Extreme Platform ONE Networking v25.11.0-280 (Patch 3) Release Notes

New Features, Limitations, and Known Issues

9041152-04 Rev AA
August 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/

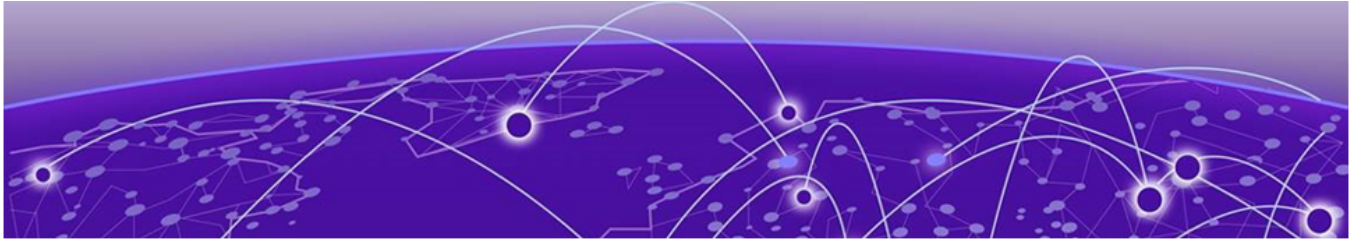


Table of Contents

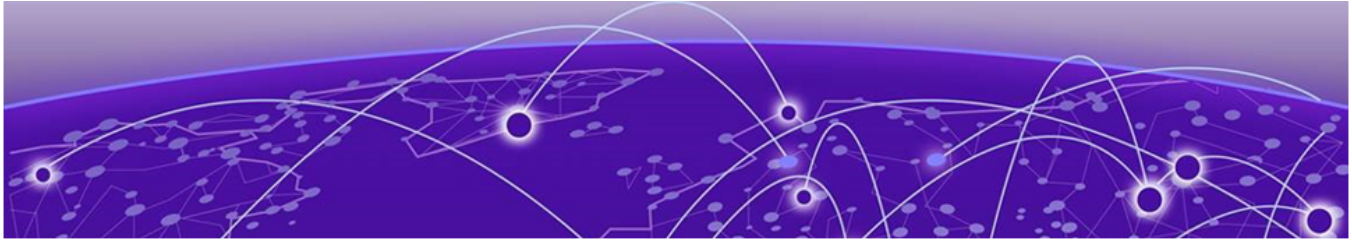
Abstract **4**
Help and Support v
Subscribe to Product Announcements v

General Release Information **7**
Current Release: 25.11.0-280 (Patch 3) 7
Release: 25.11.0-280 (Patch 3) Addressed Issues 7
Release: 25.11.0-280 (Patch 2) 7
Release: 25.11.0-280 (Patch 2) Addressed Issues 8
Release: 25.11.0-280 (Hotfix 1) 8
Release: 25.11.0-280 (Patch 1) 9
Release: 25.11.0-280 9
Introduction to Extreme Platform ONE Networking 9
Extreme Platform ONE Public IP Address Blocks 10
Supported Applications 11
Browser Support and Display Settings 11
Desktop Browsers 11
Display Settings 12

Previous Release **13**
New Features 13
Addressed Issues 18

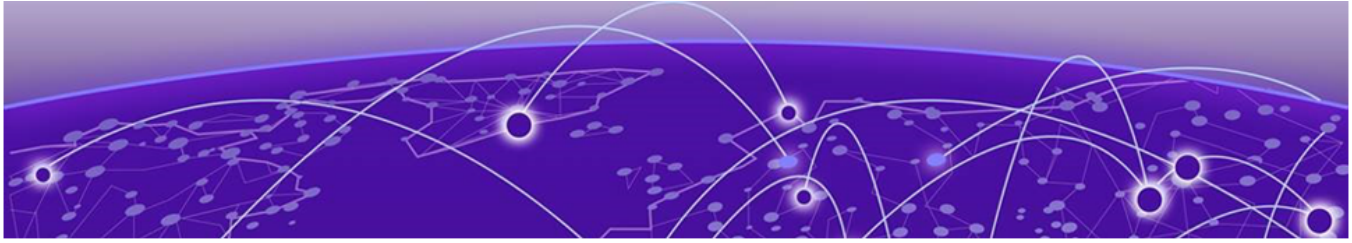
Known Issues **26**
Limitations 31

Device Support Information **32**
Universal Compute Platform 32
Access Points (Universal Hardware) 33
Switches (Universal Hardware) 35
ExtremeCloud IQ Site Engine 37



Abstract

This release notes document for Extreme Platform ONE Networking version 25.11.0-280 (Patch 3) provides a technical overview of a cloud-managed networking platform that unifies ExtremeCloud IQ, SD-WAN, security, analytics, and third-party device management within a centralized interface. It details core functionality such as device onboarding, inventory and lifecycle management, SSO-based authentication, AI-assisted diagnostics, alerting, topology visualization, and firmware lifecycle control across distributed, multi-site deployments. This release addresses an issue where IQ Agent overwrites any user-configured power monitor trap settings on the switch and reports an issue where performance monitoring data may be delayed or temporarily unavailable due to an internal database processing issue. It outlines deployment prerequisites, supported hardware and firmware versions, and interoperability constraints, while documenting addressed defects in APIs, RBAC, UI, and topology accuracy, alongside known issues such as API inconsistencies, UI limitations, and onboarding constraints. The guide supports intermediate to advanced administrators with troubleshooting, configuration guidance, scalability considerations, and secure network operations.



