Extreme networks

Extreme Platform ONE™ Networking v25.14.0-331

Component update 25.14.1-3

Release Notes

New Features, Limitations, and Known Issues

9041245-02 Rev AA
October 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/

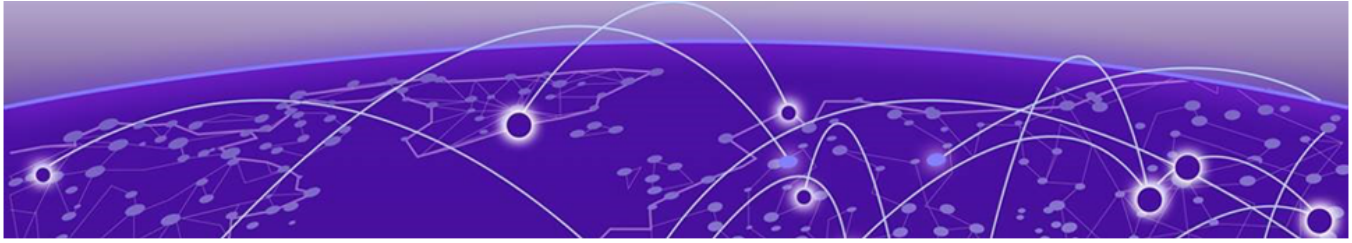


Table of Contents

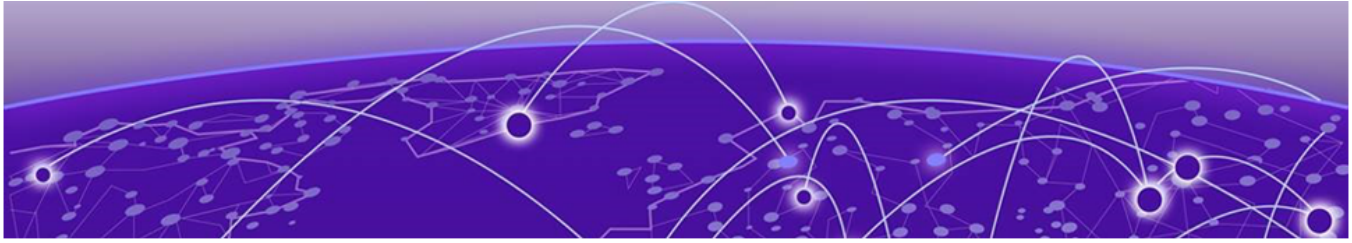
Abstract **4**
Help and Support v
Subscribe to Product Announcements v

General Release Information **7**
Current Release: 25.14.0-331 Component update 25.14.1-3 7
Release: 25.14.0-331 (Patch 1) 7
Release: 25.14.0-331 (Patch 1) Addressed Issues 7
Release: 25.14.0-331 7
Introduction to Extreme Platform ONE Networking 8
Extreme Platform ONE Public IP Address Blocks 8
Supported Applications 9
Browser Support and Display Settings 10
Desktop Browsers 10
Display Settings 10

Previous Release **11**
New Features 11
Addressed Issues 14

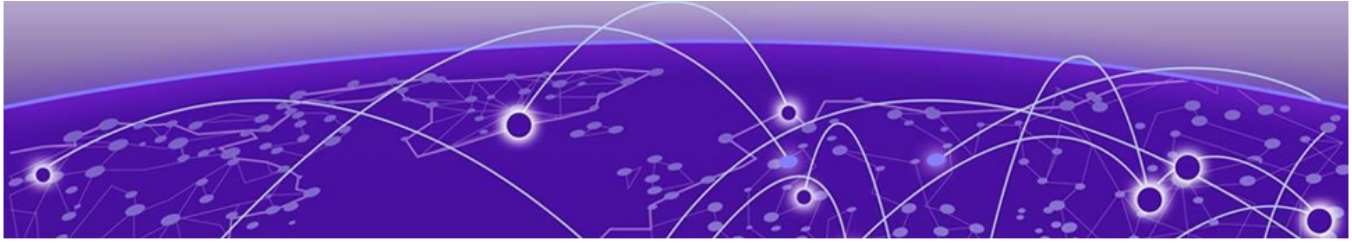
Known Issues **20**
Limitations 26

Device Support Information **27**
Universal Compute Platform 27
Access Points (Universal Hardware) 28
Switches (Universal Hardware) 30
ExtremeCloud IQ Site Engine 32



