Extreme Platform ONE™ Networking v25.16.0-352 Release Notes

New Features, Limitations, and Known Issues

9041337-00 Rev AA
November 2026

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

Legal Notice

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

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

Trademarks

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

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

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

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/



Table of Contents

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

General Release Information **7**
Current Release: 25.16.0-352 7
Introduction to Extreme Platform ONE Networking 7
Extreme Platform ONE Public IP Address Blocks 7
Supported Applications 8
Browser Support and Display Settings 9
Desktop Browsers 9
Display Settings 9

New Features **10**

Addressed Issues **14**

Known Issues **20**
Limitations 27

Device Support Information **28**
Universal Compute Platform 28
Access Points (Universal Hardware) 29
Switches (Universal Hardware) 31
ExtremeCloud IQ Site Engine 33
Third-Party Management Engine 37



Abstract

This release notes document for Extreme Platform ONE™ Networking version 25.16.0-352 (November 2026) describes platform enhancements, supported hardware and software, addressed defects, known issues, limitations, and deployment requirements for cloud-managed enterprise networking environments. The release introduces support for Switch Engine/EXOS 32.7.4.15-patch1-14, 33.7.1-patch1-32, and 34.1 image management, Fabric Engine/VOSS 9.4.2 onboarding and lifecycle management, IQ Engine 10.9.2 Multi-Link Operation (MLO), enhanced radio mode combinations, ESL dongle support, and expanded Third-Party Management Engine (TPME) capabilities for Cambium, SecureStacks, ERS, and ISW devices. Intended for administrators, network operations teams, and support engineers, the release notes provide intermediate-to-advanced technical guidance for deployment, upgrades, troubleshooting, and enterprise-scale network management.

Help and Support

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

Extreme Agent ONE™ Coworker "Talk to Support"

For customers with Extreme Platform ONE™ ExtremeWorks / ExtremeWorks Premier subscriptions, technical support cases can be created using Extreme Agent ONE™ Coworker. This option requires that a user has an existing Extreme Networks Support Portal account login (using the same email address as used to log into Extreme Platform ONE™ Networking.) For more information about Extreme Agent ONE™ Coworker "Talk to Support", see the Extreme Agent ONE™ Coworker documentation.

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: 25.16.0-352

November 2026

Related Links

- Known Issues on page 20
- Device Support Information on page 28

Introduction to Extreme Platform ONE Networking

The following are a few key features:

- Comprehensive UI: Provides access to alerts, licensing details, inventory, and firmware updates.
- Alerts and Notifications: Find and fix problems quickly. Real-time notifications ensure you receive prompt notifications about system updates and security notices.
- Contextual AI Support: Meet your Extreme Agent ONE™ Coworker—your contextual helper. Powered by the latest in AI technology, Agent ONE Coworker provides instant support and guidance, ensuring you have the answers you need, when you need them.
- Single Sign-On (SSO): Access Extreme Platform ONE Networking applications with a single sign-on, removes the need for multiple credentials.

Extreme Platform ONE Public IP Address Blocks

Data Center	IP Block	Addresses and Ports
Global Data Center (GDC)	44.234.22.92/30 18.194.95.0/28 34.253.190.192/26 3.234.248.0/27	
Australia (AUS)	13.210.3.192/28 18.98.198.80/28	Firewall Address and Port Information
Azure, Canada Central (ACA)	20.151.64.48/28	Firewall Address and Port Information
Azure, US East (AVA)	52.226.89.112/28	Firewall Address and Port Information
Brazil (BR)	18.228.70.16/28	Firewall Address and Port Information

Data Center	IP Block	Addresses and Ports
Germany (FRA)	3.67.81.96/27 18.194.95.0/28	Firewall Address and Port Information
India (IN)	13.232.67.8/29 3.6.70.64/29	Firewall Address and Port Information
Ireland (IE)	34.253.190.192/26	Firewall Address and Port Information
Japan (JP)	18.176.203.112/29 13.231.6.232/29 57.181.58.0/28	Firewall Address and Port Information
Netherlands (NL-GCP)	34.91.82.64/27	Firewall Address and Port Information
Singapore (SG-GCP)	34.87.158.80/28	Firewall Address and Port Information
Spain (ES)	18.101.49.128/27	Firewall Address and Port Information
Sweden (SE)	13.48.186.224/29 13.48.4.184/29 13.48.4.240/28	Firewall Address and Port Information
Switzerland (ACH)	51.107.1.192/28	Firewall Address and Port Information
United Arab Emirates (UAE)	3.28.159.128/28	Firewall Address and Port Information
United Kingdom (UK-AGB)	51.143.233.80/28	Firewall Address and Port Information
US East (VA)	34.202.197.0/26 44.192.245.0/26 3.234.248.0/27	Firewall Address and Port Information
US East 2 (VA2)	34.202.197.0/26 44.192.245.0/26 3.234.248.0/27	Firewall Address and Port Information
US-Iowa (IA-GCP)	34.67.130.64/27	Firewall Address and Port Information
US Ohio (OH)	3.145.235.64/26	Firewall Address and Port Information

Supported Applications

Extreme Platform ONE Networking eliminates the need to log in separately to the Extreme Networks multi-domain network management solutions by unifying them within a single user interface.

For example, if you subscribe to ExtremeCloud IQ, and have a site, you can view all connected sites and onboarded devices from ExtremeCloud IQ and Extreme Platform ONE Networking.

Note
The applications available when you log in are specific to the subscription licenses purchased by your organization. Access to applications might also be defined by the role assigned if your organization implements Single Sign-On.