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 11

Current Release: 25.11.0-280 (Patch 3)

August 2026

Related Links

- Known Issues on page 26
- Device Support Information on page 32

Release: 25.11.0-280 (Patch 3) Addressed Issues

Issue ID	Description
CFD-16527	Addressed the issue where IQ Agent overwrote any user-configured power monitor trap settings on the switch whenever it connected or restarted. IQ Agent now applies trap settings only to switches with factory-default settings.
XCP-25328	In some environments, performance monitoring data may be delayed or temporarily unavailable due to an internal database processing issue. Background data aggregation jobs are running continuously without completing on schedule, which can increase system load and slow the availability of performance metrics and analytics.

Release: 25.11.0-280 (Patch 2)

July 2026

This release fixes several post-release issues: the Elasticsearch cluster was upgraded from v7.17 to v8.19 with two related regressions patched — a Kafka/schema registry queue buildup and the CoPilot Anomaly API returning empty results. Device usage and capacity data is restored through the XIQ API, configuration pushes no longer fail on older ExtremeCloud IQ Engine versions (pre-10.8.7) with large IP Firewall rule sets. Also, a Helm chart deployment defect in the Performance Monitor API was fixed for environment-agnostic GCP auth configuration.

Related Links

- Known Issues on page 26

- Device Support Information on page 32

Release: 25.11.0-280 (Patch 2) Addressed Issues

Issue ID	Description
CFD-17677	Addressed the issue where access points running IQ Engine firmware earlier than 10.8.7 failed to receive configuration updates when an IP firewall policy contained more than approximately 32 rules after upgrading to ExtremeCloud IQ release 25.11.0.
XCP-24649	Addressed the issue where direct client event ingestion was suspended after upgrading the release 25.11 hotfix, so that wired and wireless device usage and capacity client column data is now retrieved directly from the ExtremeCloud IQ API and returned as part of the API output.
XCP-24874	Addressed the issue in the `perfmonitor-api` Helm chart where the `GCP_AUTH_URL` and `GCP_AUTH_CREDS` environment variables were hardcoded in a way that prevented successful deployment across different environments. These variables have been updated with proper templating to support flexible, environment-agnostic deployments.
XIQ-50701	Upgraded the Elasticsearch cluster from version 7.17 to 8.19. To ensure application continuity during the transition, REST API Compatibility Mode was enabled, allowing existing 7.17 clients to communicate with the 8.x cluster without disruption.
XIQ-51661	Addressed the issue where monitoring queues accumulated across multiple region, resulting in stale monitoring metrics being displayed to customers after upgrading to ExtremeCloud IQ release 25.11.0.
XIQ-51749	Addressed the issue where the CoPilot Anomaly API returned empty results due to shard failures caused by the `indices.id_field_data.enabled` setting being disabled by default in Elasticsearch 8.x. Anomaly search queries sorting on the `_id` field failed during the sort phase, causing hits to be dropped silently.

Release: 25.11.0-280 (Hotfix 1)

July 2026

This release resolves an issue where configuration pushes failed for APs running ExtremeCloud IQ Engine versions prior to 10.8.7 when an IP Firewall policy contained more than approximately 25–32 rules.

Related Links

- Known Issues on page 26
- Device Support Information on page 32

Release: 25.11.0-280 (Patch 1)

July 2026

This release hardens security and restricts API key access to user management endpoints. It also resolves issues with inactive client purge events and improves Devices API results. Additionally, legacy ExtremeCloud IQ APIs are supported for populating wired and wireless client health, providing a reliable fallback option if blocking issues are encountered.

Related Links

- Known Issues on page 26
- Device Support Information on page 32

Release: 25.11.0-280

June 2026

This release includes enhancements to Third-Party Management Engine (TPME) expansion, Device 360 (D360) views, Wi-Fi 7 troubleshooting, RadSec authentication, configuration repository support (FTP/SCP/TFTP), WIPS alerting, and improved firmware upgrade workflows, with extended OS support for Switch Engine/EXOS, Fabric Engine/VOSS, and IQ Engine platforms.

Related Links

- Known Issues on page 26
- Device Support Information on page 32

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

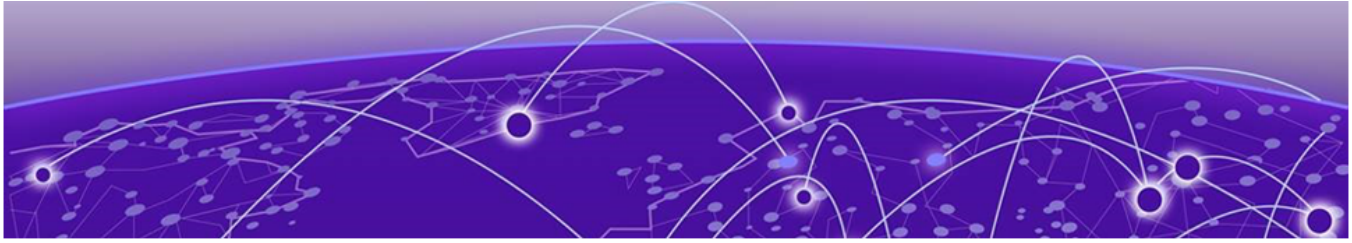
Extreme Platform ONE supports the latest 64-bit versions of the following desktop browsers:

- 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 13
Addressed Issues on page 18

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

New Features

Table 1 on page 14 lists the new features introduced in Extreme Platform ONE Networking release 25.11.0-280.

For more information about Extreme Platform ONE Networking features, see the Extreme Platform ONE Networking v25.11.0 User Guide.

Device OS Support

This release supports the following device operating systems.

