Extreme Platform ONE™ Networking v25.15.0-337 Component Update 25.15.1-4 Release Notes

New Features, Limitations, and Known Issues

9041309-01 Rev AA
November 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
Subscribe to Product Announcements v

General Release Information **7**
Current Release: 25.15.0-337 Component Update 25.15.1-4 7
Release: 25.15.0-337 Component Update 25.15.1-4 Addressed Issues 8
Release: 25.15.0-337 8
Introduction to Extreme Platform ONE Networking 8
Extreme Platform ONE Public IP Address Blocks 9
Supported Applications 10
Browser Support and Display Settings 10
Desktop Browsers 10
Display Settings 10

Previous Release **11**
New Features 11
Addressed Issues 12

Known Issues **15**
Limitations 21

Device Support Information **22**
Universal Compute Platform 22
Access Points (Universal Hardware) 23
Switches (Universal Hardware) 25
ExtremeCloud IQ Site Engine 26
Third-Party Management Engine 29



Abstract

This release notes document for Extreme Platform ONE™ Networking version 25.15.0-337 Component Update 25.15.1-4 (November 2026) describes platform enhancements, supported hardware and software, addressed defects, known issues, limitations, and deployment requirements for cloud-managed enterprise networking environments. This release addressed issues related to: MDM device ID and serial number synchronization, Agent ONE failed requests for client health data, and support for IQ Engine 10.9.2a and 10.8.5h. These emergency patch releases update the bundled PHP runtime to address critical vulnerabilities. Intended for administrators, network operations teams, and support engineers, the release notes provide intermediate-to-advanced technical guidance for deployment, upgrades, troubleshooting, and enterprise-scale network management.

Help and Support

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

Extreme Portal

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

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.

4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

General Release Information

Browser Support and Display Settings on page 10

Current Release: 25.15.0-337 Component Update 25.15.1-4

November 2026

This release delivers key platform stability and resilience enhancements to ensure uninterrupted real-time monitoring, event logging, and SD-WAN management. These updates eliminate background pipeline delays and improve connection handling, ensuring telemetry and event timelines remain continuous and management sessions remain fully responsive during platform maintenance. It also improves data consistency in the device IP routing analytics REST API by restoring standard date-time formatting for ping protection event timestamps.

Related Links

- Known Issues on page 15
- Device Support Information on page 22

Release: 25.15.0-337 Component Update 25.15.1-4 Addressed Issues

Table 1 lists Addressed Issues in Extreme Platform ONE Networking release 25.15.0-337 Component Update 25.15.1-4.

Table 1: Addressed Issues in Release 25.15.0-337 Component Update 25.15.1-4

Issue ID	Description
CFD-18584	Addressed an issue where the Security Policy Engine was unable to match device rules during EAP-TLS authentication for devices synchronized from MDM platforms. MDM device IDs and serial numbers are now properly synchronized and evaluated during certificate authentication.
CFD-18883	Addressed the issue where requests for wireless client health data, including the Performance Monitoring client health API and queries from Agent ONE, can sometimes fail with an HTTP 400 (Bad Request) error, code 1728, resulting in Agent ONE providing incomplete or incorrect answers about wireless client health and the wrong number of connected clients.
NVO-20680	Extreme Platform ONE Networking now supports IQ Engine 10.9.2a and 10.8.5h. These emergency patch releases update the bundled PHP runtime to address critical vulnerabilities CVE-2026-109618 and CVE-2026-109619, and Extreme Networks recommends upgrading affected access points as soon as possible.

Release: 25.15.0-337

October 2026

Related Links

- Known Issues on page 15
- Device Support Information on page 22

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 Extreme Agent ONE™ Coworker—your contextual helper. Powered by the latest in AI technology, Agent ONE Coworker 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
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.
- Universal ZTNA: 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 12

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

New Features

Table 2 on page 12 lists the new features introduced in Extreme Platform ONE Networking release 25.15.0-337.

For more information about Extreme Platform ONE Networking features, see the Extreme Platform ONE Networking v25.15.0 User Guide.

Device OS Support

This release supports the following device operating systems.