Extreme Platform ONE Networking supports the following applications:

- ExtremeCloud IQ: Provides centralized configuration and network monitoring, reporting, alarms, and statistics for Extreme Networks devices.
- ExtremeCloud SD-WAN: Provides unified wired and wireless management through fabric services. You can enable a secure network, automate application performance management, and create a centralized management of applications with intuitive user experiences.
- Universal ZTNA: Provides network, application, and device access security within a single solution.

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 11 lists the new features introduced in Extreme Platform ONE Networking release 25.16.0-352.

For more information about Extreme Platform ONE Networking features, see the Extreme Platform ONE Networking v25.16.0 User Guide.

Device OS Support

This release supports the following device operating systems.

- Switch Engine/EXOS**:**
  - IQAgent Version
    - Switch Engine/EXOS release < 31.7: upgrade to IQAgent version 0.9.32
    - Switch Engine/EXOS release >= 31.7 < 33.2 upgrade to IQAgent version 0.9.45
    - Switch Engine/EXOS Engine release >= 33.2 upgrade to IQAgent version 1.9.45
  - 33.7.1.6-patch1-32 Latest Supported GA Patch

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

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

    Onboard, Monitor, Config, Image Mgmt, and Global Download Support
  - 32.7.4.15-patch1-14 Previous Supported GA Patch

    Onboard, Monitor, Config, Image Mgmt, and Global Download Support
- Fabric Engine/VOSS**:**
  - IQ Agent Support
    - XA1400 series 0.7.4
    - All others 0.9.36
  - 9.4.2.0 Latest Supported GA Image

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

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

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

- IQ Engine **Support:**
  - IQ Engine release 10.9.3

New Hardware Support

Extreme Platform ONE now supports the following hardware:

- AP3020 and AP3020X access points
- AP3060 access point

Table 1: New Features in release 25.16.0-352

Feature ID	Feature	Description
XIQ-53505	Extreme Tunnel Concentrator Appliance UI	The ability to launch the Extreme Tunnel Concentrator Appliance UI directly from Extreme Platform ONE Networking, originally planned for release 25.16, has been deferred to release 25.17 to allow additional quality testing and validation.
XIQ-53504	ExtremeCloud IQ Site Engine Appliance UI Access	The ability to launch the ExtremeCloud IQ Site Engine user interface directly from Extreme Platform ONE Networking, originally planned for release 25.16, has been deferred to release 25.17 to allow additional quality testing and validation.
XIQ-53502	ExtremeCloud IQ Controller/ Universal Compute Platform Server/ Appliance UI Access	The ability to launch the ExtremeCloud IQ Controller/ Universal Compute Platform Appliance user interface directly from Extreme Platform ONE Networking, originally planned for release 25.16, has been deferred to release 25.17 to allow additional quality testing and validation.
XIQ-53245	Switch Engine/ EXOS 32.7.4.15-patch1-14 Support	Extreme Platform ONE Networking supports image download for Switch Engine/EXOS 32.7.4.15-patch1-14 GA on all supported single and stacked Switch Engine/ EXOS SKUs. Version 34.1.1 is the latest image in the global image download list. The 440-G2, 450-G2, and 460-G2 products remain on 33.7, and 34.x does not appear for these products.
XIQ-52999	Switch Engine/ EXOS 33.7.1-patch1-32 Support	Extreme Platform ONE Networking supports image download for Switch Engine/EXOS 33.7.1-patch1-32 GA on all supported single and stacked Switch Engine/ EXOS Engine SKUs. Version 34.1.1 is the latest image in the global image download list. The 440-G2, 450-G2, and 460-G2 products remain on 33.7, and 34.x does not appear for these products.
XIQ-52556	Radio Mode Combination Support	Extreme Platform ONE Networking supports the radio mode combinations of the AP3020, AP3020X, and AP3060 access points. Each access point has two software-programmable data radios. The radio mode selector displays only the modes that the selected platform supports, and the availability of 6 GHz modes depends on country and regulatory authorization.

Table 1: New Features in release 25.16.0-352 (continued)

Feature ID	Feature	Description
XIQ-52237	Informational Note Display for AP5020, AP5022, and AP5060 Access Points	A note was added to the 802.11be radio profile user interface indicating that The Radio Profile configuration under **Common Objects** > **Policy** > **Radio Profiles** allows the Maximum Number of Clients field to be set from 1 to 512. However, the AP5020, AP5022, and AP5060 platforms support a maximum of 300 clients per radio. Values above 300 configured here will not be exceeded on these platforms.
XIQ-51699	IQ Engine 10.9.2 Multi-Link Operation (MLO) Support	IQ Engine 10.9.2 supports MLO radio mode combinations on the AP3020W access point. The AP3020W supports MLO with the 2.4 GHz + 5 GHz and 6 GHz + 5 GHz radio combinations. The availability of 6 GHz depends on the country.
XIQ-49696, XIQ-49697, XIQ-51696	Dongle Support	The AP3020 and AP3020X access points support the Solum dongle, Ugate dongle, and Hanshow dongle for ESL.
XIQ-47951	Switch Engine/ EXOS 34.1 Support	Extreme Platform ONE Networking supports image download for Switch Engine/EXOS 34.1 GA on all supported single and stacked Switch Engine/EXOS SKUs. Version 34.1.1 is the latest image in the global image download list. The 440-G2, 450-G2, and 460-G2 products remain on 33.7, and 34.x does not appear for these products.
XCP-27335	Fabric Engine/ VOSS 9.4.2 Support	Extreme Platform ONE Networking supports onboarding, monitoring, configuration, and image download for Fabric Engine/VOSS 9.4.2 on the 7830, 7720, 7520, 5720, 5520, 5420, and 5320 Universal switches, applicable 4220 Universal switches, and the VSP7400 and VSP4900.
XCP-23970	Activity Hub Provides Actions for Third-Party Management Engine (TPME) Tasks	New actions are available for TPME firmware upgrade tasks in the Activity Hub: Cancel, Retry, and Reschedule. • A scheduled firmware upgrade task can be canceled, and the task status changes to Canceled. • A firmware upgrade task can be retried on the device level, which creates a new task for the selected devices only. • A task in the Scheduled state can be rescheduled, which updates the scheduled time of the existing task. Deleting a device or its TPME owner changes the task status to Archived when no targets remain, or removes the deleted devices from the task scope when targets remain.
SEN-1036	Basic Device Recognition for Cambium Switches	Extreme Platform ONE Networking provides basic device recognition for Cambium switches. The device type (model), serial number, and firmware version are identified.