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

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

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

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

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

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

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

- 9.2.1.1 Previous Supported GA Image

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

- IQEngine Support:
  - IQEngine release 10.8.7

New Hardware Support

Extreme Platform ONE Networking contains no new hardware in this release.

Table 1: New Features in release 25.11.0-280

Feature ID	Feature	Description
SEN-584	Third-Party Management Engine OVA Guest OS Version Support	Updates the Third-Party Management Engine (TPME) OVA guest OS version to support VMware vSphere Client versions 8.x and 6.7.0.54000.
WS-3925	Preferred Language Selection	Users can select their preferred display language from the profile center. Each user sets their own language preference independently of other users in the same organization. Supported languages include Portuguese (Brazil), French, Mandarin (Simplified Chinese), Italian, and Hindi, with English as the default.
WS-4449	Enhanced Email Validation for Enterprise Agreement Submissions	Enhanced email validation has been implemented in the Enterprise Agreement submission workflow. The optional email field in the contact details page now includes validation to prevent the entry of restricted competitor domain email addresses.
WS-3971	Global Settings Navigation Enhancement	The **Administration & Settings** left navigation now includes Global/VIQ/Account settings at the L1 level. This consolidates **Integrations** and **Backup & Restore** into global settings. This configuration area is accessible to Admin roles only.
XCP-3729	Software Upgrade Lifecycle Journey	The Software Upgrade Lifecycle Journey guides network administrators through firmware management. Users receive notifications about devices running old or non-compliant firmware, view firmware details categorized by cloud, controller, and SE, filter devices by site, building, floor, model, or NOS, and schedule upgrades with review and confirmation steps.
XCP-8432	Enterprise Agreements	Enterprise Agreements enable a self-service buying program through the existing cart flow. The system identifies accounts under an Enterprise Agreement, displays supported SKUs by product family, prevents duplicate purchases of the same family through the traditional cart, and integrates with IT and LIC services for subscription fulfillment.

Table 1: New Features in release 25.11.0-280 (continued)

Feature ID	Feature	Description
XCP-9754	Inventory Manager Support for TPME-managed Devices	The **Inventory Manager** now supports configuration backup and firmware upgrade for TPME-managed devices. Supported device families include ERS Series (3500, 3600, 4500, 4800, 4900, 5500, 5600, 5900), VSP 9000, 210 and 220 series, EXOS devices (firmware 16.2+), VOSS devices (firmware 8.6+), VDX, SLX, MLX, ICX, and EOS (A, B, C, K, S/SSA, 7100 series).
XCP-12052	Configuration and Firmware Repository Support	Provides configuration and firmware repository options for devices managed by the TPME. Supported protocols include TFTP, SCP, and FTP, each configurable with IPv4/IPv6 addresses, port, credentials, and directory. Multiple TPMEs can share the same repository.
XCP-17767	On-Demand Configuration Backup for TPME-Managed Devices	Enables on-demand configuration backup for TPME-managed devices from Extreme Platform ONE Networking. Users can select single or multiple devices and trigger an immediate backup. The system uploads configuration files to the designated repository (FTP, SCP, or TFTP) and retains them for 365 days by default.
XCP-18187	Support for Duplicate Serial Numbers Across Different Virtual IQ Accounts	TPME supports duplicate serial numbers across different Virtual IQ (VIQ) accounts within the same region. Devices in separate VIQs can share a serial number while maintaining independent device monitoring and statistics. Serial numbers remain unique within a single VIQ and within the same redirector for natively cloud-onboarded devices.
XCP-18235	Manual Controller Onboard Support	Users can manually onboard controllers (ExtremeCloud IQ-Controller) to the cloud. The onboarding flow requires the serial number (Lock ID) and MAC address as mandatory entries, with optional location selection. Network Policy does not apply to controller onboarding. Added controllers appear on the Appliances tab. Go to **Monitor** > **Network Devices** > **Appliances** or **Subscription & Services** > **Inventory** > **Appliances**. Controllers are not included in **Device Health**, **Usage**, or **Capacity** tabs.
XCP-18774	WIPS Alert Details	WIPS alert details now include sensor MAC address, expert description, and subcategory information. All alerts support Acknowledge and Clear actions. Rogue AP alerts display BSSID, SSID(s), RSSI, and channel information.

Table 1: New Features in release 25.11.0-280 (continued)

Feature ID	Feature	Description
XCP-21944	New WIPS Tab	A new **WIPS** tab is added to **Alert Policies**. All WIPS alert rules appear under this tab with **Type** set to Event. Users can enable or disable rules, configure trigger settings (default: Immediate), and set severity defaults. A filter by Enabled/Disabled status is available. Site-based policies do not support WIPS alerts at this time.
XCP-23347	Improved Enterprise Agreement Request History Tracking	Improved the Enterprise Agreement request history tracking to ensure accurate record-keeping. The system now correctly handles failed submission requests, preventing duplicate or incomplete entries from being created in the request history when submissions fail validation.
XIQ-37043	Controller-Managed APs Appear on Heat Maps	Controller-managed APs now appear on heat maps. APs are matched to Extreme Platform ONE locations at the floor level and can be positioned on floorplans. All heatmap types are supported for 2.4 GHz, 5 GHz, and 6 GHz frequencies. This feature provides monitoring only; device configuration is not included.
XIQ-47152	New Device Status Icon Filter Support	New Device Status icon filter support added in 25.11 for the following icons: • Anchor AP • Locally Managed – ExtremeCloud IQ • Locally Managed – Not ExtremeCloud IQ • Device Update Unsuccessful • Provisioned Device Configuration • Roll Back Undetermined • Configured At Device Level • Switch Stack • Switch Stack Warning • Radsec Proxy Server • Sensor Mode Interface Active • Sensor Mode Interface Inactive • Spectrum Intelligence • Fabric Attach • Fabric Attach Issue • Managed By Extreme IoT • Configuration Pending • Connected Device • Disconnected Device • Configuration Audit Match • Configuration Audit Mismatch • Simulated Device