- Switch Engine/EXOS**:**
  - IQAgent Version
    - Switch Engine/EXOS release < 31.7: upgrade to IQAgent version 0.9.32
    - Switch Engine/EXOS release >= 31.7 < 33.2 upgrade to IQAgent version 0.9.45
    - Switch Engine/EXOS Engine release >= 33.2 upgrade to IQAgent version 1.9.45
  - 33.7.1.6-patch1-26 Latest Supported GA Patch

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

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

    Onboard, Monitor, Config, Image Mgmt, and Global Download Support
  - 31.7.4.2-patch1-7 Previous Supported GA Image

    Onboard, Monitor, Config, Image Mgmt, and Global Download Support
- Fabric Engine/VOSS**:**
  - IQ Agent Support
    - XA1400 series 0.7.4
    - All others 0.9.45
  - 9.4.2.0 Latest Supported GA Image

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

- 9.3.4.0 Previous Supported GA Patch

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

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

- IQ Engine **Support:**
  - IQ Engine release 10.9.2

New Hardware Support

Extreme Platform ONE contains no new hardware in this release.

Table 2: New Features in release 25.15.0-337

Feature ID	Feature	Description
XIQ-52684	Fabric Engine/ VOSS Version 9.4.2 Support	Adds support for onboarding, monitoring, configuring, and downloading images for Fabric Engine/VOSS version 9.4.2 on the 7830, 7720, 7520, 5720, 5520, 5420, 5320, and applicable 4220 Universal Switches, and on the VSP7400 and VSP4900.
XIQ-52850	Switch Engine/ EXOS 33.7.1.6-patch1-26 GA Download Image Support	Support is now offered for global image download for Switch Engine/EXOS 33.7.1.6-patch1-26 for all supported Switch Engine/EXOS SKUs, both single and stacked. The following images are available in the download dropdown: 31.7.4.2-patch1-7, 32.7.4.15.patch1-11, 33.7.1.6.patch1-26, and 34.1.1. No other images are available.

Addressed Issues

Table 3 lists Addressed Issues in Extreme Platform ONE Networking release 25.15.0-337.

Table 3: Addressed Issues in release 25.15.0-337

Issue ID	Description
CFDs	
CFD-18361	Addressed the issue where the **Locked Users** page displayed an unknown error in Extreme Platform ONE Networking and ExtremeCloud IQ (Classic), which prevented unlocking users.
CFD-18419	Addressed the issue where creating a custom AP template for the AP305cx displayed an unknown error in Extreme Platform ONE Networking and ExtremeCloud IQ (Classic).
Device Management	
XCP-26914	Addressed the issue where unmanaging and then managing a TPME managed device caused the ad hoc configuration backup task to appear as scheduled, and no further tasks appeared in **Task Center**.
Roles	

Table 3: Addressed Issues in release 25.15.0-337 (continued)

Issue ID	Description
XCP-26861	Addressed the issue where data for a TPME and its managed devices did not appear in Device360 for users with the Observer role.
XCP-27338	Addressed the issue where users with the NetSecOps (External) role could not start an SSH session to TPME-managed devices from the **Inventory** and **Network Devices** pages.
Upgrading	
XCP-25556	Addressed the issue where a firmware upgrade failed with a "Something went wrong" error when a custom firmware image had the same version as an existing global image.
XCP-27263	Addressed the issue where the **Scope** column for a completed bulk firmware upgrade task in **Task Center** displayed an incorrect device count, or a MAC address or serial number, after devices that were in the task were deleted.
XCP-27484	Addressed the issue where the firmware upgrade initiation notification displayed an error without information about the started upgrades when an upgrade started for only some of the selected devices.
XCP-28228	Addressed the issue where selecting a firmware image for a TPME-managed device intermittently selected an incorrect image.
User Interface	
WS-4773, WS-4784, WS-4792	Addressed the issues where the navigation menu expanded to the full width of the mobile screen and the AI widget appeared above the menu, where the switcher menu did not appear in the app bar in the mobile view, and where the date picker pop-up appeared cropped in the vertical view of tablet devices.
XCP-24119	Addressed the issue where the delete dialog on the **Inventory** and **Network Devices** pages displayed the **Delete Configuration** option for devices that do not support it. The option applies only to cloud-managed IQ Engine access points.
XCP-24557	Addressed the issue where the **Usage and Capacity** widget on the **Dashboard** does not include issue counts for stack devices.
XCP-26969	Addressed the issue where a **Task Center** entry was removed after an **Add Application** task completed when you selected an application that was already installed on a UCP device.
XCP-27310	Addressed the issue where an updated TPME hostname was not reflected on the **Inventory** and **Network Devices** pages.
XCP-27903	Addressed the issue where SSH sessions to appliance cluster members failed from the **Inventory**, Device360, and **Network Devices** pages.
XCP-28423	Addressed the issue where Client360 did not display information for a connected client.