Abstract

This release notes document for Extreme Platform ONE™ Networking version 25.14.0-331 Component update 25.14.1-3 (October 2026) details new platform capabilities, software and hardware support requirements, resolved defects, known issues, and operational limitations for cloud-managed enterprise networking environments. This release resolved an issue causing sporadic latency and slow page-rendering when navigating the Dashboard, Devices, Clients, and Sites views. The release documents support for Switch Engine/EXOS, Fabric Engine/VOSS, IQ Engine 10.9.2, Universal Compute Platform, and ExtremeCloud IQ Site Engine integrations. It outlines onboarding, monitoring, inventory, topology visualization, API, RBAC, SSO, and configuration management workflows, while identifying addressed issues affecting CAPWAP connectivity, client visibility, authentication, licensing, firmware upgrades, and user interface behavior. Known issues and limitations include schema migration risks, SSO session persistence, visualization constraints, TPME management restrictions, scaling considerations, and firmware compatibility requirements. Intended for network administrators, operations teams, and technical support personnel, the release notes provide deployment prerequisites, supported browser and firmware versions, troubleshooting guidance, security-related authentication considerations, and compatibility information necessary for successful enterprise-scale deployment and platform upgrades.



Help and Support

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

Extreme Portal

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

The Hub

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

Call GTAC

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

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

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

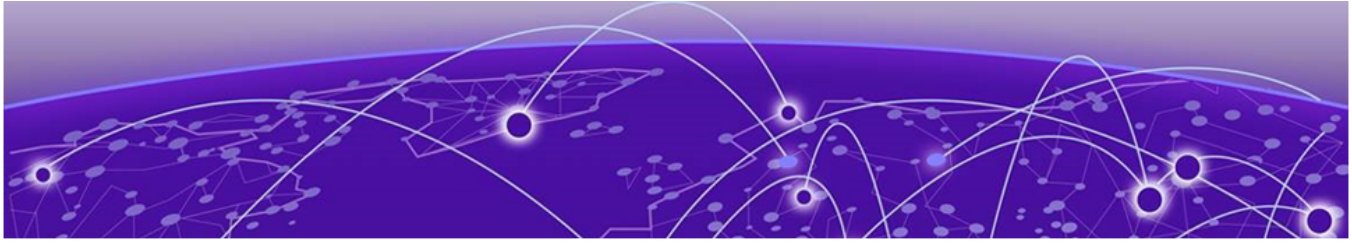
Subscribe to Product Announcements

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

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

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

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



General Release Information

Browser Support and Display Settings on page 10

Current Release: 25.14.0-331 Component update 25.14.1-3

October 2026

This release resolved an issue causing sporadic latency and slow page-rendering when navigating the **Dashboard**, **Devices**, **Clients**, and **Sites** views.

Related Links

- Known Issues on page 20
- Device Support Information on page 27

Release: 25.14.0-331 (Patch 1)

October 2026

This patch release addresses database performance issues, improves login service stability and capacity, and includes updated OpenAPI documentation.

Related Links

- Known Issues on page 20
- Device Support Information on page 27

Release: 25.14.0-331 (Patch 1) Addressed Issues

Issue ID	Description
XCP-29053	Updated the Asset Management OpenAPI specification and Developer Portal documentation for the POST /devices endpoint to include previously undocumented response fields: `delete_allowed` and `xiq_se_server_id`. The schema and documentation now fully reflect the active API response models for cloud-managed and ExtremeCloud IQ Site Engine-managed devices.

Release: 25.14.0-331

September 2026

Related Links

- Known Issues on page 20
- Device Support Information on page 27

Introduction to Extreme Platform ONE Networking

The following are a few key features:

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

Extreme Platform ONE Public IP Address Blocks

Data Center	IP Block	Addresses and Ports
Global Data Center (GDC)	44.234.22.92/30 18.194.95.0/28 34.253.190.192/26 3.234.248.0/27	
Australia (AUS)	13.210.3.192/28 18.98.198.80/28	Firewall Address and Port Information
Azure, Canada Central (ACA)	20.151.64.48/28	Firewall Address and Port Information
Azure, US East (AVA)	52.226.89.112/28	Firewall Address and Port Information
Brazil (BR)	18.228.70.16/28	Firewall Address and Port Information
Germany (FRA)	3.67.81.96/27 18.194.95.0/28	Firewall Address and Port Information
India (IN)	13.232.67.8/29 3.6.70.64/29	Firewall Address and Port Information
Ireland (IE)	34.253.190.192/26	Firewall Address and Port Information
Japan (JP)	18.176.203.112/29 13.231.6.232/29 57.181.58.0/28	Firewall Address and Port Information
Netherlands (NL-GCP)	34.91.82.64/27	Firewall Address and Port Information
Singapore (SG-GCP)	34.87.158.80/28	Firewall Address and Port Information
Spain (ES)	18.101.49.128/27	Firewall Address and Port Information

