Extreme Platform ONE Networking v25.12.0-301 Release Notes

New Features, Limitations, and Known Issues

9041172-00 Rev AB
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/

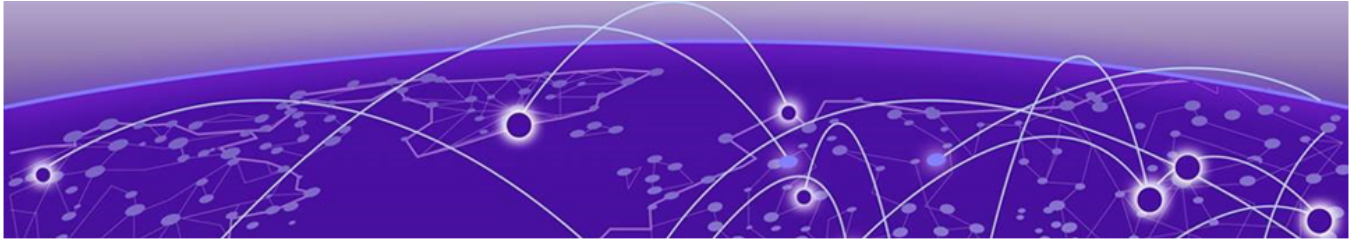


Table of Contents

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

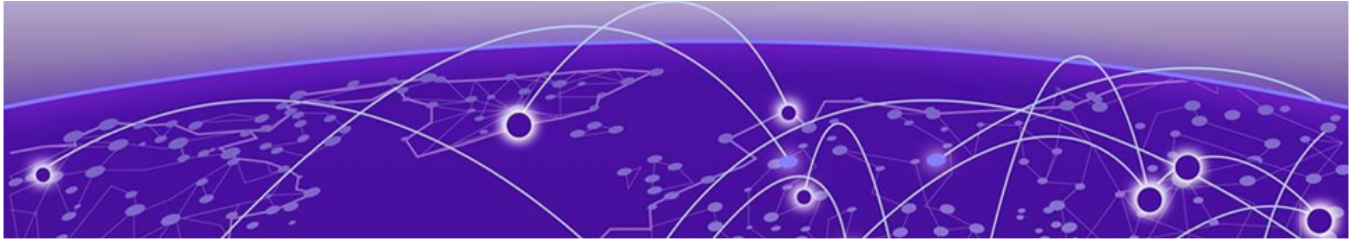
General Release Information **7**
Current Release: 25.12.0-301 7
Introduction to Extreme Platform ONE Networking 7
Extreme Platform ONE Public IP Address Blocks 8
Supported Applications 9
Browser Support and Display Settings 9
Desktop Browsers 9
Display Settings 10

New Features **11**

Addressed Issues **14**

Known Issues **21**
Limitations 28

Device Support Information **29**
Universal Compute Platform 29
Access Points (Universal Hardware) 30
Switches (Universal Hardware) 32
ExtremeCloud IQ Site Engine 34



Abstract

This release notes document for Extreme Platform ONE Networking version 25.12.0-301 (August 2026) provides technical information for network administrators, operators, and IT professionals managing cloud-managed, wired, wireless, fabric, and third-party network infrastructure. It describes new platform capabilities including Visualization-based SSH sessions for Third-Party Management Engine (TPME) devices, support for duplicate serial numbers across VIQs, improved TPME default deployment settings, UZTNA subscription licensing with 1:1 SUI/SPUI consumption, expanded Device 360 Resource Manager validation, and onboarding, monitoring, configuration, and firmware management support for Fabric Engine/VOSS 9.4.1 and 9.3.3 platforms. The release notes provide guidance on supported applications, browser requirements, public cloud connectivity, firmware compatibility, device onboarding, licensing, monitoring, configuration workflows, and supported hardware and Site Engine releases. Significant addressed issues span authentication, SSO, API behavior, onboarding, licensing synchronization, 802.1X authentication, firmware upgrades, client monitoring, visualization, and user interface performance. Known issues and limitations identify TPME deployment constraints, RBAC and SSO session handling concerns, backup and restore exceptions, topology visualization restrictions, audit logging gaps, interoperability caveats, and firmware prerequisites, while documenting workarounds, troubleshooting considerations, deployment constraints, and supported infrastructure components.