Table 1: New Features in release 25.16.0-352 (continued)

Feature ID	Feature	Description
SEN-872	SecureStacks Device Support	TPME provides SecureStacks device (EOS A-series, B-series, C-series, and D-series) support with statistics gathering, NOS API data collection, discovery, serial number resolution, LLDP information gathering, configuration backup and restore, and firmware upgrade.
SEN-751	ERS Series Device Configuration Archive	TPME provides Inventory Manager archives device configurations for ERS Series 3500, 3600, 4500, 4800, 4900, 5500, 5600, and 5900 devices with feature parity with ExtremeCloud IQ Site Engine. Secure transfer (SCP/SFTP) is the preferred method, and FTP or TFTP is the last resort.
SEN-711	ISW Family Device Support	TPME provides ISW family device support with serial number resolution, LLDP information gathering, statistics gathering, configuration backup and restore, and firmware upgrade. The support covers the ISW, ISW-4W, and ISW-24W device types.
WS-4757	Deprecated Connect Level VIQ Start Option	The option to start a new Connect level VIQ has been deprecated.

Addressed Issues

Table 2 lists Addressed Issues in Extreme Platform ONE Networking release 25.16.0-352.

Table 2: Addressed Issues in release 25.16.0-352

Issue ID	Description
CFDs	
CFD-15435	Addressed the issue where IQ Engine did not recognize devices that run iOS 26 as Apple iOS because of a new DHCP option 55 fingerprint. The devices appeared as unknown in the logs and in **Client 360**.
CFD-16417	Addressed the issue where user names were not displayed in the client connection history for SSIDs that use PPSK when the time range is longer than 1 day.
CFD-16763	Addressed the issue where the maximum caching time that was configured on an SSID was not applied. Clients received a PMK time left in cache of 3600 seconds instead of the expected 216000 seconds.
CFD-17447	Addressed the issue where an MLD-ID was not generated for an MLO SSID that was deleted and then added again to the configuration. As a result, the MLD information element was missing from beacon frames, and clients could not establish MLO connections.
CFD-17631, CFD-17632	Addressed the issue where incorrect French translations or Italian translations appeared in the user interface.
CFD-18112	Addressed the issue where Instant Port (IPP) profiles on switches reset to an unauthenticated state after a configuration push, even when no configuration changes exist. The connected devices did not reauthenticate.
CFD-18225	Addressed the issue where Third-Party Management Engine (TPME) devices displayed a cluster icon with the tooltip ExtremeCloud Appliance Cluster (Open) in the **Network Devices** > **All Devices** view.
CFD-18392	Addressed the issue where the widgets in **Manage** > **Summary** did not load data for a site that has a single AP460S6C running IQ Engine 10.8.5f.
CFD-18426	Addressed the issue where adding an SSO user to a Credential Distribution Group failed with an error message stating that the user is already a member of another Credential Distribution Group.

Table 2: Addressed Issues in release 25.16.0-352 (continued)

Issue ID	Description
CFD-18459	Addressed the issue where an Extreme Platform ONE Networking administrator was logged out after selecting the linked host name or MAC address in the Source field of the alert details window in **Monitoring** > **Alerts**.
CFD-18467	Addressed the issue where local users in Extreme Platform ONE Networking tenants that an MSP manages see only the MSP admin and MSP super admin roles for IdP group mapping.
CFD-18535	Addressed the issue where a sustained stream of failed PPSK authentications filled the NAS table of the AP and blocked all authentication.
CFD-18539	Addressed the issue where toggling a policy, such as Rogue AP, on or off in **Administration & Settings** > **Alert Policies** > **Global Policy** > **WIPS** did not generate an entry in the audit log.
CFD-18555	Addressed the issue where selecting **Clear** in the Date/Time picker of **Activity Hub** did not reset a custom date and time range.
CFD-18559	Addressed the issue where the 3-dot device action menu of a TPME-managed device on the **Discovered** tab differed between the **Network Devices** and **Inventory** views in action labels, action order, and available actions.
CFD-18576	Addressed the issue where **Device 360** displayed the previous daily backup schedule after the schedule of a TPME-managed device changed to weekly in **Activity Hub**.
CFD-18580	Addressed the issue where **Activity Hub** showed Created By: system instead of the administrator user name for a firmware upgrade that an administrator started manually from **Network Devices** > **Upgrade Firmware**.
CFD-18606	Addressed the issue where the **Per-Site** table on the dashboard listed the sites of the home account in addition to the sites of the external account after an administrator switched to an external admin account.
CFD-18634	Addressed the issue where some APs appeared offline in the JP-RDC after a release upgrade. Event logs showed the CAPWAP connection as disconnected while the APs remained connected and operational.
CFD-18715	Addressed the issue where the delta configuration for AP4000 devices continued to include the commands `no interface eth0 rate-limit multicast` and `no interface eth1 rate-limit multicast`, which caused delta updates to fail.
CFD-18857	Addressed the issue where the `GET /assets/v1/contracts/{contract_id}/lines` API call returned HTTP 400 with the error `Unknown LineStatus: RMA Requested` when a contract line had a status outside the five accepted values.
CFD-18899	Addressed the issue where the selected Cloud Managed or Controller Managed card in the **Manually Add Devices** and **Import** dialogs displayed a dark background with a dark heading and icon in the Light theme, which made the text nearly unreadable.