Table 3: Addressed Issues in release 25.15.0-337 (continued)

Issue ID	Description
XCP-28868	Addressed the issue where selecting the export icon in the table on the **Inventory** page displayed a Bad Request error instead of downloading the table content as a CSV file.
XCP-29289	Addressed the issue where the **Feature Navigator** of the Configuration Profile displayed the unsupported options **Inventory Scheduler** and **Management Profile**.

Known Issues

Table 4 lists the Known Issues in Extreme Platform ONE Networking release 25.15.0-337 Component Update 25.15.1-4.

Table 4: Known Issues in release 25.15.0-337 Component Update 25.15.1-4

Issue ID	Description
CFD	
CFD-18080	In the current release, the **Clients** view displays only actively connected clients by default. As a result, clients are removed from the main **Clients** list shortly after they disconnect. Previously connected clients can still be viewed by applying the Disconnected filter. This behavior is a known limitation and is functioning as designed. A future release is planned to introduce enhanced historical client visibility and remove the current restriction that limits the default view to connected clients only.
API	
XCP-23938	The release 25.12 database schema migration introduced NOT NULL columns without defaults to platform_common_db CDC tables, causing the Debezium AVRO connector to fail with a schema registry incompatibility error.
XCP-23971, XCP-24089	On the **Device360 Port Stats** and **Clients** pages, graphs and UI widgets (including the Port Stats graph, Port Description grid, Port Stats Summary, Link PoE, and Usage/Utilization widgets) pull data from the legacy monitoring APIs instead of from the PerfMonitor APIs.
XCP-26696, XCP-26702, XCP-26712	The `cs-metastore-event-ingestion`, `xcloudiq-license-scheduler`, CAS, and CNS applications are deployed with a single replica and without a configured health check.
Device Management	
XCP-17157	Extreme Platform ONE Networking does not support setting or updating the Third-Party Management Engine (TPME) hostname using the **Configure** option. This is a documented limitation.
XCP-18640	The **Retry** action is disabled after the configuration deployment fails for the Third-Party Management Engine.
XCP-19055	The RESET VIQ operation does not remove configuration data. Configuration Profiles and Access Profiles remain intact after the reset, leaving the VIQ in an inconsistent state.

Table 4: Known Issues in release 25.15.0-337 Component Update 25.15.1-4 (continued)

Issue ID	Description
XCP-21438	The Extreme Platform ONE Security application displays an Auto-Logout popup when the Extreme Platform ONE Networking idle session timeout is reached because Extreme Platform ONE Security reads its own 30-minute default timeout instead of the Extreme Platform ONE Networking session configuration.
XCP-22265	Export and import of VIQ, backup and restore of VIQ does not work properly if the TPME or ExtremeCloud IQ Site Engine is present.
XCP-23121	Client entries are not removed from the Client table when a device transitions to an unmanaged state.
XCP-23565	In scaled environments with 24,000 wired clients, only approximately 18,345 clients are displayed in the **Client Health** page; all clients are visible in ExtremeCloud IQ (Classic).
XIQ-19320	Wi-Fi Interface Transmission power values may not update correctly on the **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-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 some countries.
XIQ-36259	Importing an Ekahau planner file does not import all walls.
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 supported SKUs.
XIQ-51481	Firmware upgrade for AP4060 series access points is not available. The access points do not appear in the **Upgrade Firmware** selection, and the upgrade does not complete when initiated from the device 3-dot menu.
XIQ-52230	In Extreme Platform ONE 25.12.0, you must push the update to the AP first, and then push the update to the Tunnel Concentrator.
XIQ-52706	Resetting a VIQ can result in unrecoverable data loss if the backup used for restoration is incomplete or the restore operation fails. The current Backup and Restore capability does not yet include all Extreme Platform ONE data. Verify that all required data has been exported before initiating a Reset VIQ operation.
Inventory	