Table 1: New Features in release 25.11.0-280 (continued)

Feature ID	Feature	Description
XIQ-47937	Fabric Engine/ VOSS 9.4.0 Support	Supports Fabric Engine/VOSS 9.4.0 for onboarding, monitoring, configuration, and image download for all supported SKUs, including 5000 and 7000 series Universal Switches, VSP7400, and VSP4900. Updates the downloadable image list to include 9.4.0 as the latest GA image, with 9.3.2 (N-1), 9.2.3 (N-2), and 8.10.9 for XA1400 only.
XIQ-48207	Deletion of Cloud-Onboarded Controllers	Users can delete cloud-onboarded controllers from the **Monitoring** > **Network Devices** > **Appliances** tab. Both single-select and multi-select delete actions are supported.
XIQ-48209	D360 Detail View Available for Onboarded Controllers	A D360 (Device 360) detail view is available for onboarded controllers. The view displays controller information including operating mode, license state, firmware version, and health status. The summary section shows the controller type (physical appliance or UCP) with a clickable UCP hostname linking to D360. Client hostnames and MAC addresses link to the C360 page. The **Configure** action opens the native controller interface via SSO. The only supported action is **Delete**.
XIQ-48524	Service Management Tab	A new **Service Management** tab under **Global Settings** allows users to enable WIPS (Wireless Intrusion Prevention System) and Guest Services. WIPS service has a dependency on Network Policy, communicated through a pop-up notification. Users can enable but cannot disable services in this release; the toggle shows **Enabled** but is Inactive if a user attempts to disable.
XIQ-48939	Manage and Unmanage Devices Managed by XIQ-SE from the Inventory View	Users can manage and unmanage devices managed by XIQ-SE from the **Inventory** view. This action applies to both the XIQ-SE appliance (parent) and its child devices. Managing a child device requires the parent XIQ-SE to be connected. Stack devices follow virtual stack representation and cannot be changed individually. Actions are available from **Subscription & ServicesInventoryAppliances**.

Addressed Issues

Table 2 lists Addressed Issues in Extreme Platform ONE Networking release 25.11.0-280.

Table 2: Addressed Issues in release 25.11.0-280

Issue ID	Description
CFDs	
CFD-17081	Addressed the issue where the AP Search field in the Real Time Troubleshooting feature did not populate or accept input after a location was selected.
CFD-17225	Addressed the issue where the VLAN Probe utility was missing from the **Network Devices** 3-dot menu. The option was previously accessible through **Utilities** > **Initiate VLAN Probe**.
CFD-17230	Addressed multiple issues with IP Firewall rule configuration in Extreme Platform ONE Networking and ExtremeCloud IQ (Classic): • IP address range was not selectable when creating a firewall rule from within a network policy. • IP ranges configured through Common Objects and attached to a User Profile were not retained in the configuration pushed to the access point. • Port ranges defined in Network Services were not saved and were missing after editing the object.
CFD-17231	Addressed the issue where navigating to **Network Policies** > **Common Objects** > **Network Objects** displayed an "An unknown error has occurred" error. Add and delete actions completed successfully, but the error appeared after every operation, and API calls were executed multiple times with intermittent errors.
CFD-17260	Addressed the issue where cloning a Network Policy in Extreme Platform ONE Networking returned the error "Cloning is not enabled for this Policy."
Alerts	
XCP-21726	Addressed the issue where alerts that were bulk-acknowledged reverted to an unacknowledged state after the page was refreshed.
API	
XCP-19243	Addressed the issue where the PerfMon API returns inconsistent and non-deterministic data schemas for legacy device types.
XCP-20428	Addressed the issue where null values are returned for client IP address fields (client_ip and ipv4) in the wired client API response, even when an IP address is assigned and visible in ExtremeCloud IQ.
XCP-20647	Addressed the issue where the listDevice API returns the field "is_locally_managed" in the response payload, which is not defined in the API output specification.

Table 2: Addressed Issues in release 25.11.0-280 (continued)

Issue ID	Description
XCP-20770	Addressed the issue where the asset summary/history API specification does not mark the request body as required in the OpenAPI specification.
XCP-20819	Addressed the issue where the ClientStats service sends the bwUsage field as an object containing avg, max, and min values instead of the required int64 format as defined in the specification.
XCP-21042	Addressed the issue where the bulk device import API (/v1/devices/onboard/import-xlsx) returned a 400 error when importing UCP devices with the `managed_by=Cloud` query parameter.
XCP-22931	Addressed the issue where the PerfMon `/metric-data API` accepted wired devices as input for the "wireless interface stats" metric group and returned only wireless client metrics instead of returning an appropriate error.
XCP-23118	Addressed the issue where the `pm/v1/analytics/usage-capacity` API returned N/A for all Usage Capacity data.
XIQ-48097	Addressed the issue where the Third-Party Management Engine (TPME) devices API accepts search queries with fewer than three characters and returns results instead of returning a 400 BAD_REQUEST response.
XIQ-48534	Addressed the issue where the OperationalChannelPowerMapEvent sent to AI-CORE contained null values for channel_numbers and tx_powers for all interfaces on the AP3000X.
XIQ-49961	Addressed the issue where the POST `/ng-reports/scheduled/custom` API returns a generic 400 BAD_REQUEST response without providing actionable validation details.
XIQ-49959	Addressed the issue where the CLI command `interface wifi0 radio profile radio_11be-2g` failed on the AP5060D running IQ Engine 10.8.7.
Device Management	
SEN-618	Addressed the issue where a DNS server configuration change on the TPME did not take effect immediately. The TPME continued using the previous DNS server until a reboot was performed.
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-18164	Addressed the issue where 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.