Table 2: Addressed Issues in release 25.16.0-352 (continued)

Issue ID	Description
API	
XCP-26635	Addressed the issue where `POST /v2/guests/{id}/block` returned 200 OK but did not block the guest. The guest status stayed ACTIVE, the device iwa not blocked, and no 24-hour automatic unblock timer started.
XCP-31080	Addressed the issue where POST and GET device API calls returned HTTP 200 with an empty response and no device data.
XCP-31728	Addressed an issue where the Audit Logs API returned inconsistent record counts or no results for extended date ranges.
XCP-31774	Addressed the issue where the Configuration API accepted the same address for `management-ip-address` and `management-default-gateway`.
XCP-31775	Addressed the issue where the Configuration API accepted a default gateway outside the subnet of the management IP address and accepted the network address or broadcast address as the management IP address or gateway.
Browser Issues	
XIQ-49898	Addressed an issue where opening local appliance web interfaces (ExtremeCloud IQ Controller, ExtremeCloud IQ Site Engine, and Tunnel Concentrator) from Extreme Platform ONE Networking failed with an HTTP 403 Forbidden error. Administrators (Admin and NetSecOps roles) can use the action menu in **Network Devices** and **Device 360** to access local appliance management graphical user interfaces directly.
Device Management	
XCP-18640	Addressed the issue where a retry did not occur after a configuration deployment to a TPME failed.
XCP-22461	Addressed the issue where a rule that combines location and model conditions was not applied to the device.
XCP-23577	Addressed the issue where a rule condition with the **Model** field and the Starts With operator does not take effect when the value includes a hyphen after the four-digit model number, such as 5320-. The rule takes effect when the value omits the hyphen.
XCP-26600	Addressed the issue where resolving a conflict failed for a three-node stack setup.
XCP-26762	Addressed the issue where a device that onboarded successfully through Extreme Platform ONE Networking and a rules engine rule was not assigned to the expected configuration profile.
XCP-27031	Addressed the issue where users could not create or edit rules in a configuration profile.
XCP-30800	Addressed the issue where deploying a configuration profile failed with a conflict on `/l2-service-feature` after a VLAN is deleted from a configuration profile that was already deployed.

Table 2: Addressed Issues in release 25.16.0-352 (continued)

Issue ID	Description
XIQ-52355	Addressed the issue where an AP switched from AIRRM to ACSP after a user changed the channel to static and then back to Auto on **Device 360**.
XIQ-53069	Addressed the issue where disabling the secure tunnel feature on an AP required a complete configuration push to take effect.
Roles	
XCP-27353	Addressed the issue where the list and export of guest records were not limited to the records that the user created when the user had the Guest Management role.
SSO	
XCP-19325	Addressed the issue where an SSO account displayed all sites after logging in when no sites were selected for the IdP.
Upgrading	
XCP-26380	Addressed the issue where the global and local firmware upgrade lists displayed devices that TPME manages.
User Interface	
XCP-19865	Addressed the issue where no failure details are displayed in the user interface when a TPME configuration deployment fails. The deployment API response confirms a failed status but does not include a failure reason, and no corresponding audit log entry is generated.
XCP-20971	Addressed the issue where the **Create** button on the **Configuration Profile** screen intermittently disappeared.
XCP-24223	Addressed the issue where a deleted device remained visible on the **Usage & Capacity** and **Device Health** pages, and the **Device 360** panel did not load when opened from **Usage & Capacity (Wireless)**.
XCP-26462	Addressed the issue where task names in **Activity Hub** did not update after the host name of a TPME-managed device changed, although the inventory displayed the new name.
XCP-26988	Addressed the issue where the **Firmware Status** widget in **Inventory** > **Switches** displayed No Updates Needed and did not show a PSIRT/CVE count for a device whose OS version had matching PSIRT data.
XCP-27801	Addressed the issue where the SSH Session option did not appear in the 3-dot menu of a standalone UCP device in **Network Devices** > **Appliance**.
XCP-27802	Addressed the issue where the 3-dot menu on the **Device 360** page of a UCP device did not load options.
XCP-28722	Addressed the issue where Run History in **Activity Hub** did not display an action icon to open the details.
XIQ-46203	Addressed the issue where the label of the Source field in **Monitoring** > **Clients** > **Users** displayed other instead of others.