Table 4: Known Issues in release 25.15.0-337 Component Update 25.15.1-4 (continued)

Issue ID	Description
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.
Logs	
XIQ-47371	Multiple logs are generated for both single and bulk device deletions.
Onboarding	
WS-3579	Notifications are sometimes split into two messages during certain user actions such as onboarding or device deletion operations.
Roles	
CFD-16351, XCP-11511	An issue exists where Extreme Platform ONE Networking does not restrict admin visibility based on location, affecting only the Observer and the Operator roles.
XCP-10308	**Manage** or **Unmanage** actions are not performed for the NetSecOps role.
XCP-24515	Users with the Observer (Read Only) role can see and click the select-all check box in the **Alerts** page table header, which should be hidden for read-only users.
XIQ-45333, XIQ-45477	Manage/Unmanage actions are not working for Extreme Platform ONE Networking BizOps role users, showing the "something went wrong" error, and for NetSecOps role users with Write access to inventory, resulting in permission errors.
SSO	
XCP-8507	The login button does not activate for certain SSO-enabled user login instances.
XCP-22975	When logging out of an SSO account and logging back in with a different SSO user, the system may incorrectly display the previous user's account information. This occurs because session data from the prior login is not fully cleared on logout. **Workaround:** Fully close the browser (all tabs and windows) after logging out of the SSO account before logging in with the new user.
XIQ-49634	When switching to a different SSO account from ExtremeCloud IQ, you are redirected to Extreme Platform ONE Networking but remain on the original SSO account.
Troubleshooting	
XIQ-48210	Downloading the AFC Geolocation report produces a corrupt file that is not in the expected CSV format, making it unusable for troubleshooting.
Upgrading	

Table 4: Known Issues in release 25.15.0-337 Component Update 25.15.1-4 (continued)

Issue ID	Description
N/A	Starting in 25.14.0, firmware upgrades use the new V2 API (DLCS) and upgrade activity is tracked in **Task Center** rather than the **Firmware History** page. Existing entries from 25.13.0 and earlier remain visible in **Firmware History**, but any new upgrade initiated in 25.14.0 or later will appear only in **Task Center**. The **Reschedule**, **Cancel**, and **Retry** actions are no longer available in **Firmware History**. Support for these actions in **Task Center** is targeted for a future release.
XCP-12063, XCP-12064, XCP-16651	An audit log is not generated for a scheduled a firmware upgrade, when firmware upgrade successfully completes, or when a firmware upgrade fails.
XCP-17804	Following an upgrade, certain data schemas may fail to register due to compatibility conflicts with previously stored schema versions. This can prevent some telemetry and client event data from being processed correctly until the issue is resolved.
User Interface	
NVO-15001	Port Description in **Link & Port Details** for devices managed by TPME contain incorrect values.
WS-4616	When an existing user clicks the **Pendo Resource Center** icon in Extreme Platform ONE Networking, the **Product Tours** section does not appear.
WS-4783	On mobile devices, the AI Expert widget does not fit the screen size, and dragging the widget works inconsistently.
WS-4785	On mobile devices, data on the internal users page of Access Management does not load until you rotate the device to landscape orientation and back to portrait orientation. The page layout also breaks when you scroll horizontally.
WS-4793	On mobile devices in portrait orientation, the account switcher pop-up does not display accounts until you rotate the device to landscape orientation.
XCP-4999	Currently, when filtering on a switch stack, when 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-18729	When viewing the **Device 360** page for a TPME-managed device, the Model field displays as "Unknown" instead of the actual device model. All other device details are unaffected.
XCP-19002	Fabric Attach links display as operationally down in the visualization even when they are operationally up. This issue affects Switch Engine downstream and SMLT Cluster upstream configurations that use Fabric Attach without authentication.
XCP-19865	No failure details are displayed in the user interface when a TPME configuration deployment fails. The deployment API response confirms a failed status but does not include a failure reason, and no corresponding audit log entry is generated.
XCP-20134	The filter chip for the Extreme Platform ONE Networking selection in the Application Access column filter in **Access Management** is not displayed, preventing confirmation that the filter has been applied.