Table 2: Addressed Issues in release 25.11.0-280 (continued)

Issue ID	Description
XCP-20011	Addressed the issue where 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.
XCP-21131	Addressed the issue where the user-modified default Access Profile was not deployed to the Third-Party Management Engine in some situations.
XCP-21137	Addressed the issue where device-level schedule overrides did not take effect when a site-level schedule was configured.
XCP-21261	Addressed the issue where the Sites XML import functionality does not properly validate site hierarchy, allowing invalid XML files to be imported.
XCP-21609	Addressed the issue where TPME-managed devices did not return to the Connected state after an unmanage and re-manage operation.
XIQ-49371	Addressed the issue where the **Primary Controller** and **Backup Controller** fields for enhanced-discovery APs displayed the actual controller IP addresses instead of the values configured by the user during Enhanced Discovery setup.
XIQ-51114	Addressed an issue where the AFC agent used incorrect certification IDs for AP-5060U, AP-5060D, AP-5022, AP-5022FX, and AP-5022S6D access points.
Inventory	
XCP-18242	Adressed the issue where a location assigned to multiple devices simultaneously is correctly reflected in the **Network Devices** table but not in the Inventory page.
Licensing	
WS-4448	Addressed the issue where no email attachment was included in the confirmation email sent after submitting an Enterprise Agreement request.
XCP-23157	Addressed the issue where the **Enterprise Agreement** tab was displayed in the **Request History** page for VIQ accounts that did not have an Enterprise Agreement entitlement.
Logs	
XCP-16530	Addressed the issue where the Audit logs are generated out of sequence when exporting a device.
Onboarding	
XCP-22686	Addressed the issue where a device onboarded without a site location (default site) was not removed from the **Usage and Capacity** page after the device was deleted.

Table 2: Addressed Issues in release 25.11.0-280 (continued)

Issue ID	Description
XCP-22846	Addressed the issue where serial numbers containing special characters from third-party devices onboarded using ExtremeCloud IQ-SE or TPME were rejected by the cloud. The serial numbers are sanitized or an expanded set of characters is accepted.
XCP-23069	Addressed the issue where newly onboarded Switch Engine/EXOS and Fabric Engine/VOSS devices in the GovRamp environment failed to connect after onboarding, with the device status icon remaining red. Previously onboarded devices were not affected.
XIQ-49244	Addressed an issue where creating an auto provisioning policy for AP5060 devices would enable the IoT radio by default, causing a "missing IoT profile" error. The IoT radio now remains disabled during auto provisioning policy creation, consistent with the existing behavior when creating templates.
Roles	
XCP-18269	Addressed the issue where the **Start Discovery** and **Add Device** actions were denied with a 403 Forbidden error for users with Bizops and Netsecops roles in Inventory, despite those roles having write access.
XCP-20938	Addressed the issue where BizOps users can successfully add a VOSS/Fabric Engine device on the **Network Devices** page but cannot see the added device on that page.
XCP-21028	Addressed the issue where creating both internal and external BizOps users is not possible when the RDC is running release 25.9.0 and the region is on release 25.10.0.
XCP-21282	Addressed the issue where SSO users with the Guest Management role cannot successfully create PPSK users and receive an `Access Denied` error when attempting to create accounts in user groups.
XCP-21527	Addressed the issue where an external user with the ExtremeCloud IQ Installer role is mapped to the Observer role in Extreme Platform ONE Networking instead of retaining the Installer role privileges.
Upgrading	
XCP-23196	Addressed the issue where the **Firmware Upgrade** option was not available when navigating from **Device Inspector** > **D360** > **Action** > **Firmware Upgrade**.
User Interface	
SEN-646	Addressed the issue where the device count in the TPME CLI did not match the count shown in the Extreme Platform ONE Networking **Inventory** page after device discovery.
WS-3923	Addressed the issue where the breadcrumb on the **Network Profile** page displays **Network Configuration / Network Policies** instead of only **Network Policies**, causing an inconsistency with the left navigation.

Table 2: Addressed Issues in release 25.11.0-280 (continued)

Issue ID	Description
WS-4399	Addressed the issue where clicking an alert from the Bell icon or the **Notification Center** page did not navigate to the specific alert when a persistent filter was already applied on the **Alerts** page. The application navigated to the filtered Alerts list, hiding the selected alert.
XCP-16957	Addressed the issue where the **Firmware Upgrade History** page displays a maximum of two filtered columns.
XCP-18722	Addressed the issue where the error message is not formatted properly when a duplicate Access Profile is created.
XCP-18901	Addressed the issue where sorting tables based on location results in incorrect results and error messages.
XCP-18944	Addressed the issue when TPME devices are discovered using SNMP, the Manage Tags feature on the **Visualization** page displays an "UNKNOWN" tag alongside the expected "snmpDiscovered" tag.
XCP-19039	Addressed the issue where the **Device 360** page does not open if the same S/N is managed in the same RDC, but a different VIQ. Configuration assignment does not show the device in the selection if the same S/N is managed in the same RDC but a different VIQ.
XCP-19300, XCP-19301	Addressed the issue where "Uptime" and "Connected For" data is not available for devices managed by the Third-Party Management Engine in Network Devices.
XCP-20852	Addressed the issue where the Global Sites filter does not return sites in alphabetical order.
XCP-21275	Addressed the inconsistency where the Extreme Platform ONE Networking user interface restricted site group hierarchy to two levels, while the ExtremeCloud IQ API and ExtremeCloud IQ (Classic) both supported three levels.
XCP-21344	Addressed the issue where clicking **View** on an **SNMP Timers** table entry did not display the table details.
XCP-22334	Addressed the issue where the CLI Credentials configuration panel for a TPME did not display the saved username in the **Username** field.
XCP-22666	Addressed the issue where pagination controls were non-functional in the **Sites** module when a site group containing 1,000 or more sites was expanded.
XCP-22743	Addressed an issue in the **Client Health** user interface where the **Unassigned IP** tile in the **IP Connectivity Issues** widget on the **Monitoring** > **Clients** page was not displaying the unassigned IP count. The **Unassigned IP** tile now displays N/A instead of a count, because unassigned IP addresses are no longer classified as a connectivity issue. The tile remains visible in the widget to maintain consistency with the total client count shown in the page header.