Table 2: Addressed Issues in release 25.16.0-352 (continued)

Issue ID	Description
XIQ-50626	Addressed the issue where the **Status** column in **Network Devices** > **Device Status** > **All Devices** did not display the Undetermined status icon for devices that the Undetermined status filter selected. A disconnected icon appeared instead.
XIQ-51409	Addressed the issue where **Inventory** displays actions that locally managed APs do not support. Only the **Assign Location**, **Delete**, and **Enhanced Discovery** actions are expected for these APs.
XIQ-51837	Addressed the issue where the **Maximum Number of Clients** field of a radio profile in **Common Objects** > **Policy** > **Radio Profiles** was limited to 255 and returned the error must be less than or equal to 255 when **Supported Radio Modes** was set to a Wi-Fi 7 (be) variant. The valid range is 1 to 512.
XIQ-52219	Addressed the issue where Supplemental CLI (SCLI) commands remained in the **Delta Configuration Audit** view after a successful Complete Update.
Visualize	
NVO-18815	Addressed the issue where the Physical Ports table displayed ERR after a saved port mapping in a configuration profile was reopened.
NVO-19499	Addressed the issue where the user interface allowed saving a LAG configuration with a non-numeric MLT ID.
NVO-19630	Addressed the issue where the API for the L2 Ports report (`/platformmanager/v1/report/l2port`) was unavailable and the L2 Stats Details were missing in the user interface under System Setting.
NVO-19635	Addressed the issue where the Contains and Starts With operators for the **Model** field in onboarding rules did not accept a custom value.
NVO-19765	Addressed the issue where the Professional Install configuration option was missing from the **Edit Access Point** page under Wireless Configuration in the user interface.
NVO-19806	Addressed the issue where the initial deployment of a configuration profile with no custom configuration to a VOSS device failed with conflicts.
NVO-19925	Addressed the issue where the Batch reporting option was missing from the **Destination** dialog when an IoT profile in **Wireless Configuration** > **IOT Profiles** used the BLE Scan function.
NVO-19926	Addressed the issue where the Vendor filter option and the Real-time reporting and Batch reporting destination options were missing when an IoT profile in **Wireless Configuration** > **IOT Profiles** used the BLE Scan function and the Generic Scan application.
NVO-19938	Addressed the issue where the user interface under **Wireless Configuration** did not offer a separate Tunnel Concentrator profile option or page.

Table 2: Addressed Issues in release 25.16.0-352 (continued)

Issue ID	Description
NVO-20468	Addressed the issue where the **Operating Modes** option in the Device Profile of AP4020 and AP4060 in the user interface differed from the controller user interface and included an Operating modes + Sensor value.
NVO-20492	Addressed the issue where the Active APs, Non-active APs, and Clients columns were missing from the **Sites** page under Wireless in the user interface.

Known Issues

Table 3 lists the Known Issues in Extreme Platform ONE release 25.16.0-352.

Table 3: Known Issues in release 25.16.0-352

Issue ID	Description
CFD	
CFD-18080	In the current release, the **Clients** view displays only actively connected clients by default. As a result, clients are removed from the main **Clients** list shortly after they disconnect. Previously connected clients can still be viewed by applying the Disconnected filter. This behavior is a known limitation and is functioning as designed. A future release is planned to introduce enhanced historical client visibility and remove the current restriction that limits the default view to connected clients only.
API	
XCP-21292	The Overrides Conflicts Resolver does not display the updated Value on Device after the value changes on the device from A.00.00 to B.00.00.
XCP-22128	The vr-name property for l2-service-feature appears as a conflict in the Overrides Conflicts Resolver, although vr-name is not configurable for a VLAN in the user interface and has no default value in the schema.
XCP-23938	The release 25.12 database schema migration introduced NOT NULL columns without defaults to platform_common_db CDC tables, causing the Debezium AVRO connector to fail with a schema registry incompatibility error.
XCP-23971, XCP-24089	On the **Device360 Port Stats** and **Clients** pages, graphs and UI widgets (including the Port Stats graph, Port Description grid, Port Stats Summary, Link PoE, and Usage/Utilization widgets) pull data from the legacy monitoring APIs instead of from the PerfMonitor APIs.
XCP-26696, XCP-26702, XCP-26712	The `cs-metastore-event-ingestion`, `xcloudiq-license-scheduler`, CAS, and CNS applications are deployed with a single replica and without a configured health check.
XCP-28936	The cis-service in the GDC contains a duplicate gdc-kafka endpoint. The duplicate key cis.rdc.kafka.bootstrap.servers requires removal.
XCP-31523	The `override/create-modify` API returns HTTP 400 and applies no changes when a property in the request already holds its current value. The user interface displays `Failed to save device profile` when a user updates a static management IP address.

Table 3: Known Issues in release 25.16.0-352 (continued)