Data Center	IP Block	Addresses and Ports
Sweden (SE)	13.48.186.224/29 13.48.4.184/29 13.48.4.240/28	Firewall Address and Port Information
Switzerland (ACH)	51.107.1.192/28	Firewall Address and Port Information
United Arab Emirates (UAE)	3.28.159.128/28	Firewall Address and Port Information
United Kingdom (UK-AGB)	51.143.233.80/28	Firewall Address and Port Information
US East (VA)	34.202.197.0/26 44.192.245.0/26 3.234.248.0/27	Firewall Address and Port Information
US East 2 (VA2)	34.202.197.0/26 44.192.245.0/26 3.234.248.0/27	Firewall Address and Port Information
US-Iowa (IA-GCP)	34.67.130.64/27	Firewall Address and Port Information
US Ohio (OH)	3.145.235.64/26	Firewall Address and Port Information

Supported Applications

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

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

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

Extreme Platform ONE Networking supports the following applications:

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

Browser Support and Display Settings

Note
Extreme Platform ONE does not support 32-bit browsers.

Desktop Browsers

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

- Chrome
- Edge
- Firefox
- Opera
- Safari

Microsoft Internet Explorer is not supported.

Display Settings

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

Previous Release

New Features on page 11
Addressed Issues on page 14

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

New Features

Table 1 on page 12 lists the new features introduced in Extreme Platform ONE Networking release 25.14.0-331.

For more information about Extreme Platform ONE Networking features, see the Extreme Platform ONE Networking v25.14.0 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 0.9.44
    - Switch Engine/EXOS release >= 33.2 upgrade to IQAgent version 1.9.44
  - 33.7.1.6-patch1-11 Latest Supported GA Patch

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

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

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

    Onboard, Monitor, Config, Image Mgmt, and Global Download Support
- Fabric Engine/VOSS:
  - 0.9.41 IQAgent Support
  - 9.4.1.0 Latest Supported GA Image

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

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

- 8.10.9.0 Previous Supported GA Image

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

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

New Hardware Support

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

Table 1: New Features in release 25.14.0-331

Feature ID	Feature	Description
NVO-11822	Enhanced Visibility and Support for Partially Connected Devices	Improves detection and reporting of specific error categories for devices that fail to connect to the Network Visualization and Orchestration backend during onboarding.
NVO-16304	Visualization and Navigation Usability Enhancements	Renames **Restore Settings** to **Restore Saved User Settings** in all views, adjusts the **Burst** view when it extends beyond the screen, and scrolls the **Quick Location Navigator** to the selected item when it opens.
SEN-284	Automated Third-Party Management Engine Deployment and Management on Universal Compute Platform 1130	Adds support for deploying the Third-Party Management Engine (TPME) on the Universal Compute Platform (UCP) 1130, including automatic onboarding to Extreme Platform ONE Networking, location and serial number inheritance from the Universal Compute Platform, and CLI console access for basic connectivity configuration.
SEN-756	Static IP and Dedicated Interface Support for TPME on UCP 1130	Adds static IP support when the TPME runs on a Universal Compute Platform. The engine reports its correct IP address instead of an address behind network address translation, and other services on the engine remain accessible from outside the platform.
SEN-911	Centralized User and SSH Access Management for TPME	Adds a default user account with a set password to the configuration of a newly deployed TPME virtual machine, without adding the account automatically on upgrade.
WS-4526, XCP-21442	Centralized Task Center for Scheduled and Historical Operations	Adds the **Task Center**, where users view historical and scheduled tasks such as firmware upgrades, configuration backups, and backup restores, along with their status and results.
XCP-9752	Configuration Restore for TPME -Managed Devices	For connected devices managed through the TPME, you can now restore a device configuration from a previous backup from **Inventory**, **Network Devices**, or the **Object Inspector**. Available backups are listed by name, date/time, and file size, and are searchable; you can also preview a backup's contents before restoring.