Table 2: Addressed Issues in release 25.11.0-280 (continued)

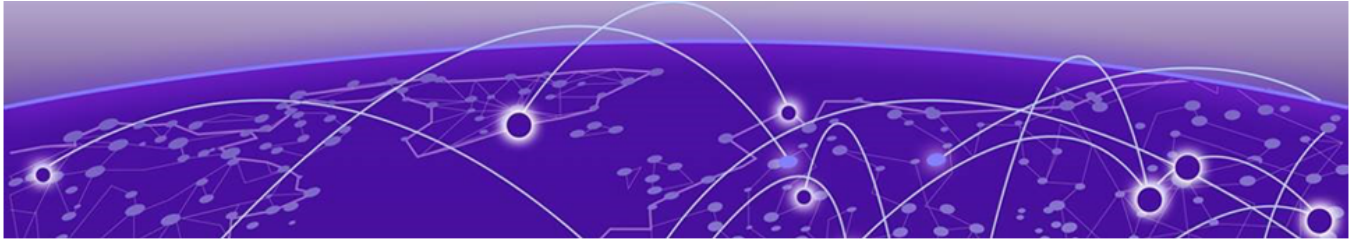
Issue ID	Description
XCP-22744	Addressed the issue where clients with an unassigned IP address displayed a red dot in the IPv4 column on the **Monitoring** > **Clients** page. Unassigned IP is not considered a client issue and now displays a green dot.
XCP-22755	Addressed the issue where the Memory filter on the **Device Health** page did not include a stack device when only one slot in the stack had a memory issue exceeding the threshold.
XCP-22772	Addressed the issue where a device with 90% CPU usage did not display a red dot indicator in the **CPU Usage%** column on the **Device Health** page, even though the device was counted under **CPU Usage Issues**.
XCP-22872	Addressed the issue where the **Traffic Anomaly** widget displayed -1 for the **Healthy Clients** count when no healthy clients were present. The count now correctly displays as 0.
XCP-22874	Addressed the issue where the **Client Health** widget displayed an incorrect total client count. MAC-learned clients and disconnected clients were not included in the total.
XCP-22876	Addressed the issue where a broadcast traffic percentage of 75% was not classified as a **Traffic Anomaly** in the **Client Health** widget. Broadcast utilization at or above 75% is defined as an anomaly.
XCP-22879	Addressed the issue where **Device Health** and **Usage & Capacity** grid rows for stack devices were misaligned with the grid columns.
XCP-22977	Addressed the issue where wired clients present in the LLDP and FDB tables were not appearing on the **Monitoring** > **Clients** page.
XCP-23002	Addressed the issue where the **Usage and Capacity** page displayed N/A for traffic statistics of stack member slots with no active ports, instead of displaying 0.
XCP-23085	Addressed the issue where the site-level filter on the **Client Health** page continued to display clients from a device's previous site location after the device was moved to a new site.
XCP-23097	Addressed the issue where the SQL query for retrieving wireless client statistics does not time out when no stats are found for a given device serial number.
XCP-23105	Addressed the issue where the **Client Health** widget allowed both the **Anomalies Clients** and **Healthy Clients** filters to be applied simultaneously. Applying both mutually exclusive filters produced inconsistent or empty data. Only one filter can now be active at a time.
XCP-23113	Addressed the issue where the **Device Health** grid was not filtered correctly when multiple issue filters were applied. Devices without the selected issue type appeared in the filtered results.

Table 2: Addressed Issues in release 25.11.0-280 (continued)

Issue ID	Description
XCP-23435	Addressed the issue where cross-tenant data leakage occured on the **Wired Usage & Capacity** page. When multiple accounts were concurrently active on the same environment, the API may return data belonging to another tenant, including an incorrect ownerID. The issue also affected the **Client** page grid and **Device Health** grid.
XCP-23450	Addressed the issue where a single stack device generated duplicate row entries on the Usage and Capacity page.
XCP-23598	Addressed the issue where the congestion packet count stopped updating in the **Client Health** page when the value exceeded 2.1 billion.
XIQ-48217	Addressed the issue where the export option was unavailable in the **Other Devices** tab on the **Network Devices** page for Third-Party Management Engine-managed devices in the user interface.
XIQ-49737	Addressed the issue where the **Update Enhanced Discovery** option was missing for locally managed access points.
XIQ-49951	Addressed the issue where the **Clients** > **Applications** view showed no data for **Application** and **Category** fields and displayed an excessive number of decimal places in the Data Usage column for onboarded controllers.
Visualize	
NVO-14730	Addressed the issue where the model for a device managed by the Third-Party Management Engine is Unknown in the Object Inspector.
NVO-14880	Addressed the issue where 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-15117	Addressed the issue where **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	Addressed the issue where some devices that were managed by the Third-Party Management Engine had Partially Connected status in Visualization due to LLDP data discovery issues.
NVO-15304	Addressed the issue where pushing an ISPP port change from Extreme Platform ONE Networking caused an unintended AAA RADIUS server reconfiguration on EXOS/Switch Engine 33.5 and later.