Issue ID	Description
XCP-31607	When saving the Device Profile feature in a configuration profile fails, the user interface displays the generic message Failed to save device profile. Please try again instead of the specific error message that the API returns.
XIQ-53218	The API specification for floor walls documents the wall type field as type_id, but the server accepts and returns only typeId. A request that uses type_id returns HTTP 400.
XIQ-53219	The published API specification shows snake case names for fields that the server uses in camelCase, such as connectionStatus for the POST `/dashboard/wireless/client-health/grid` call. Developers who follow the specification can send or read incorrect field names.
Device Management	
XCP-19055	The RESET VIQ operation does not remove configuration data. Configuration Profiles and Access Profiles remain intact after the reset, leaving the VIQ in an inconsistent state.
XCP-21438	The Extreme Platform ONE Security application displays an Auto-Logout popup when the Extreme Platform ONE Networking idle session timeout is reached because Extreme Platform ONE Security reads its own 30-minute default timeout instead of the Extreme Platform ONE Networking session configuration.
XCP-22265	Export and import of VIQ, backup and restore of VIQ does not work properly if the TPME or ExtremeCloud IQ Site Engine is present.
XCP-23121	Client entries are not removed from the Client table when a device transitions to an unmanaged state.
XCP-23565	In scaled environments with 24,000 wired clients, only approximately 18,345 clients are displayed in the **Client Health** page; all clients are visible in ExtremeCloud IQ (Classic).
XCP-30564	A second deployment of a configuration profile after a RADIUS server is modified displays IPv4 subnet conflicts for subnets that are not configured in the account. This affects Switch Engine and Fabric Engine devices.
XCP-31181	When the out-of-band (OOB) management interface is configured with a static IP address through a device-level override in a configuration profile, deployment fails, the device moves to the unmanaged state, and the default static route is not configured on the vr-mgmt virtual router.
XCP-31185	Deploying a configuration profile with a DNS server and a RADIUS server to a 5320 device that is managed through the in-band management interface fails with the error message resource not found.
XCP-31577	In a TPME configuration profile, the **Operating System** condition of a rule in **Profile Assignment** > **View Rules** > **Create Rule** does not offer the value OS ONE TPME.
XCP-31734	In the Device Profile at the device context, when **Include Site Location** is on and the **System/SNMP Location** box has a value, deployment leaves the location empty on the NOS. This affects Switch Engine and Fabric Engine devices, including stacks.

Table 3: Known Issues in release 25.16.0-352 (continued)

Issue ID	Description
XCP-31736	In the Device Profile at the device context, when **Include Site Location** is off and the **System/SNMP Location** box has a value, deployment applies the site value to the NOS instead of the configured System/SNMP Location. This affects Switch Engine and Fabric Engine devices.
XIQ-19320	Wi-Fi Interface Transmission power values may not update correctly on the **Managed Device** page after bulk edit operations.
XIQ-19368	User interface overrides Supplemental CLI option incorrectly pushes Supplemental CLI configuration instead of UI configuration for multicast rate limit settings.
XIQ-19498	Changing transmission type for eth0 interface on AP5010 incorrectly generates delta CLI for speed configuration.
XIQ-19509	Configuring eth0 interface with minimum speed and half duplex transmission type causes AP to go offline.
XIQ-33498	An issue exists where client mode and backhaul mesh link options need to be disabled on AP5050U/D 6GHz FCC configurations to ensure proper regulatory compliance.
XIQ-34724	An issue exists where delta configuration push fails for AP5020 Wifi0 with dual 5G mode when 5G-Low channels are not supported in some countries.
XIQ-36259	Importing an Ekahau planner file does not import all walls.
XIQ-46182	An issue exists where the EXOS and Switch Engine 31.7.4.2-patch1-7 cannot be onboarded, monitored, or configured through drag-and-drop image management for all EXOS and Switch Engine supported SKUs.
XIQ-51481	Firmware upgrade for AP4060 series access points is not available. The access points do not appear in the **Upgrade Firmware** selection, and the upgrade does not complete when initiated from the device 3-dot menu.
XIQ-52230	When Tunnel Concentrator Service is configured with APs, the AP configuration must be audited and pushed first, followed by the Tunnel Concentrator configuration push. Otherwise, the AP may not appear in the Tunnel Concentrator configuration, and the tunnel may not function.
XIQ-52706	Resetting a VIQ can result in unrecoverable data loss if the backup used for restoration is incomplete or the restore operation fails. The current Backup and Restore capability does not yet include all Extreme Platform ONE data. Verify that all required data has been exported before initiating a Reset VIQ operation.
Inventory	
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.

Table 3: Known Issues in release 25.16.0-352 (continued)

Issue ID	Description
Logs	
XIQ-47371	Multiple logs are generated for both single and bulk device deletions.
Onboarding	
WS-3579	Notifications are sometimes split into two messages during certain user actions such as onboarding or device deletion operations.
Roles	
CFD-16351, XCP-11511	An issue exists where Extreme Platform ONE Networking does not restrict admin visibility based on location, affecting only the Observer and the Operator roles.
XCP-10308	**Manage** or **Unmanage** actions are not performed for the NetSecOps role.
XCP-24515	Users with the Observer (Read Only) role can see and click the select-all check box in the **Alerts** page table header, which should be hidden for read-only users.
XIQ-45333, XIQ-45477	Manage/Unmanage actions are not working for Extreme Platform ONE Networking BizOps role users, showing the "something went wrong" error, and for NetSecOps role users with Write access to inventory, resulting in permission errors.
SSO	
XCP-8507	The login button does not activate for certain SSO-enabled user login instances.
XCP-22975	When logging out of an SSO account and logging back in with a different SSO user, the system may incorrectly display the previous user's account information. This occurs because session data from the prior login is not fully cleared on logout. **Workaround:** Fully close the browser (all tabs and windows) after logging out of the SSO account before logging in with the new user.
XIQ-49634	When switching to a different SSO account from ExtremeCloud IQ, you are redirected to Extreme Platform ONE Networking but remain on the original SSO account.
Troubleshooting	
XIQ-48210	Downloading the AFC Geolocation report produces a corrupt file that is not in the expected CSV format, making it unusable for troubleshooting.
Upgrading	
N/A	Starting in 25.14.0, firmware upgrades use the new V2 API (DLCS) and upgrade activity is tracked in **Activity Hub** rather than the **Firmware History** page. Existing entries from 25.13.0 and earlier remain visible in **Firmware History**, but any new upgrade initiated in 25.14.0 or later will appear only in **Activity Hub**. The **Reschedule**, **Cancel**, and **Retry** actions are no longer available in **Firmware History**. These actions are supported in **Activity Hub** .
XCP-12063, XCP-12064, XCP-16651	An audit log is not generated for a scheduled firmware upgrade. There is no log when a firmware upgrade successfully completes or when a firmware upgrade fails.