Table 1: New Features in release 25.14.0-331 (continued)

Feature ID	Feature	Description
XCP-10751	Multi-Select and Bulk Deletion for KDDR Logs	Adds multiselect and **Select All** support for deleting Kernel Diagnostic Data Recorder (KDDR) logs in Extreme Platform ONE Networking.
XCP-17768, XCP-21158, XCP-18078	Inventory Manager Enhancements for TPME	Adds firmware upgrade support and configuration backup scheduling to the Inventory Manager for the TPME . Users upload firmware to a configured repository, and the engine transfers the image to the third-party device by CLI script or SNMP. Extreme Platform ONE reads the firmware version, blocks corrupt or unsupported files, and determines device compatibility before performing the upgrade. The upgrade is fully logged in the history and audit logs. Captured data includes who performed the upload and the outcome for each device. Users configure daily, weekly, or monthly backups with a configurable start time.
XCP-19393	Centralized SSH & CLI Credential Configuration for TPME	Centralized SSH and CLI Credential Configuration for TPME is now supported.
XCP-25714	Enhanced Location Synchronization for TPME	Enhanced Location Synchronization for TPME . Synchronizes site, building, and floor information across the **Inventory** page and **Network Devices** page for TPME devices.
XCP-27334	Fabric Engine/ VOSS Version 9.3.4 Support	Adds support for onboarding, monitoring, configuring, and downloading images for Fabric Engine/VOSS version 9.3.4 on the 7830, 7720, 7520, 5720, 5520, 5420, 5320, and applicable 4220 Universal Switches, and on the VSP7400 and VSP4900.
XIQ-46782	Access Point Real-Time Power Draw Reporting in Device360	Reports the actual power draw for Wi-Fi 6E and Wi-Fi 7 access points that support the power usage statistic. The value displays, rounded to the nearest whole watt, on the eth0 interface in **D360** > **Wired Interfaces**. Supported access points include the AP3000, AP5000, AP5020, AP4020, AP302W, AP305C, and AP4000; the AP510C and AP650 do not support the statistic.
XIQ-46815, XIQ-50555	Device360 Support for Third-Party Managed Devices	Adds device details for devices managed through the TPME. Adds a **Properties** tab with SNMP timer details, configuration and firmware repository, and configuration backup schedule. Expands the **Overview** tab status with Backup, Restore, and Firmware Upgrade information. Adds more details to the Port Stats view.
XIQ-49984, XIQ-49987	Report in Device360 for Backup Schedules for TPME Devices	Adds a report in Device360 for backup schedules for TPME devices. Detailed information includes: last backup status, backup schedule, and link to backup history.

Addressed Issues

Table 2 lists Addressed Issues in Extreme Platform ONE Networking release 25.14.0-331.

Table 2: Addressed Issues in release 25.14.0-331

Issue ID	Description
CFDs	
CFD-14649	Addressed the issue where a delta configuration push failed with a rate-limit multicast error for an aggregated interface, and prevented further delta updates on the affected access point.
CFD-17067	Addressed the issue where NAC Profile and NAC Details did not populate for most clients in **Client 360**, even though ExtremeControl reported the corresponding end-system details.
CFD-17082	Addressed the issue where an inactive wireless device showed as a wired device on the connected switch port instead of retaining its last known access point association.
CFD-17244	Addressed the issue where certificate bundles created under **Common Objects** > **Certificate Management** for OpenRoaming were not persisted or validated correctly.
CFD-17501	Addressed the issue where an access point showed as offline in ExtremeCloud IQ while its CAPWAP client status indicated a secure connection to the CAPWAP server.
CFD-17704	Addressed the issue where an AP4020 running IQ Engine 10.8.5.4 intermittently lost its CAPWAP connection.
CFD-17878	Addressed the issue where new AP3000 access points failed to onboard because they did not receive a country code, CAPWAP server IP address, or Hive Manager primary or backup name.
CFD-17996	Addressed the issue where access points showed as online but were unreachable during a bulk configuration push.
CFD-18029	Addressed the issue where an eduroam SSID could not be deleted under Extreme Platform ONE Security after the eduroam integration was performed.
CFD-18081	Addressed the issue where acknowledging alerts on a second page failed when the alerts page was set to display 500 alerts.
CFD-18102	Addressed the issue where the **Resource Center** icon did not reopen the **Resource Center** overlay after the overlay was closed.
CFD-18103	Addressed the issue where toggling **Additional Columns** on and off in the **Network Devices** default view reset the customized column order.
CFD-18109	Addressed the issue where IP range classification rules in network policies could not extend beyond a single /24 subnet.
CFD-18110	Addressed the issue where running the Show IKE SA diagnostic under **Utilities** > **Diagnostic** did not complete.
CFD-18123	Addressed the issue where the default last-24-hour time range in the **Users** view did not advance to include the current time.