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

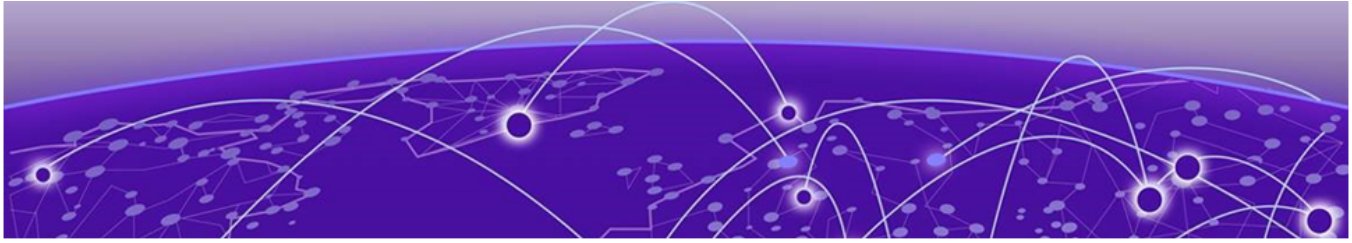
Subscribe to Product Announcements

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 9

Current Release: 25.12.0-301

August 2026

This release includes new platform capabilities including Visualization-based SSH sessions for Third-Party Management Engine (TPME) devices, support for duplicate serial numbers across VIQs, improved TPME default deployment settings, UZTNA subscription licensing with 1:1 SUI/SPUI consumption, expanded Device 360 Resource Manager validation, and onboarding, monitoring, configuration, and firmware management support for Fabric Engine/VOSS 9.4.1 and 9.3.3 platforms.

Related Links

- Known Issues on page 21
- Device Support Information on page 29

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.

ExtremeCloud IQ and 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:

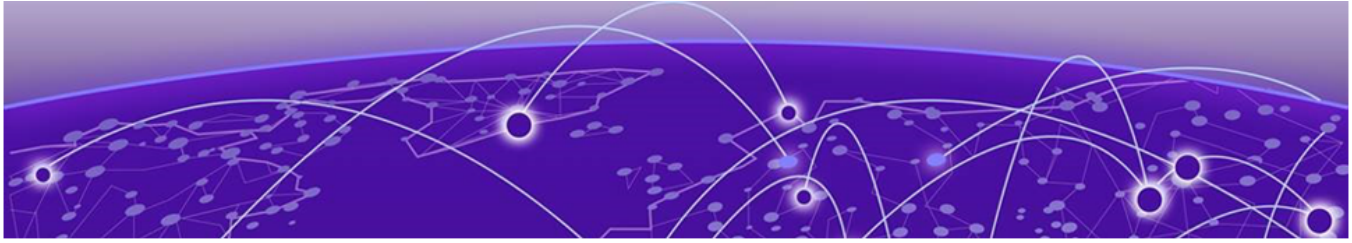
- Chrome
- Edge
- Firefox

- Opera
- Safari

Microsoft Internet Explorer is not supported.

Display Settings

Extreme Platform ONE supports display resolutions of 1280 x 1024 or higher.



New Features

Table 1 on page 12 lists the new features introduced in Extreme Platform ONE Networking release 25.12.0-301.