Table 3: Known Issues in release 25.16.0-352 (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	
WS-4616	When an existing user clicks the **Pendo Resource Center** icon in Extreme Platform ONE Networking, the **Product Tours** section does not appear.
WS-4782	The **Visualization** layer views appear cropped when viewed on a tablet device.
WS-4783	On mobile devices, the Agent ONE widget does not fit the screen size, and dragging the widget works inconsistently.
WS-4785	On mobile devices, data on the internal users page of Access Management does not load until you rotate the device to landscape orientation and back to portrait orientation. The page layout also breaks when you scroll horizontally.
WS-4793	On mobile devices in portrait orientation, the account switcher pop-up does not display accounts until you rotate the device to landscape orientation.
XCP-4999	Currently, when filtering on a switch stack, when a search matches any child device, the entire stack is displayed instead of individual devices.
XCP-5065	**Search** and **Filter** does not filter the appliance cluster.
XCP-18729	When viewing the **Device 360** page for a TPME-managed device, the Model field displays as "Unknown" instead of the actual device model. All other device details are unaffected.
XCP-19002	Fabric Attach links display as operationally down in the visualization even when they are operationally up. This issue affects Switch Engine downstream and SMLT Cluster upstream configurations that use Fabric Attach without authentication.
XCP-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 Universal ZTNA through the 9-dot menu, Universal ZTNA displays an "Auto-Logout in 1528 seconds" pop-up instead of following the Extreme Platform ONE Networking idle timeout behavior.
XCP-22682	Management port statistics are not displayed on the **Usage and Capacity** page for Switch Engine/EXOS devices that have all standard ports disabled.
XCP-22746	The **Total Client** count on the **Usage and Capacity** page returns 0 for wired devices, even when client entries exist for those devices.
XCP-23090	Device health issue reporting latency has increased. Temperature issues on Fabric Engine devices now take approximately 3 to 4 minutes to appear under **Device Health**, compared to approximately 1 minute in previous releases.

Table 3: Known Issues in release 25.16.0-352 (continued)

Issue ID	Description
XCP-23112	When a filter is applied on the **Device Health** page, other columns such as **CPU Usage%**, **Memory Usage%**, and **PSU Usage%** display N/A. This behavior applies to all **Device Health** issue filters.
XCP-23128	IPv4 and IPv6 null values (N/A) are not sorted correctly during ascending and descending sort operations on the client table. Null values appear at the end during ascending sort and not at the beginning during descending sort.
XCP-23139	Extreme Platform ONE Networking displays N/A for all metrics in the second row for a Switch Engine/EXOS switch in the **Device Health** and **Usage and Capacity** pages when multiple Switch Engine/EXOS switches are onboarded.
XCP-23406	The **Total Queue Congestion Packets** column under **Usage & Capacity** > **Wired** displays an incorrect value for Stack devices.
XCP-23436	The **Total Throughput (RxPktsPerSec / TxPktsPerSec)** column in the wired device grid on the **Usage & Capacity** page intermittently displays 0 or no value for devices that are actively transmitting traffic.
XCP-23450	A duplicate device row appears on the **Usage and Capacity** page.
XCP-24182	When no client issues are detected, the **Client Health** page displays '0 data found' instead of a 'No Issues' confirmation indicator.
XCP-24477	When navigating to the **Assets** page with an invalid `x.tab` parameter, the application defaults to the **All** tab correctly but does not remove the invalid parameter from the URL.
XCP-24524	The site ID is missing from the sites with issues grid response.
XCP-24537	The **Discovered** tab in the Assets/Inventory page uses 'unknown' as the URL parameter value instead of 'discovered', creating a mismatch between the user interface label and the URL parameter.
XCP-24714	The **Device Status** and **Device Health** widgets on the dashboard do not include the stack member device count.
XCP-24941	The **Device Health** page of the dashboard displays an incorrect total of managed devices after devices move to the offline state.
XCP-27843	Clarified CPU and memory utilization support in Performance Monitoring: CPU and memory statistics are supported on newer device platforms; legacy CAPWAP devices (such as AP4000 and AP410C) do not report these metrics to Performance Monitoring and may display a value of 0%.
XCP-30096	When a user launches an SSH session to a second device from the **Visualize** page, Extreme Platform ONE Networking logs the user out and redirects to the login page.
XCP-31146	A Fabric Engine device supports a maximum of 10 RADIUS servers, but the user interface allows mapping 32 RADIUS servers. Deployment reports success while only 10 servers are pushed to the device, and the user interface does not indicate that the remaining servers are dropped.
XCP-31620	The outdoor option for indoor APs is displayed, including AP5020, AP3000X, and AP3020W, and the outdoor setting is saved.