Table 2: Addressed Issues in release 25.11.0-280 (continued)

Issue ID	Description
NVO-15492	Addressed the issue when a new LACP Link Aggregation Group (LAG) is created between two Switch Engine/EXOS devices, the websocket connection does not automatically detect and display the new LAG on the network visualization canvas. The LAG configuration is correctly established on both devices with LLDP neighbors present, but the canvas continues to show the individual ports as down connections rather than displaying the aggregated link bundle.
NVO-15501	Addressed the issue when a port was removed from an EXOS LACP Link Aggregation Group (LAG), the websocket connection did not detect the configuration change and the Inspector panel continued to display the original port count. After performing an **Update Topology** operation, the LAG status changed to *degraded* but the **Inspector** panel still incorrectly showed all original ports rather than reflecting the reduced port membership.
NVO-15606	Addressed the issue where the link between an Switch Engine/EXOS switch and its TPME-discovered neighbor was not visible in the **Network Visualization** page, despite the LLDP neighbor data being present in the API response.
NVO-15689	Addressed the issue where the **Network Visualization** page does not automatically update to reflect the deletion of a Link Aggregation Group (LAG) between Switch Engine/EXOS devices.
NVO-15757	Addressed the issue where links between two Aruba switches onboarded through TPME were not displayed in the **Network Visualization** page.
NVO-15908	Addressed the issue where the **Network Visualization** link details panel closed unexpectedly when a WebSocket Link Up or Link Down event was received.
NVO-17017	Addressed the issue where configuration collection was incomplete during a template push on a 4220 stack device.
NVO-17340	Addressed the issue where managed access points disappeared from the **Physical Layer** view when LLDP Neighbors was disabled in the settings.



Known Issues

Table 3 lists the Known Issues in Extreme Platform ONE Networking release 25.11.0-280 (Patch 3).

Table 3: Known Issues in release 25.11.0-280 (Patch 3)

Issue ID	Description
API	
SEN-555	The state/system API returns a negative sysUpTime value for third-party devices with a system uptime exceeding approximately 248 days. This occurs due to a 32-bit integer overflow in the sysUpTime field. The Third-Party Management Engine (TPME) currently caps the reported sysUpTime at the maximum int32 value (2,147,483,647) to prevent negative values from being reported.
Device Management	
XCP-5227	Incorrect `Managed_by value` for locally managed devices.
XCP-18640	The **Retry** action is disabled after the configuration deployment fails 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-21263	When attempting to upgrade devices and filtering to show only locally managed devices, the device type field displays as empty and no devices are returned. This occurs even when locally managed devices exist and are onboarded in the system.
XCP-23115	MAC client status does not transition to Disconnected after the MAC entry is deleted from the FDB table, even after multiple polling intervals.
XCP-23121	Client entries are not removed from the client table when a device transitions to an unmanaged state.
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.

Table 3: Known Issues in release 25.11.0-280 (Patch 3) (continued)

Issue ID	Description
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 supported SKUs.
Inventory	
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-19029	In **Configuration | Third-Party Management**, the Third-Party Management Engine is listed as assigned to the site even if the site was already deleted.
Licensing	
XCP-20454	When more Third-Party Management Engine devices are discovered than available licenses allow, the devices initially activate the available licenses but then transition to an unmanaged state. The activated licenses remain consumed in the backend even though the devices are in an unmanaged state.
Logs	
XIQ-47371	Multiple logs are generated for both single and bulk device deletions.
Onboarding	
WS-3579	A toast notification splits into two separate messages when a user performs a navigation action while a toast is active, such as during onboarding or device deletion operations.
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.

Table 3: Known Issues in release 25.11.0-280 (Patch 3) (continued)

Issue ID	Description
XCP-20938	BizOps users can successfully add a VOSS/Fabric Engine device on the **Network Devices** page but cannot see the added device on that page. The device only appears on the **Inventory** page.
XCP-21032	BizOps users are unable to view Third-Party Management Engine (TPME) device details in the Device 360 (D360) page. When attempting to access the D360 page for TPME-managed devices, the page opens but displays no device data.
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.
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 XIQ, you are redirected to Extreme Platform ONE Networking but remain on the original SSO account.
Troubleshooting	
XIQ-48210	Downloading the AFC Geolocation report produced a corrupt file that was not in the expected CSV format, making it unusable for troubleshooting.
Upgrading	
XCP-12063, XCP-12064, XCP-16651	An audit log is not generated for a scheduled a firmware upgrade, when a firmware upgrade successfully completes, or when a firmware upgrade fails.
XCP-13051	While a firmware upgrade is in progress for a device in Extreme Platform ONE Networking it is deleted in ExtremeCloud IQ.
XCP-14211	The **Firmware Version** dropdown is not visible during a firmware upgrade when multiple APs are selected and the last device in the list is reviewed on high-resolution displays.
XCP-17804	After upgrading to 25R7, the schema registry service encounters 409 errors for the hm-device-stats-value and xiq-client-events-value topics. The affected schemas must be deleted before the registry service calls can succeed.
User Interface	