For more information about Extreme Platform ONE Networking features, see the Extreme Platform ONE Networking v25.12.0 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 25.12.0-301

Feature ID	Feature	Description
NVO-10573	**Visualization** supports for SSH sessions for Third-Party Management Engine managed devices.	The **Visualization** page now supports SSH sessions for Third-Party Management Engine (TPME)-managed third-party devices. Users can right-click a TPME-managed device in the **Visualization** page and select **SSH Session** to open a new browser tab with an active CLI session, providing an experience consistent with Switch Engine/EXOS and Fabric Engine/VOSS devices.
NVO-14877	Third-Party Management Engine support for duplicate serial numbers within the same RDC	The TPME now supports duplicate serial numbers within the same RDC, enabling TPME-managed devices with identical serial numbers to be managed across multiple VIQs simultaneously.
SEN-549	Third-Party Management Engine Improved Default Configuration	The TPME appliance now deploys with an improved default configuration. ZTP is disabled, NTP is enabled with pre-configured time servers, SSH daemon keys are generated uniquely for each new VM deployment, and the hostname is assigned a unique value derived from the device serial number using the format TPME-XXXXX.
XCP-20581	Data Download Support Added for Wired Pages	Data export (download) functionality, previously available only on wireless device pages, is supported across wired device pages. Users can download data from **Network Devices** > **Device Health** > **Wired**, **Network Devices** > **Usage and Capacity** > **Wired**, and **Clients** > **Wired**.
XCP-21303	UZTNA Subscription Licensing with 1-to-1 SUI/ SPUI License Consumption	Extreme Platform ONE Networking introduces UZTNA (Unified Zero Trust Network Access) subscription licensing with 1-to-1 SUI/SPUI license consumption. The new UZTNA SKU grants access to Extreme Platform ONE Networking and supports MSP-configurable maximum capacity.
XCP-22934	Fabric Engine/ VOSS 9.4.1 Support	Extreme Platform ONE Networking adds onboard, monitor, configure, and firmware image download support for Fabric Engine/VOSS 9.4.1 on supported Extreme switch models.
XCP-22935	Fabric Engine/ VOSS 9.3.3 Support	Extreme Platform ONE Networking adds onboard, monitor, configure, and firmware image download support for Fabric Engine/VOSS 9.3.3 on supported Extreme switch models.

Table 1: New Features in release 25.12.0-301 (continued)

Feature ID	Feature	Description
XIQ-45377	Option to Erase Configuration on Device Deletion	When deleting a device, administrators have the option to also erase the device's configuration. The erase option is presented during the delete workflow and is disabled by default. Both the delete and erase actions are audited. This applies to wireless and wired devices. **Note:** Only initiation of the action can be confirmed. Success or failure of the erase action is not reported back to the user interface.
XIQ-46596	Persistent Column Order Preferences	Column selections and column order are remembered across sessions. Previously, any custom column arrangement was reset to default upon logout. Column preferences are persisted globally across all pages with column views and retained until they are explicitly changed.
XIQ-49728	Configuration Audit Icon Now Active	The Audit icon active and clickable for IQ Engine (IQE)-based devices. Clicking the icon displays the delta configuration CLI commands, the complete configuration CLI commands, and a summary of configuration changes. A "Clear Audit Mismatch" action (previously called "Ignore") is also available to dismiss audit discrepancies.
XIQ-49796	Improved Device Onboarding Flow	The device onboarding user interface has been redesigned to reduce user confusion during initial setup. The **Managed By** label is prominently displayed. The **Cloud** and **Controller** buttons have been visually de-emphasized to guide users to read the label first. Contextual help text has been added beneath each option to clarify its purpose, and the serial number field for controller onboarding displays updated guidance.
XIQ-50781	Fabric Engine/ VOSS 9.4.1, 9.3.3, 8.10.9 Support	Support is added for for onboard, monitor and image download with Fabric Engine/VOSS 9.4.1, 9.3.3, 8.10.9. Supported switch models are: 7830, 7720, 7520, 5720, 5520, 5420, 5320 and applicable Universal Hardware 4220 switches, VSP7400, and VSP4900. Version 8.10.9 is only supported on XA1400.

Addressed Issues

Table 2 lists Addressed Issues in Extreme Platform ONE Networking release 25.12.0-301.