Table 3: Known Issues in release 25.16.0-352 (continued)

Issue ID	Description
XCP-32499	In Third-Party Management Configuration, the Access Profile, CLI Credentials, and Configuration and Firmware Repository cannot be edited using the 3-dot menu. **Workaround:** Select **View/Edit** in **Feature Assignment** before selecting the 3-dot menu and **Edit**. **Edit** will now open from the 3-dot menu.
XCP-32500	In Third-Party Management Configuration, the Access Profile, CLI Credentials, and Configuration and Firmware Repository cannot be deleted using the 3-dot menu. **Workaround:** Select **View/Edit** in **Feature Assignment** before selecting the 3-dot menu and **Delete**. **Delete** will now open from the 3-dot menu.
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-47622	The **Users** grid XAPI request times out when the Status=Connected filter is applied to a dataset of approximately 148,000 user records.
XIQ-47708	The summary widgets on the **Users** page fail to load when the page contains approximately 500,000 user records.
XIQ-49488	The **Client Density** heatmap displays an inaccurate client count that does not match the count shown on the client **Inventory** page.
XIQ-51014	On the **Device 360** page of a device that ExtremeCloud IQ Site Engine manages, the **Wired Usage** and **Capacity** values, such as Clients, Total Bandwidth, and total throughput Rx and Tx, display NA.
XIQ-51408	The **Inventory** page displays the **Upgrade Firmware** action for controllers, which is not a supported action for controllers.
XIQ-52081	When navigating to the **Clients** page from the **Client Health** widget on the Dashboard, switching between the Wired and Wireless tabs may cause continuous page flickering and rapid URL alternation. This issue occurs only when the **Clients** page is accessed through the Dashboard widget; accessing the **Clients** page directly is not affected. **Workaround:** Navigate to the **Clients** page directly from the menu rather than through the **Client Health** widget on the Dashboard, or refresh the page if flickering occurs.
XIQ-52087	The **Roaming Issues** filter on the **Clients** > **Wireless** widget returns clients with no roaming issues instead of clients that have roaming issues.
XIQ-53321	In the AP template and on the **Device 360** configuration page of AP4020 and AP3020 models, disabling Client mode allows selection of the **Sensor** checkbox for all interfaces, although the **Sensor** option is not supported.
Visualize	
NVO-15748	The **Visualization** page and **Device Inspector** panel do not update the device IP address after the management IP address is manually changed. The updated IP address displays correctly in the **Network Devices** page and **Device 360**.
NVO-19438	When multiple APs connect to the same switch, searching for an AP by IP address on the **Visualization** page opens the inspector panel of the parent switch instead of the inspector panel of the AP.

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 28
Access Points (Universal Hardware) on page 29
Switches (Universal Hardware) on page 31
ExtremeCloud IQ Site Engine on page 33
Third-Party Management 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.

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

Firmware compatibility is critical for feature functionality. New features may require specific firmware versions to operate as intended. The following tables list the minimum firmware versions required for the new features introduced in this release:

Universal Compute Platform

Table 4: Required Firmware Versions for Universal Compute Platform

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

Access Points (Universal Hardware)

Table 5: Required Firmware Versions for Universal Hardware Access Points

Device Model	Latest Supported Release	Recommended Sustaining Release	Recommended Minimum Release
AP302W	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP305C	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP305C-1	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP305CX	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP3000	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP3000X	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP3020/W/X	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.5
AP3060	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.5
AP4000	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP4000-1	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP4020/X/FX	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.4
AP4060	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.4
AP410C	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP410C-1	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP460C	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP460S6C	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP460S12C	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP5010	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2

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

Device Model	Latest Supported Release	Recommended Sustaining Release	Recommended Minimum Release
AP5020	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP5022/FX/S6D	IQ Engine 10.9.3 AP 10.20.1	N/A	N/A
AP5050U/D	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (10.8.5.6)	IQ Engine 10.8.2
AP5060U/D	IQ Engine 10.9.3 AP 10.20.1	N/A	N/A
AP510C/CX	IQ Engine 10.9.3 AP 10.20.1	IQ Engine 10.8.5g (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)	33.7.1.6	• 4120 • 4220 • 5120 • 5320 • 5420 • 5520 • 5720 • 7520 • 7720
EXOS	33.7.1.6	• 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	9.4.2.0	• 4220 • 5320 • 5420 • 5520 • 5720 • 7520 • 7720
VOSS	9.4.2.0	• VSP7432CQ • VSP7400-48Y • VSP4900-48P • VSP4900-24XE • VSP4900-24S • VSP4900-12MXU-12XE

ExtremeCloud IQ Site Engine

Table 7: Supported Features for ExtremeCloud IQ Site Engine Versions

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

Table 7: Supported Features for ExtremeCloud IQ Site Engine Versions (continued)

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

Table 7: Supported Features for ExtremeCloud IQ Site Engine Versions (continued)

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

Table 7: Supported Features for ExtremeCloud IQ Site Engine Versions (continued)

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

Table 7: Supported Features for ExtremeCloud IQ Site Engine Versions (continued)

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

Third-Party Management Engine

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

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

Table 8: Third-Party Management Engine feature support matrix

Company	Family	Configuration		Firmware Upgrade	Protocol	SSH Session WebSSH	LLDP Maps
		Backup	Restore				
Aruba	ArubaOS	Yes	Yes	Yes	SCP	Yes	No
Aruba/ HPE	AOS-CX	Yes	Yes	Yes	SCP	Yes	No
Cisco Systems	IOS-XE	Yes	Yes	Yes	SCP	Yes	Yes
Enterasys Networks	Secure-Stacks	Yes	Yes	Yes	TFTP	Yes	Yes
	S/K/71xx	Yes	Yes	No	SCP	Yes	Yes
Extreme Networks	ERS	Yes	Yes	Yes	TFTP	Yes	Yes
	ISW, ISW-4W and ISW-24W	Yes	Yes	Yes	TFTP	Yes	Yes
	Summit (EXOS version 16.2 or later)	Yes	Yes	Yes	SCP	Yes	Yes
	VSP (VOSS version 8.6 or later)	Yes	Yes	Yes	SCP	Yes	Yes