Table 4: Known Issues in release 25.15.0-337 Component Update 25.15.1-4 (continued)

Issue ID	Description
XCP-21438	When the Extreme Platform ONE Networking idle session timeout is reached while navigating Universal ZTNA through the 9-dot menu, Universal ZTNA displays an "Auto-Logout in 1528 seconds" pop-up instead of following the Extreme Platform ONE Networking idle timeout behavior.
XCP-22682	Management port statistics are not displayed on the **Usage and Capacity** page for Switch Engine/EXOS devices that have all standard ports disabled.
XCP-22746	The **Total Client** count on the **Usage and Capacity** page returns 0 for wired devices, even when client entries exist for those devices.
XCP-23090	Device health issue reporting latency has increased. Temperature issues on Fabric Engine devices now take approximately 3 to 4 minutes to appear under **Device Health**, compared to approximately 1 minute in previous releases.
XCP-23112	When a filter is applied on the **Device Health** page, other columns such as **CPU Usage%**, **Memory Usage%**, and **PSU Usage%** display N/A. This behavior applies to all **Device Health** issue filters.
XCP-23128	IPv4 and IPv6 null values (N/A) are not sorted correctly during ascending and descending sort operations on the client table. Null values appear at the end during ascending sort and not at the beginning during descending sort.
XCP-23139	Extreme Platform ONE Networking displays N/A for all metrics in the second row for a Switch Engine/EXOS switch in the **Device Health** and **Usage and Capacity** pages when multiple Switch Engine/EXOS switches are onboarded.
XCP-23307	Filter options and **Edit**/**Delete** actions are not available for Subscription & Licensing request history.
XCP-23406	The **Total Queue Congestion Packets** column under **Usage & Capacity** > **Wired** displays an incorrect value for Stack devices.
XCP-23436	The **Total Throughput (RxPktsPerSec / TxPktsPerSec)** column in the wired device grid on the **Usage & Capacity** page intermittently displays 0 or no value for devices that are actively transmitting traffic.
XCP-23450	A duplicate device row appears on the **Usage and Capacity** page.
XCP-24182	When no client issues are detected, the **Client Health** page displays '0 data found' instead of a 'No Issues' confirmation indicator.
XCP-24477	When navigating to the **Assets** page with an invalid `x.tab` parameter, the application defaults to the **All** tab correctly but does not remove the invalid parameter from the URL.
XCP-24524	The site ID is missing from the sites with issues grid response.
XCP-24537	The **Discovered** tab in the Assets/Inventory page uses 'unknown' as the URL parameter value instead of 'discovered', creating a mismatch between the user interface label and the URL parameter.
XCP-27325	**Task Center** displays change_me as the location for firmware upgrades of unassigned cloud native devices.

Table 4: Known Issues in release 25.15.0-337 Component Update 25.15.1-4 (continued)

Issue ID	Description
XCP-27843	Clarified CPU and memory utilization support in Performance Monitoring: CPU and memory statistics are supported on newer device platforms; legacy CAPWAP devices (such as AP4000 and AP410C) do not report these metrics to Performance Monitoring and may display a value of 0%.
XIQ-42050, XIQ-42051	Issues exist with FIPS enabled filters. The **Manage Application** page displays all applications instead of filtering to show only FIPS-enabled applications, and the **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-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-49488	The **Client Density** heatmap displays an inaccurate client count that does not match the count shown on the client **Inventory** page.
XIQ-51408	The **Inventory** page displays the **Upgrade Firmware** action for controllers, which is not a supported action for controllers.
XIQ-52081	When navigating to the **Clients** page from the **Client Health** widget on the Dashboard, switching between the Wired and Wireless tabs may cause continuous page flickering and rapid URL alternation. This issue occurs only when the **Clients** page is accessed through the Dashboard widget; accessing the **Clients** page directly is not affected. **Workaround:** Navigate to the **Clients** page directly from the menu rather than through the **Client Health** widget on the Dashboard, or refresh the page if flickering occurs.
XIQ-52087	The **Roaming Issues** filter on the **Clients** > **Wireless** widget returns clients with no roaming issues instead of clients that have roaming issues.
Visualize	
NVO-15660	A Link Aggregation Group (LAG) configured between an EXOS/Switch Engine switch and an access point intermittently loses its LAG visualization on the network canvas and displays as a single link. The LAG configuration is correctly shown on both the Switch Engine/EXOS device and the AP, but the visualization canvas fails to consistently represent the aggregated link bundle.
NVO-15748	The **Visualization** page and **Device Inspector** panel do not update the device IP address after the management IP address is manually changed. The updated IP address displays correctly in the **Network Devices** page and **Device 360**.

