.8.6 AP 10.17.1	IQ Engine 10.8.2
AP3000	IQ Engine 10.8.6 AP 10.17.1	IQ Engine 10.8.2
AP3000X	IQ Engine 10.8.6 AP 10.17.1	IQ Engine 10.8.2
AP4000	IQ Engine 10.8.6 AP 10.17.1	IQ Engine 10.8.2
AP4000-1	IQ Engine 10.8.6 AP 10.17.1	IQ Engine 10.8.2
AP4020	IQ Engine 10.8.6 AP 10.17.1	IQ Engine 10.8.2
AP410C	IQ Engine 10.8.6 AP 10.17.1	IQ Engine 10.8.2
AP410C-1	IQ Engine 10.8.6 AP 10.17.1	IQ Engine 10.8.2
AP460C	IQ Engine 10.8.6 AP 10.17.1	IQ Engine 10.8.2
AP460S6C	IQ Engine 10.8.6 AP 10.17.1	IQ Engine 10.8.2
AP460S12C	IQ Engine 10.8.6 AP 10.17.1	IQ Engine 10.8.2
AP5010	IQ Engine 10.8.6 AP 10.17.1	IQ Engine 10.8.2
AP5020	IQ Engine 10.8.6 AP 10.17.1	IQ Engine 10.8.2
AP5050U	IQ Engine 10.8.6 AP 10.17.1	IQ Engine 10.8.2
AP5050D	IQ Engine 10.8.6 AP 10.17.1	IQ Engine 10.8.2
AP510C/CX	IQ Engine 10.8.6 AP 10.17.1	IQ Engine 10.8.2

Switches (Universal Hardware)

Table 6: Required Firmware Versions for Switches

Device Family	Version	Devices
Switch Engine (single/ stacked)	33.5	<ul style="list-style-type: none"> • 4120 • 4220 • 5120 • 5320 • 5420 • 5520 • 5720 • 7520 • 7720
EXOS	33.5	<ul style="list-style-type: none"> • 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	9.3.0.0	<ul style="list-style-type: none">• 4120• 4220• 5120• 5320• 5420• 5520• 5720• 7520• 7720
VOSS	9.3.0.0	<ul style="list-style-type: none">• VSP7432CQ• VSP7400-48Y• VSP4900-48P• VSP4900-24XE• VSP4900-24S• VSP4900-12MXU-12XE