Table 2: Addressed Issues in release 25.14.0-331 (continued)

Issue ID	Description
CFD-18180	Addressed the issue where uploading a captive web portal (CWP) file under SSIDs returned a file named `TRUE` instead of the uploaded file.
CFD-18186	Addressed the issue where Cloud PPSK users could not authenticate for up to a few hours after creation.
CFD-18214	Addressed the issue where clicking a diagnostic widget in the Object Inspector reloaded the entire web application instead of opening the corresponding detail view, and in some cases required the user to log in again.
CFD-18221	Addressed the issue where setting a port type to Trunk in a device template omitted the VLAN configuration, so all trunk ports used the default VLAN and could not be customized during port type configuration.
CFD-18226	Addressed the issue where clicking the client count in the **Client Health** widget (from a managed access point Object Inspector) opened the Clients view with an unsupported hostname filter and returned no results.
CFD-18229	Addressed the issue where clients connected to an access point were not displayed under **Monitoring** > **Clients** in Extreme Platform ONE Networking.
CFD-18233	Addressed the issue where exporting the `kat_encryption_audit_log` table failed with an internal error.
CFD-18271	Addressed the issue where saving an open SSID with an ExtremeGuest captive portal and a custom, non-default user profile reverted the profile to the default guest profile (VLAN 1).
CFD-18296	Addressed the issue where the Discovered section of **Network Devices** > **Device Status** entered an endless refresh loop when sorted by any column other than serial number.
CFD-18309	Addressed the issue where a timed-out account deletion prevented a customer from using the associated email address to register a new account.
CFD-18330	Addressed the issue where a duplicate portal account for a customer email address prevented the customer from being added as an administrator.
Account Management	
XCP-24592	Addressed the issue where switching to an account with a Pilot license opened ExtremeCloud IQ (New) instead of ExtremeCloud IQ (Classic) as the default landing page.
XCP-26459	Addressed the issue where a newly added external user did not appear in the External Users list and returned an HTTP 400 error.
XIQ-52932	Addressed an issue where IDM gateway post-authentication logging timeouts caused valid Cloud PPSK authentication requests to fail with an Access-Reject.
API	

Table 2: Addressed Issues in release 25.14.0-331 (continued)

Issue ID	Description
XCP-26361	Addressed the issue where the `cs-metaflow-telemetry-server` and `cs-metaflow-metrics-telemetry-server` deployments remained in a degraded state.
XCP-26979	Addressed the issue where the `cs-event-mvtx-highpriority` and `cs-metric-mvtx-highpriority` applications remained in a degraded health state after deployment.
Device Management	
XCP-22882	Addressed the issue where assigning an Access Profile to TPME-managed devices did not set the deployment status to "Draft".
XCP-23557	Addressed the issue where the **Access Management External Users** page fails to load and returns a validation error when the page size is set to 500.
XCP-24254	Addressed the issue where the user interface did not show the configuration delta and audit logs for a device in the deployment dialog.
XCP-27441	Addressed the issue where an intermittent "Device Not Found" error displayed when a user selected the **Restore** action.
XIQ-52258	Addressed the issue where an AP5022S6D configured for dual 6 GHz operating mode (6H/5/6L) included channels 97 through 125 in the 6H band for the Peru, Kazakhstan, Dominican Republic, and Brazil country codes.
XIQ-52259	Addressed the issue where the AP3020 applied an incorrect transmit power to the WiFi1 interface for the Italy country code.
XIQ-52263	Addressed the issue where SSID configuration on an AP3020 failed when the security mode was set to WPA with TKIP.
Logs	
XIQ-52219	Addressed the issue where Supplemental CLI commands remained listed in the **Delta Configuration Audit** view after a **Complete Update** successfully applied them.
Onboarding	
XCP-25738	Addressed the issue where onboarding a Switch Engine/EXOS or Fabric Engine/VOSS device with an access point serial number did not display a validation message and the onboarding API returned an HTTP 500 error.
Roles	
XCP-21032	Addressed the issue where BizOps users are unable to view TPME device details in the Device360 page. When attempting to access the page for TPME-managed devices, the page opens but displays no device data.
XCP-24402	Addressed the issue where an SSH session launched from Visualization for a user with the Observer role, then timed out immediately.

Table 2: Addressed Issues in release 25.14.0-331 (continued)