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 22
Access Points (Universal Hardware) on page 23
Switches (Universal Hardware) on page 25
ExtremeCloud IQ Site Engine on page 26
Third-Party Management Engine on page 29

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.

Note
Extreme Platform ONE Networking and ExtremeCloud IQ support onboarding only for homogeneous stacks. Stacks consisting of different models (mixed mode, mixed platforms) are not supported. Mixed stacks can be managed by ExtremeCloud IQ Site Engine.

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 5: Required Firmware Versions for Universal Compute Platform

Device Model	Latest Supported Release	Comments
ExtremeCloud Edge (UCP)	5.15.01	Supported hardware models: 1130C 2130C 3150C 3160C 4120C

Access Points (Universal Hardware)

Table 6: Required Firmware Versions for Universal Hardware Access Points

Device Model	Latest Supported Release	Recommended Sustaining Release	Recommended Minimum Release
AP302W	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP305C	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP305C-1	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP305CX	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP3000	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP3000X	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP3020/W/X	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.5
AP4000	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP4000-1	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP4020/X/FX	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.4
AP4060	IQ Engine 10.9.1 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.4
AP410C	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP410C-1	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP460C	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP460S6C	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP460S12C	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP5010	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP5020	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2

Table 6: Required Firmware Versions for Universal Hardware Access Points (continued)

Device Model	Latest Supported Release	Recommended Sustaining Release	Recommended Minimum Release
AP5022/FX/S6D	IQ Engine 10.9.2 AP 10.20.1	N/A	N/A
AP5050U/D	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP5060U/D	IQ Engine 10.9.2 AP 10.20.1	N/A	N/A
AP510C/CX	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2

Switches (Universal Hardware)

Table 7: Required Firmware Versions for Switches

Device Family	Version	Devices
Switch Engine (single/ stacked)	33.6.1.14	• 4120 • 4220 • 5120 • 5320 • 5420 • 5520 • 5720 • 7520 • 7720
EXOS	33.6.1.14	• 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 7: Required Firmware Versions for Switches (continued)

Device Family	Version	Devices
Fabric Engine	9.4.1.0	• 4220 • 5320 • 5420 • 5520 • 5720 • 7520 • 7720
VOSS	9.4.1.0	• VSP7432CQ • VSP7400-48Y • VSP4900-48P • VSP4900-24XE • VSP4900-24S • VSP4900-12MXU-12XE

ExtremeCloud IQ Site Engine

ExtremeCloud IQ Site Engine Version	Supported Features
25.8.13	• License allocation • Device Assignment to the Extreme Platform ONE • Device Statistics • Port Statistics • Unmanage/Manage device • Device Group to CCG mapping • Stack members • NAC details update for wireless end-systems • Wired end-systems reported to Extreme Platform ONE • Detect and report orphaned devices • Compatible with Extreme Platform ONE subscriptions
25.11.10	• License allocation • Device Assignment to the Extreme Platform ONE • Device Statistics • Port Statistics • Unmanage/Manage device • Device Group to CCG mapping • Stack members • NAC details update for wireless end-systems • Wired end-systems reported to Extreme Platform ONE • Detect and report orphaned devices • Compatible with Extreme Platform ONE subscriptions

ExtremeCloud IQ Site Engine Version	Supported Features
25.11.11	• License allocation • Device Assignment to the Extreme Platform ONE • Device Statistics • Port Statistics • Unmanage/Manage device • Device Group to CCG mapping • Stack members • NAC details update for wireless end-systems • Wired end-systems reported to Extreme Platform ONE • Detect and report orphaned devices • Compatible with Extreme Platform ONE subscriptions
25.11.12	• License allocation • Device Assignment to the Extreme Platform ONE • Device Statistics • Port Statistics • Unmanage/Manage device • Device Group to CCG mapping • Stack members • NAC details update for wireless end-systems • Wired end-systems reported to Extreme Platform ONE • Detect and report orphaned devices • Compatible with Extreme Platform ONE subscriptions
26.02.10	• License allocation • Device Assignment to the Extreme Platform ONE • Device Statistics • Port Statistics • Unmanage/Manage device • Device Group to CCG mapping • Stack members • NAC details update for wireless end-systems • Wired end-systems reported to Extreme Platform ONE • Detect and report orphaned devices • Compatible with Extreme Platform ONE subscriptions
26.02.11	• License allocation • Device Assignment to the Extreme Platform ONE • Device Statistics • Port Statistics • Unmanage/Manage device • Device Group to CCG mapping • Stack members • NAC details update for wireless end-systems • Wired end-systems reported to Extreme Platform ONE • Detect and report orphaned devices • Compatible with Extreme Platform ONE subscriptions