Table 3: Known Issues in release 25.11.0-280 (Patch 3) (continued)

Issue ID	Description
NVO-15001	Port Description in Link & Port details for devices managed by Third-Party Management Engine contain incorrect values.
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-17326	Tables in the user interface refresh slowly when the pagination is set for 500.
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 Third-Party Management Engine configuration deployment fails. The deployment API response confirms a failed status but does not include a failure reason, and no corresponding audit log entry is generated.
XCP-20134	The filter chip for the Extreme Platform ONE Networking selection in the Application Access column filter in **Access Management** is not displayed, preventing confirmation that the filter has been applied.
XCP-21438	When the Extreme Platform ONE Networking idle session timeout is reached while navigating SD-WAN through the 9-dot menu, SD-WAN 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-22984	Client connection status changes are reflected in the data grid in near real-time. After a client disconnects, there may be a delay of up to 2.5 minutes before the status update is reflected on the **Client Health** page due to cache refresh timing. Further optimizations to reduce this window are planned for a future release.
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.

Table 3: Known Issues in release 25.11.0-280 (Patch 3) (continued)

Issue ID	Description
XCP-23307	Filter options and **Edit**/**Delete** actions are not available for Subscription & Licensing request history.
XCP-23381	Users can navigate to the request creation flow from the **Submitted Request Summary** page by clicking sections in the progress bar. The progress bar sections should not be clickable from the **Summary** page.
XCP-23406	The **Total Queue Congestion Packets** column under **Usage & Capacity** > **Wired** displays an incorrect value for Stack devices. The user interface consumes an internal API that excludes congestion drops from certain Stack member ports in the BACKUP_IN_SYNC state, resulting in a lower packet count than the correct aggregated value returned by the Swagger endpoint.
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-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-48218	Selecting **Configure** from **Network Devices** displays **Third Party Management** instead of **Configuration Profile**.
XIQ-50544	Client 360 view for a NAC client displays a VLAN ID of -1 in the user interface.
XIQ-50598	A discrepancy exists in Tx/Rx Bytes values between the **Port Stats** window in ExtremeCloud IQ (Classic) and the Extreme Platform ONE Networking **Client 360** view for the same device and time interval.
Visualize	
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-15025	LLDP devices discovered through the Third-Party Management Engine do not support tagging.

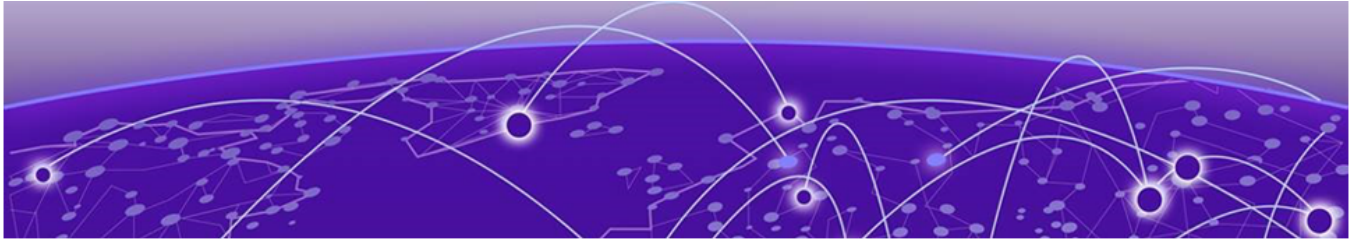
Table 3: Known Issues in release 25.11.0-280 (Patch 3) (continued)

Issue ID	Description
NVO-15660	A Link Aggregation Group (LAG) configured between an EXOS/ Switch Engine switch and an Access Point intermittently loses its LAG visualization on the network canvas and displays as a single link instead. The LAG configuration is correctly shown on both the EXOS/ Switch Engine device and the AP, but the visualization canvas fails to consistently represent the aggregated link bundle.
NVO-15783	Devices disappear from the Fabric canvas when dynamic changes occur. The issue does not occur consistently and does not affect the Physical View.
NVO-17598	The **Configure Fabric** > **Auto Sense** page displays "0" for all I-SID CVID fields that have no value, instead of displaying the expected descriptive placeholder text.

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 32
Access Points (Universal Hardware) on page 33
Switches (Universal Hardware) on page 35
ExtremeCloud IQ Site Engine on page 37

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)	5.14.01	Supported hardware models: 1130C 2130C 3150C 3160C 4120C

Access Points (Universal Hardware)

Table 5: Required Firmware Versions for Universal Hardware Access Points

Device Model	Latest Supported Release	Recommended Minimum Release
AP302W	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP305C	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP305C-1	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP305CX	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP3000	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP3000X	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP4000	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP4000-1	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP4020	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP410C	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP410C-1	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP460C	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP460S6C	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP460S12C	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP5010	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP5020	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP5022/FX/S6D	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP5050U/D	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2

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

Device Model	Latest Supported Release	Recommended Minimum Release
AP5060U/D	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2
AP510C/CX	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.2

Switches (Universal Hardware)

Table 6: Required Firmware Versions for Switches

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

Table 6: Required Firmware Versions for Switches (continued)

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

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.

ExtremeCloud IQ Site Engine

Version	Supported Features
25.5.11	• 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 subscriptions
25.5.12	• 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 subscriptions
25.8.10	• 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 subscriptions

Version	Supported Features
25.8.11	• 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 subscriptions
25.8.12	• 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 subscriptions
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 subscriptions

Version	Supported Features
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 subscriptions
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 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 subscriptions

Version	Supported Features
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 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 subscriptions
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 subscriptions

Version	Supported Features
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 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 subscriptions