Table 2: Addressed Issues in release 25.12.0-301

Issue ID	Description
CFDs	
CFD-16081 03225487, 03289794	Addressed the issue where the ExtremeCloud IQ PIL subscription count intermittently dropped during scheduled licensing checks, causing ExtremeCloud IQ Site Engine to receive spurious license violation alerts multiple times per week; the correct total subscription count was restored within approximately one minute.
CFD-17209	Addressed the issue where the Resource Center icon overlapped with scrollbars and action buttons (Import/Bulk) on Guest Management screens by relocating it in the header.
CFD-17266 (03274724)	Addressed the issue where onboarding a CE2000 Universal Appliance using a Locking-ID with a specific serial number format failed with a schema validation error; the serial number pattern has been updated to recognize this format.
CFD-17340 (03279781)	Addressed an issue where applying UZTNA SSID configuration to AP305C and AP410C access points running IQEngine versions earlier than 10.8.7 could remove required legacy RADIUS-over-TLS proxy settings, causing 802.1X authentication failures.
CFD-17378 (03281164)	Addressed an issue where the Japanese translation of user interface labels in the **Network Devices** > **Add Device** workflow were incorrect. The labels for manual onboarding mode and the add device dialog have been corrected.
CFD-17467 (03279457)	Addressed an issue where EXOS switches with the same IP address configured for both the primary and secondary SNTP servers failed device initial collection. The table index has been updated to correctly distinguish between primary and secondary servers sharing the same IP address, allowing collection and configuration pushes to complete successfully.

Table 2: Addressed Issues in release 25.12.0-301 (continued)

Issue ID	Description
CFD-17476 (03283666)	Addressed an issue where Switch Engine/EXOS switches that are managed through out-of-band management port experienced a netlogin outage when an incorrect VLAN name (`VLAN_ <ID>` instead of the actual `VLAN name`) was pushed in the AAA/RADIUS configuration after enabling the Instant Secure profile for Extreme Platform ONE Security integration. This caused the RADIUS server to be marked inactive, breaking 802.1X authentication.
CFD-17494 (03283138, 03285074)	Addressed the issue where uploading a logo image to a Captive Web Portal (CWP) profile in Extreme Platform ONE Networking failed while the same image uploaded successfully in ExtremeCloud IQ. The image upload endpoint in Extreme Platform ONE Networking has been corrected to accept standard image file types.
CFD-17552 (03282369)	Addressed the issue where two specific support contracts failed to load their details when selected in the **Contracts** section of Extreme Platform ONE Networking, while all other contracts displayed correctly regardless of the user role or account.
CFD-17557 (03285565)	Addressed the issue where in Extreme Platform ONE Networking, the **Backup & Restore** > **Default Device Password** page did not display a **Save** button after toggling on the **Enable** device management settings for Switch Engine/EXOS and Fabric Engine/VOSS switches option, preventing the setting from being applied.
CFD-17564 (03287829)	Addressed an issue where AP5020 access points experienced 802.1X authentication failures and SSID outages after upgrading to IQ Engine 10.8.7.0 due to a misconfigured UZTNA transport mode. The fix includes a per-SSID transport selector, letting admins choose between Direct Tunnel (10.8.7.0+) and Legacy Proxy (older firmware), with automatic exclusion of non-qualifying APs.
CFD-17668 (03290175)	Addressed an issue in Extreme Platform ONE Networking where the **About** > **Firewall Configuration Guide** link incorrectly redirected all users to the US East region documentation regardless of their actual region. Users are now redirected to the appropriate regional Firewall Configuration Guide.
Account Management	
XCP-24406	Addressed the issue when after switching accounts using the Account Switcher, the **Access Management** page continued to display data from the previously selected account until the page was manually refreshed.
API	

Table 2: Addressed Issues in release 25.12.0-301 (continued)