ExtremeCloud IQ Site Engine Version	Supported Features
26.02.12	• License allocation • Device Assignment to the Extreme Platform ONE • Device Statistics • Port Statistics • Unmanage/Manage device • Device Group to CCG mapping • Stack members • NAC details update for wireless end-systems • Wired end-systems reported to Extreme Platform ONE • Detect and report orphaned devices • Compatible with Extreme Platform ONE subscriptions
26.02.13	• License allocation • Device Assignment to the Extreme Platform ONE • Device Statistics • Port Statistics • Unmanage/Manage device • Device Group to CCG mapping • Stack members • NAC details update for wireless end-systems • Wired end-systems reported to Extreme Platform ONE • Detect and report orphaned devices • Compatible with Extreme Platform ONE subscriptions
26.06.10	• License allocation • Device Assignment to the Extreme Platform ONE • Device Statistics • Port Statistics • Unmanage/Manage device • Device Group to CCG mapping • Stack members • NAC details update for wireless end-systems • Wired end-systems reported to Extreme Platform ONE • Detect and report orphaned devices • Compatible with Extreme Platform ONE subscriptions
26.06.11	• License allocation • Device Assignment to the Extreme Platform ONE • Device Statistics • Port Statistics • Unmanage/Manage device • Device Group to CCG mapping • Stack members • NAC details update for wireless end-systems • Wired end-systems reported to Extreme Platform ONE • Detect and report orphaned devices • Compatible with Extreme Platform ONE subscriptions

ExtremeCloud IQ Site Engine Version	Supported Features
26.08.10	• License allocation • Device Assignment to the Extreme Platform ONE • Device Statistics • Port Statistics • Unmanage/Manage device • Device Group to CCG mapping • Stack members • NAC details update for wireless end-systems • Wired end-systems reported to Extreme Platform ONE • Detect and report orphaned devices • Compatible with Extreme Platform ONE subscriptions
26.08.11	• License allocation • Device Assignment to the Extreme Platform ONE • Device Statistics • Port Statistics • Unmanage/Manage device • Device Group to CCG mapping • Stack members • NAC details update for wireless end-systems • Wired end-systems reported to Extreme Platform ONE • Detect and report orphaned devices • Compatible with Extreme Platform ONE subscriptions
26.08.12	• License allocation • Device Assignment to the Extreme Platform ONE • Device Statistics • Port Statistics • Unmanage/Manage device • Device Group to CCG mapping • Open Site Engine with SSO • Stack members • NAC details update for wireless end-systems • Wired end-systems reported to Extreme Platform ONE • Detect and report orphaned devices • Compatible with Extreme Platform ONE subscriptions

Third-Party Management Engine

The Third-Party Management Engine (model TPME-S) is upgraded to the latest version automatically. No user action is needed. The component may restart if an operating system upgrade is required.

Table 8 lists the TPME-managed switches that are supported for configuration backup and restore and firmware upgrade.

Table 8: Third-Party Management Engine feature support matrix

Company	Family	Configuration		Firmware Upgrade	Protocol	SSH Session (WebSSH)	LLDP Maps
		Backup	Restore				
Aruba	ArubaOS	Yes	Yes	Yes	SCP	Yes	No
Aruba/HPE	AOS-CX	Yes	Yes	Yes	SCP	Yes	No
Cisco Systems	IOS-XE	Yes	Yes	Yes	SCP	Yes	Yes
Enterasys Networks	S/K/71xx	Yes	Yes	No	SCP	Yes	Yes
Extreme Networks	Summit (EXOS version 16.2 or later)	Yes	Yes	Yes	SCP	Yes	Yes
	VSP (VOSS version 8.6 or later)	Yes	Yes	Yes	SCP	Yes	Yes