Issue ID	Description
XCP-26977	Addressed the issue where creating an internal or external user with the BizOps or Guest Management role displayed a validation error.
XCP-26998	Addressed the issue where **Task Center** data did not load for users with the NetSecOps or Observer role.
XCP-27090	Addressed the issue where the **Task Center** menu displayed for the Guest Management role.
XIQ-51101	Addressed the issue where NetSecOps and BizOps external users are unable to delete devices from the **Network Devices** page. The deletion initiation notification appears, but the deletion does not complete.
Upgrading	
XCP-14211	Addressed the issue the **Firmware Version** dropdown is not visible during a firmware upgrade when multiple APs are selected and the last device in the list is reviewed on high-resolution displays.
XCP-25227	Addressed the issue where the `cs-perfmonitor-ingestion` consumer group developed a lag after an upgrade.
User Interface	
SEN-731	Addressed the issue where a port on an Enterasys C2H124 reported as **Admin Disabled** while the link was up and operational, with devices connected, in ExtremeCloud IQ Site Engine.
SEN-913	Addressed the issue where the CPU Usage and Memory Usage charts on the TPME device details **Overview** page did not populate for devices that were not yet discovered or added.
WS-4770	Addressed the issue where several login page fields, including the forgot-password link, SSO login button, login-via-Extreme-portal link, and registration link, did not load in the mobile view.
WS-4795, WS-4796, WS-4797, WS-4798	Addressed the issues where the **Visualize**, **Dashboard**, **Alerts**, and **Network Device** pages displayed user interface issues in the mobile view.
WS-4799	Addressed the issue where users could not easily navigate back to a page after opening the 9-dot menu or profile icon in the mobile view.
WS-4800	Addressed the issue where forms on the **Profile** page did not use the full available space in the mobile view.
XCP-23080	Addressed the issue 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-23110	Addressed the issue where the **Device Health** page widget marks a device as having a CPU issue based on per-core utilization while the grid displays a non-issue average CPU value, creating a mismatch between the widget and the grid.
XCP-23841	Addressed the issue where the **Client Health** summary widget intermittently was out of sync with the data grid.

Table 2: Addressed Issues in release 25.14.0-331 (continued)

Issue ID	Description
XCP-23919	Addressed the issue where the **Resource Utilization** widget did not display in the D360 overview widget section.
XCP-24032	Addressed the issue where CPU utilization on the **Device Health** page did not update for the backup slot in a stack device.
XCP-24232	Addressed the issue where the **Sites** page took an extended time to load, expand, and collapse a site group containing a large number of sites.
XCP-24911	Addressed the issue where total throughput (Rx and Tx PPS) did not update with correct data on the **Wired Usage and Capacity** page.
XCP-24944	Addressed the issue where the Usage Capacity grid port congestion filter did not include stack devices.
XCP-25112	Addressed the issue where **Alerts** page filters were not applied correctly when navigating from the **Dashboard Alert** widget.
XCP-25759	Addressed the issue where the access profile for TPME-managed devices displayed an error state after a floor associated with those devices was deleted.
XCP-25796	Addressed the issue where the **Image Scale** page rejected a floor width or height under 1000 meters with a message stating the value could not exceed 1000 meters, preventing the image from being saved.
XCP-25928	Addressed the issue when 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.
XCP-26932	Addressed the issue where Scope displayed the wrong hostname for a device when only one device was present.
XCP-26967	Addressed the issue where timeline details did not display correctly by default on the **Task Center** summary page.
XCP-27314	Addressed the issue where the configuration backup schedule tab of D360 for the TPME showed no data.
XCP-27326	Addressed the issue where the **Client Health** page displayed a "Something went wrong" error and no client health data.
XCP-27444	Addressed the issue where the configuration firmware repository, SNMP timer, and SSH and CLI credentials tab of D360 for the TPME showed no data.
XIQ-49859	Addressed the issue where the 6 GHz channel for an AP5060 configured for low-power mode displayed on Maps as 6GHz SP instead of 6GHz LP.
XIQ-52260	Addressed the issue where the serial number overlapped an adjacent column on the **Network Devices** page after a device was managed or unmanaged.
XIQ-52350	Addressed the issue where an access point appeared twice on the **Usage & Capacity** view of the **Network Devices** page.

Table 2: Addressed Issues in release 25.14.0-331 (continued)

Issue ID	Description
XIQ-52395	Addressed the issue where the **Device Status** view for AFC wireless devices showed empty widgets for a selected site.
Visualize	
NVO-14810	Addressed the issue where devices that are managed by the TPME can be displayed twice in **Visualization** when there is link aggregation between cloud native devices and TPME-managed devices.
NVO-15493	Addressed the issue where changing ports on a 7830 switch with an 8DE VIM from auto-sense to fabric trunk applied STP settings inconsistently across the ports.
NVO-18703	Addressed the issue where a TPME-managed device did not display in its new location in the access view after the device location changed, showing only access points without their connections.

Known Issues

Table 3 lists the Known Issues in Extreme Platform ONE Networking release 25.14.0-331 Component update 25.14.1-3.