Issue ID	Description
SEN-555	Addressed the issue where 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.
XCP-22931	Addressed the issue where wired devices could be queried through the wireless interface stats metricGroup in PerfMon, returning wireless client data for wired devices.
XCP-23010	Addressed the issue where the Asset ListDevice API rejected empty request body payloads. The API now accepts empty object payloads.
XCP-24530	Addressed the issue where the x.filter.connection_states URL parameter was not applied correctly when used alone or with multiple building_ids; the filter now resolves correctly in all combinations.
XCP-24569	Addressed the issue where the Media Upload API returned an error when the mobile app attempted to upload a video file because the file extension was appended twice by the service.
Device Management	
SEN-676	Addressed the issue where the backup of some third-party device configurations did not include VLAN data stored in the vlan.dat file. Only the running configuration file was backed up, causing VLAN configurations to persist after a restore and reboot instead of reverting to the backed-up state.
SEN-706	Addressed the issue where deploying a configuration repository to a TPME device failed when the SCP repository was configured without a password. The TPME API rejected the deployment request with an invalid Password: cannot be empty error.
SEN-728	Addressed the issue where the ShowSupport output file did not display firmware repository deployment details after a successful configuration profile deployment to a TPME device. The Access Profile, repository, and SNMP timer fields appeared empty in the `ShowSupport.txt` file.
XCP-18944	Addressed an issue where when using the TPME, an unexpected Tag "Unknown" was sometimes assigned.
XCP-25033	Addressed an issue where wired clients with unassigned IP addresses were incorrectly counted as connectivity issues in the Dashboard Client widget and the Usage & Capacity Clients column.
XCP-20454	Addressed an issue where TPME-discovered devices were incorrectly marked as "UnManaged, Not Licensed" when the number of discovered devices exceeded available licenses.

Table 2: Addressed Issues in release 25.12.0-301 (continued)

Issue ID	Description
XIQ-49999	Addressed the issue where changing the operating system of an AP5022 from cloud managed to Campus mode resulted in a Device Update Unsuccessful error in Extreme Platform ONE Networking.
XIQ-50707	Addressed the issue where a multi-select **Update Device** operation failed when the selection included one connected, managed device and one disconnected device in the **New** state. The entire update failed instead of processing the eligible connected device and skipping the disconnected device.
XIQ-51064	Addressed the issue where deleting an AP from the Extreme Platform ONE Networking user interface triggered a factory reset of the device. APs with a static IP became unreachable after deletion, while APs with a dynamic IP had their hostname, password, and configuration reset.
Licensing	
WS-4585	Addressed the issue where the **Request** button on the **Licenses and Subscriptions** page was hidden after a user aborted the Enterprise Agreement request process from the **Contract** page and navigated back to the **Subscriptions** page. The abort action also incorrectly reloaded the request popup.
XCP-24443	An `Access Denied` error popup appeared when navigating to the **Subscriptions and Licensing** page a second or subsequent time in the same session.
Roles	
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. The device only appears on the **Inventory** page.
SSO	
XCP-23560	Addressed the issue where inconsistent IAM gateway versions across deployment regions caused authentication failures. All IAM gateway instances have been updated to a consistent version.
Troubleshooting	
WS-4221	Addressed GOVRAMP compliance issues that have been identified across all Extreme Platform ONE common service. All common services now meet GOVRAMP standards and function correctly after the applied fixes.
Upgrading	
XCP-21263	Addressed the issue where the firmware upgrade workflow displayed an empty **Device Type** dropdown when all selected devices were locally managed.
XCP-22271	Addressed the issue where the firmware upgrade workflow did not display all available device types when switching between locally managed and cloud managed options.

Table 2: Addressed Issues in release 25.12.0-301 (continued)

Issue ID	Description
User Interface	
SEN-743	Addressed the issue where the Port Description in Link & Port details for devices managed by Third-Party Management Engine contained an incorrect value.
WS-4599	Addressed the issue where the **IDP** tab on the **Access Management** page was hidden after navigating from the **Access Management** page to the **Contract** page and then returning to the **Access Management** page.
XCP-17326	Addressed the issue where the table user interface responded slowly and rendered data slowly when pagination was set to 500 with more than 1,000 devices.
XCP-18182	Addressed the issue where the column filter in the **Assigned Devices** and **Feature Assignment** tables showed only (Select All) with no unique values, and the **Search** field did not return results.
XCP-19391	Addressed the issue where TPME editors showed inconsistent device counts when a TPME device transitioned to a disconnected state.
XCP-19442	Addressed the issue where the MAC address displayed in the Extreme Platform ONE Networking user interface for some third-party switches did not match the base MAC address reported by the device CLI and SNMP.
XCP-21785	Addressed the issue where the TPME user interface displayed an error after devices were discovered from a second VIQ, resulting in duplicate device ID entries in the feature assignment response.
XCP-22581	Addressed the issue where the **Name** column in the **Configuration and Firmware Repository** page did not sort data when the column header was clicked.
XCP-22739	Addressed the issue where the **Delete Configuration and Firmware Repository** dialog displayed invalid filter options when the selected repository was assigned to a device.
XCP-22885	Addressed the issue where the **TFTP** and **SCP Username** fields in the **Configuration and Firmware Repository** form shared the same error state, causing error messages to appear and clear simultaneously across both fields.
XCP-22984	Addressed the issue where there were real-time synchronization issues on the **Client Health** page involving delays and discrepancies in client connection and disconnection status updates.
XCP-23115	Addressed the issue where the wired client connection status in the **Client Health** page was not updated to `Disconnected` after the client MAC entry was removed from the FDB table.
XCP-23124	Addressed the issue where the IPv6 address search in the wired client table did not return results.

Table 2: Addressed Issues in release 25.12.0-301 (continued)

Issue ID	Description
XCP-23291	Addressed the issue where the column order configured by the user in the **Request History** page (EA and Request tabs) was not preserved after navigating away and returning.
XCP-23381	Addressed the issue users could navigate to the request creation flow from the **Submitted Request Summary** page by clicking sections in the progress bar. The progress bar sections are not clickable from the **Summary** page.
XCP-23908	Addressed the issue where creating External Notification recipients (Email, Webhook, ServiceNow) failed with a 503 Service Unavailable error.
XCP-24171	Addressed the issue where bulk operations (firmware upgrade, delete, manage, unmanage) in the **Inventory** and **Network Devices** pages failed with a URL length error when multiple devices were selected.
XCP-24184	Addressed the issue where the **Internal Users** and **External Users** tabs in **Access Management** became unresponsive when performing row selection or editing actions.
XCP-24341	Addressed the issue where the **D360 Appliance** page displayed a `No static resource error` tooltip for the discovery status section of a connected TPME device.
XIQ-50302	Addressed the issue where the **Export** function on the **Client Health** page failed with a `Something went wrong` error when column sorting was applied.
XIQ-50572	Addressed the issue where the **Model** and **OS** filter options on the **Network Devices** > **Appliances** page incorrectly displayed WiNG when the listed appliances included CONTROLLER and VE6120 device types.
XIQ-50889	Addressed the issue where the device name displayed inconsistently in the **Network Devices** page depending on whether a controller was onboarded with or without a location. Controllers onboarded with a location displayed a name in the format `off-Flo-xxx` instead of the hostname.
XIQ-50893	Addressed the issue where Device 360 in Extreme Platform ONE Networking displayed action options that were not supported for locally managed APs. Triggering these unsupported actions, such as **Reboot**, returned a `Device Update Unsuccessful` error without performing any operation on the device.
XIQ-51500	Addressed the issue where the **Clients** > **Users/Applications** page failed to load when the page size was set to 500. The API rejected the request because the limit value exceeded the maximum allowed value of 100.
XIQ-51504	Addressed the issue where the **Show Startup Config** option in the **Diagnostics** window under **Network Devices** returned a blank output panel with no data displayed, even after the action was triggered successfully.
Visualize	

Table 2: Addressed Issues in release 25.12.0-301 (continued)

Issue ID	Description
NVO-14854	Addressed the issue where a TPME-managed switch, discovered as an LLDP neighbor by a cloud-managed AP, created duplicate nodes for the same switch in the **Visualization** page.
NVO-17224	Addressed the issue where initiating a firmware upgrade from the 3-dot menu in the **Network Devices** page did not display stack devices in the upgrade window, returning zero results. Firmware upgrades initiated from the **Device 360 Monitoring** page were not affected.
NVO-17225	Addressed the issue where the **Update Device** action for stack devices, triggered from the three-dot menu in the Network Devices page or from the Device 360 Monitoring page, failed with a 500 server error. This failure also prevented the Revert to Default Template action from completing.