Table 3: Known Issues in release 25.14.0-331 Component update 25.14.1-3

Issue ID	Description
CFD	
CFD-17814	Contracts associated with switches do not appear in the **Inventory** page for some assets in Extreme Platform ONE, even after removing and re-onboarding the devices.
CFD-18080	In the current release, the **Clients** view displays only actively connected clients by default. As a result, clients are removed from the main **Clients** list shortly after they disconnect. Previously connected clients can still be viewed by applying the Disconnected filter. This behavior is a known limitation and is functioning as designed. A future release is planned to introduce enhanced historical client visibility and remove the current restriction that limits the default view to connected clients only.
API	
XCP-23938	The release 25.12 database schema migration introduced NOT NULL columns without defaults to platform_common_db CDC tables, causing the Debezium AVRO connector to fail with a schema registry incompatibility error.
XCP-23971, XCP-24089	On the **Device360 Port Stats** and **Clients** pages, graphs and UI widgets (including the Port Stats graph, Port Description grid, Port Stats Summary, Link PoE, and Usage/Utilization widgets) pull data from the legacy monitoring APIs instead of from the PerfMonitor APIs.
XCP-26696, XCP-26702, XCP-26712	The `cs-metastore-event-ingestion`, `xcloudiq-license-scheduler`, CAS, and CNS applications are deployed with a single replica and without a configured health check.
Device Management	
XCP-5227	Incorrect `Managed_by value` for locally managed devices.
XCP-17157	Extreme Platform ONE Networking does not support setting or updating the Third-Party Management Engine (TPME) hostname using the **Configure** option. This is a documented limitation.
XCP-18640	The **Retry** action is disabled after the configuration deployment fails for the Third-Party Management Engine.

Table 3: Known Issues in release 25.14.0-331 Component update 25.14.1-3 (continued)

Issue ID	Description
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).
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-51853	The **Configuration Audit** view does not display the individual configuration changes, such as SSID, VLAN attributes, DNS server, NTP profile, and QoS settings, that a Network Policy applies after it is assigned to an access point.
XIQ-51982	When Wifi0 on an AP3020W is configured for 6 GHz radio in client mode, the required radio profile commands for the 6 GHz configuration are not generated.

Table 3: Known Issues in release 25.14.0-331 Component update 25.14.1-3 (continued)

Issue ID	Description
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.
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-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.

Table 3: Known Issues in release 25.14.0-331 Component update 25.14.1-3 (continued)

Issue ID	Description
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	
	Starting in 25.14.0, firmware upgrades use the new V2 API (DLCS) and upgrade activity is tracked in **Task Center** rather than the **Firmware History** page. Existing entries from 25.13.0 and earlier remain visible in **Firmware History**, but any new upgrade initiated in 25.14.0 or later will appear only in **Task Center**. The **Reschedule**, **Cancel**, and **Retry** actions are no longer available in **Firmware History**. Support for these actions in **Task Center** is targeted for a future release.
XCP-12063, XCP-12064, XCP-16651	An audit log is not generated for a scheduled a firmware upgrade, when firmware upgrade successfully completes, or when a firmware upgrade fails.
XCP-17804	Following an upgrade, certain data schemas may fail to register due to compatibility conflicts with previously stored schema versions. This can prevent some telemetry and client event data from being processed correctly until the issue is resolved.
XCP-25556	When a custom-uploaded firmware image is assigned the same version number as an existing default (system) firmware image for the same product type, a firmware upgrade using the custom image applies the default image instead. As a result, the device does not receive the intended custom firmware.
User Interface	
NVO-15001	Port Description in Link & Port details for devices managed by TPME contain incorrect values.
WS-4616	When an existing user clicks the **Pendo Resource Center** icon in Extreme Platform ONE Networking, the **Product Tours** section does not appear.
WS-4801	Clicking the **Help** icon in the mobile view does not open the **Resource Center**.
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 **Device360** 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.

Table 3: Known Issues in release 25.14.0-331 Component update 25.14.1-3 (continued)