Known Issues

Table 3 lists the Known Issues in Extreme Platform ONE Networking release 25.12.0-301.

Table 3: Known Issues in release 25.12.0-301

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 of the current implementation 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.
Device Management	
XCP-5227	Incorrect `Managed_by value` for locally managed devices.
XCP-17157	Addressed the issue where Extreme Platform ONE Networking does not support setting or updating the TPME hostname using the **Configure** option. This has been documented as a platform 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 Network Gateway Controller configuration data. Configuration Profiles and Access Profiles remain intact after the reset, leaving the VIQ in an inconsistent state.
XCP-21438	The SD-WAN application displays an Auto-Logout popup when the Extreme Platform ONE Networking idle session timeout is reached because SD-WAN reads its own 30-minute default timeout instead of the Extreme Platform ONE Networking session configuration.

Table 3: Known Issues in release 25.12.0-301 (continued)

Issue ID	Description
XCP-22265	Export and import of VIQ, backup and restore of VIQ does not work properly if the Third-Party Management Engine (TPME) or ExtremeCloud IQ Site Engine is present.
XCP-22882	When Access Profiles are assigned to TPME-managed devices, the deployment status does not change to "Draft" as expected. Other assignment actions, such as SNMP timer and CLI credentials, correctly trigger the deployment status update to "Draft".
XCP-23121	Client entries are not removed from the Client table when a device transitions to an unmanaged state.
XCP-23557	The **Access Management External Users** page fails to load and returns a validation error when the page size is set to 500.
XCP-24308	When two TPME devices are onboarded with identical hostnames, device-level configuration deployment may be initiated on the wrong TPME. This occurs because the deployment API uses hostname to identify the target device — if hostnames are not unique, the deploy request can be routed to an unintended device, resulting in unpredictable deployment behavior. **Workaround:** Ensure all TPME devices are configured with unique hostnames prior to onboarding.
XCP-24442	When a device is onboarded as a TPME-managed device in one VIQ and the same device is subsequently onboarded as a cloud-managed (SwitchEngine/EXOS) device in a different VIQ, deletion of the TPME-managed device fails.
XCP-24446	In the **Device 360** view for a TPME device, the **Start Discovery** and **Add Device** action dialogs fail to reopen after being dismissed with the **Cancel** button. Once cancelled, subsequent attempts to launch either action from the **Actions** dropdown have no effect, preventing discovery initiation or device addition without navigating away.
XCP-24603	When launching the **Device 360** view for a TPME-managed device, the connection status is incorrectly displayed as "Partially Connected". Disregard the "Partially Connected" status displayed for TPME devices.
XCP-24780	Export and import of VIQ, as well as backup and restore of VIQ, does not work properly when TPME or ExtremeCloud IQ Site Engine is present in the environment. Specifically, import fails to populate data in inferred devices and asset devices in the platform database after a VIQ export/backup/reset/import cycle.
XIQ-19320	WiFi 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.

Table 3: Known Issues in release 25.12.0-301 (continued)

Issue ID	Description
XIQ-21339	When aggregation is enabled with a rate-limit configuration in ExtremeCloud IQ, configuration fails without an error message displayed.
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-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 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	
XCP-25510	When navigating to **Administration & Settings** > **Logs** > **Audit Logs** and selecting the **Last Quarter** time filter while searching, for example, for "Created", the page may display a "Something went wrong" error. The issue is more likely to occur on accounts with a large number of audit log entries.
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	

Table 3: Known Issues in release 25.12.0-301 (continued)

Issue ID	Description
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-21032	BizOps users are unable to view Third-Party Management Engine (TPME) device details in the Device 360 page. When attempting to access the page for TPME-managed devices, the page opens but displays no device data.
XCP-24193	New RBAC user account activation links display an Invalid or Expired Link error because the user interface enforces a minimum password length of 8 characters while the backend requires a minimum of 12 characters.
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	
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-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.

Table 3: Known Issues in release 25.12.0-301 (continued)

Issue ID	Description
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 Third-Party Management Engine 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.
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 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-22188	The system uptime (`sysuptime`) value for TPME devices displays correctly in the **Device 360** view but shows an incorrect value in the **Network Devices** table (**Appliances** and **Discovered Devices** tabs).
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.

Table 3: Known Issues in release 25.12.0-301 (continued)

Issue ID	Description
XCP-23080	When both an LLDP entry and an FDB entry exist on the same switch port, only the LLDP MAC address is displayed as a wired client; the FDB MAC address should also be identified as a wired client.
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-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. 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.
XCP-23558	In the **Device 360** view, TPME-managed devices that have undergone partial or failed discovery are incorrectly displayed as "Connected" instead of "Partially Connected." The Visualization **Object Inspector** panel correctly displays "Partially Connected" as expected.
XCP-24557	The **Usage and Capacity** widget on the **Dashboard** does not include issue counts for stack devices. The widget shows 0 for sites where a stack device has congestion issues.
XCP-25928	After selecting sites for an Identity Provider (IDP) in the Attribute Mapping section, the site count displays zero instead of reflecting the number of sites selected. The selected sites are saved correctly upon saving. The count does not update in real time to show the correct number of sites chosen.
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.

Table 3: Known Issues in release 25.12.0-301 (continued)

Issue ID	Description
XIQ-48218	Selecting **Configure** from **Network Devices** displays **Third Party Management** instead of **Configuration Profile**.
XIQ-50544	There is a minor discrepancy in the Tx / Rx Bytes in the **Port Stats** window between ExtremeCloud IQ (Classic) and Extreme Platform ONE Networking Client 360.
XIQ-50598	The **Client 360** view for a NAC client displays a VLAN ID of -1 in the user interface.
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.
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-15025	LLDP devices discovered through the Third-Party Management Engine do not support tagging.
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 EXOS/Switch Engine 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 a device's IP address after the management IP address is manually changed. The updated IP address displays correctly in the **Network Devices** page and **Device 360**.
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.
NVO-17846	When enabling an Instant Secure profile for Extreme Platform One Security integration, the RADIUS netlogin configuration writes an incorrect VLAN name (VLAN_4095) to the switch instead of the correct management VLAN name. This causes the RADIUS server to be marked as inactive due to failed connectivity checks, resulting in a netlogin outage.

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 29
Access Points (Universal Hardware) on page 30
Switches (Universal Hardware) on page 32
ExtremeCloud IQ Site Engine on page 34

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. Those 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 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 Sustaining Release	Recommended Minimum Release
AP302W	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP305C	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP305C-1	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP305CX	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP3000	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP3000X	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP4000	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP4000-1	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP4020/X/FX	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.4
AP4060	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.4
AP410C	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP410C-1	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP460C	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP460S6C	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP460S12C	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP5010	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP5020	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP5022/FX/S6D	IQ Engine 10.8.7 AP 10.19.01	N/A	N/A

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

Device Model	Latest Supported Release	Recommended Sustaining Release	Recommended Minimum Release
AP5050U/D	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP5060U/D	IQ Engine 10.8.7 AP 10.19.01	N/A	N/A
AP510C/CX	IQ Engine 10.8.7 AP 10.19.01	IQ Engine 10.8.5f (10.8.5.6)	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

ExtremeCloud IQ Site Engine Version	Supported Features
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
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

ExtremeCloud IQ Site Engine Version	Supported Features
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
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

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 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
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

ExtremeCloud IQ Site Engine Version	Supported Features
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
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