Issue ID	Description
XCP-19865	No failure details are displayed in the user interface when a TPME configuration deployment fails. The deployment API response confirms a failed status but does not include a failure reason, and no corresponding audit log entry is generated.
XCP-20134	The filter chip for the Extreme Platform ONE Networking selection in the Application Access column filter in **Access Management** is not displayed, preventing confirmation that the filter has been applied.
XCP-21438	When the Extreme Platform ONE Networking idle session timeout is reached while navigating Universal ZTNA through the 9-dot menu, Universal ZTNA displays an "Auto-Logout in 1528 seconds" pop-up instead of following the Extreme Platform ONE Networking idle timeout behavior.
XCP-22682	Management port statistics are not displayed on the **Usage and Capacity** page for Switch Engine/EXOS devices that have all standard ports disabled.
XCP-22746	The **Total Client** count on the **Usage and Capacity** page returns 0 for wired devices, even when client entries exist for those devices.
XCP-23090	Device health issue reporting latency has increased. Temperature issues on Fabric Engine devices now take approximately 3 to 4 minutes to appear under **Device Health**, compared to approximately 1 minute in previous releases.
XCP-23112	When a filter is applied on the **Device Health** page, other columns such as **CPU Usage%**, **Memory Usage%**, and **PSU Usage%** display N/A. This behavior applies to all **Device Health** issue filters.
XCP-23128	IPv4 and IPv6 null values (N/A) are not sorted correctly during ascending and descending sort operations on the client table. Null values appear at the end during ascending sort and not at the beginning during descending sort.
XCP-23139	Extreme Platform ONE Networking displays N/A for all metrics in the second row for a Switch Engine/EXOS switch in the **Device Health** and **Usage and Capacity** pages when multiple Switch Engine/EXOS switches are onboarded.
XCP-23307	Filter options and **Edit**/**Delete** actions are not available for Subscription & Licensing request history.
XCP-23406	The **Total Queue Congestion Packets** column under **Usage & Capacity** > **Wired** displays an incorrect value for Stack devices. 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-23450	A duplicate device row appears on the **Usage and Capacity** page.
XCP-23558	In the **Device360** 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-23997	The **Device Health** widget does not display on the **Device360** overview page for stack devices.

Table 3: Known Issues in release 25.14.0-331 Component update 25.14.1-3 (continued)

Issue ID	Description
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-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-27843	Clarified CPU and Memory utilization support in Performance Monitoring: CPU and memory statistics are supported on newer device platforms; legacy CAPWAP devices (such as AP4000 and AP410C) do not report these metrics to Performance Monitoring and may display a value of 0%.
XIQ-42050, XIQ-42051	Issues exist with FIPS enabled filters. The **Manage Application** page displays all applications instead of filtering to show only FIPS-enabled applications, and the **Manage Summary** widget shows inaccurate data for **Top Application Groups**, **Top Usage**, and **Total Application Usage** metrics.
XIQ-46203	On the **Monitoring** > **Clients** > **Users** tab, the Source value displays Other instead of Others.
XIQ-47622	The **Users** grid XAPI request times out when the Status=Connected filter is applied to a dataset of approximately 148,000 user records.
XIQ-47708	The summary widgets on the **Users** page fail to load when the page contains approximately 500,000 user records.
XIQ-48218	Selecting **Configure** from **Network Devices** displays **Third Party Management** instead of **Configuration Profile**.
XIQ-49488	The **Client Density** heatmap displays an inaccurate client count that does not match the count shown on the client inventory page.
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-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.

Table 3: Known Issues in release 25.14.0-331 Component update 25.14.1-3 (continued)

Issue ID	Description
XIQ-52087	The **Roaming Issues** filter on the **Clients** > **Wireless** widget returns clients with no roaming issues instead of clients that have roaming issues.
Visualize	
NVO-15660	A Link Aggregation Group (LAG) configured between an EXOS/Switch Engine switch and an access point intermittently loses its LAG visualization on the network canvas and displays as a single link. The LAG configuration is correctly shown on both the Switch Engine/EXOS device and the AP, but the visualization canvas fails to consistently represent the aggregated link bundle.
NVO-15748	The **Visualization** page and **Device Inspector** panel do not update 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 **Device360**.

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 ExtremeCloud IQ 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 27
Access Points (Universal Hardware) on page 28
Switches (Universal Hardware) on page 30
ExtremeCloud IQ Site Engine on page 32

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 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP305C	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP305C-1	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP305CX	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP3000	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP3000X	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP3020/W/X	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.5
AP4000	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP4000-1	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP4020/X/FX	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.4
AP4060	IQ Engine 10.9.1 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.4
AP410C	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP410C-1	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP460C	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP460S6C	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP460S12C	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP5010	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP5020	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (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
AP5022/FX/S6D	IQ Engine 10.9.2 AP 10.20.1	N/A	N/A
AP5050U/D	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (10.8.5.6)	IQ Engine 10.8.2
AP5060U/D	IQ Engine 10.9.2 AP 10.20.1	N/A	N/A
AP510C/CX	IQ Engine 10.9.2 AP 10.20.1	IQ Engine 10.8.5f (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
25.8.12	• 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 Extreme Platform ONE 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 Extreme Platform ONE subscriptions
25.11.10	• License allocation • Device Assignment to the Extreme Platform ONE • Device Statistics • Port Statistics • Unmanage/Manage device • Device Group to CCG mapping • Stack members • NAC details update for wireless end-systems • Wired end-systems reported to Extreme Platform ONE • Detect and report orphaned devices • Compatible with Extreme Platform ONE subscriptions

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

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

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