ExtremeCloud™ Orchestrator v4.0.0 Release Notes

New Features, Supported Platforms, and Known Issues

9039317-00 Rev AB
August 2025

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/

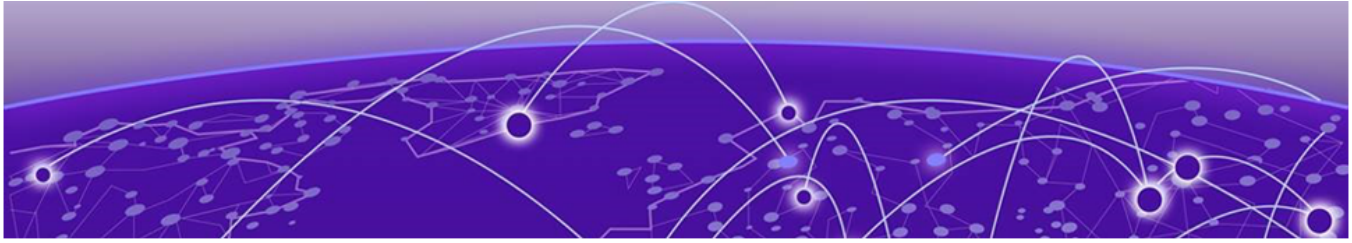
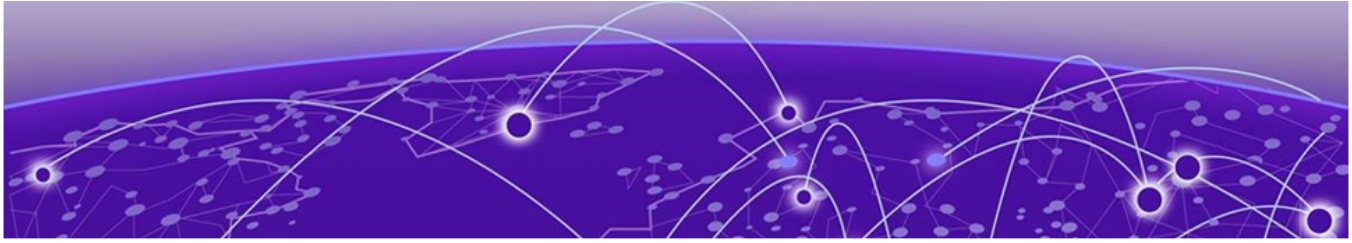
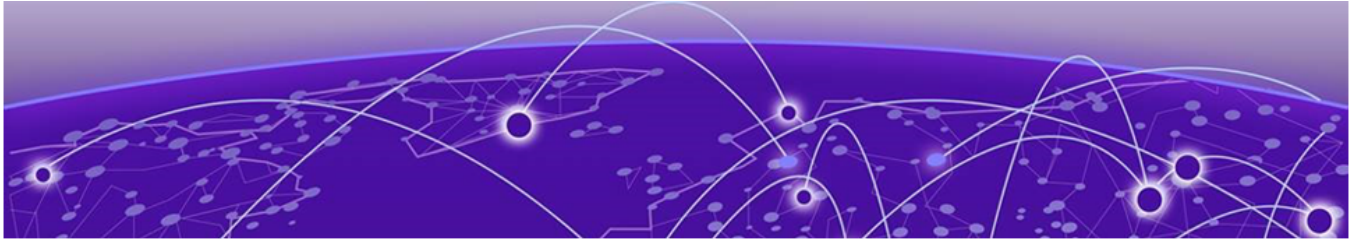


Table of Contents



Abstract

ExtremeCloud™ Orchestrator v4.0.0 introduces enhanced lifecycle management capabilities through integration with XCO ONE OS, supporting advanced fabric provisioning, multi-tenant networking, and automation features. The release includes improvements to CLI and API interfaces, expanded deployment options, and updated platform support. Operational diagnostics, notification services, and system hardening have been strengthened, alongside updates addressing known defects and security vulnerabilities.



Release Notes

New In This Release

ExtremeCloud Orchestrator 4.0.0 introduces the following features and enhancements, and resolves issues through defect fixes. For information about XCO deployment, refer to the *ExtremeCloud Orchestrator Deployment Guide, 4.0.0*.

Note

- In release 3.2.0 and later, Extreme Fabric Automation (EFA) is referred to as ExtremeCloud Orchestrator (XCO). The terms EFA and XCO refer to the same product and are used interchangeably.
- As of version 4.0.0, the ExtremeCloud Orchestrator (XCO) no longer includes support for the Visibility Skill. This deprecation follows the official End-of-Sale (EOS) announcement issued on February, 2025.

Table 1: Features and Enhancements

Feature	Description
XCO ONE OS Integration and Platform Expansion	XCO 4.0.0 introduces foundational support for XCO ONE OS devices and adds compatibility with the Extreme 8730 platform. For more information, see *ExtremeCloud Orchestrator v4.0.0 CLI Administration Guide*.
Supportsave Enhancements for SLX Devices	Additional debugging information in the command output help users identify underlying issues. For more information, see *ExtremeCloud Orchestrator v4.0.0 CLI Administration Guide*.
Next-Hop Configuration	You can configure the 'next-hop ' in a route-map for advertising eBGP IPv6 prefixes to a specific neighbor. For more information, see *ExtremeCloud Orchestrator v4.0.0 CLI Administration Guide*.
Bulk Support for Tenant EPG APIs	Bulk support for tenant EPG APIs, enables faster configuration, updates, and deletions of EPG configurations by processing multiple EPGs in a single request. For more information, see *ExtremeCloud Orchestrator v4.0.0 CLI Administration Guide*.
Support Matrix	Updated the support matrices for supported platforms and deployment models. For more information, see *ExtremeCloud Orchestrator v4.0.0 Deployment Guide*.

Table 1: Features and Enhancements (continued)

Feature	Description
New and Modified Commands	New commands: • efa inventory device firmware-download history • efa inventory device firmware-download operational-history Modified commands: • efa policy route-map list • efa policy route-map-set create • efa policy route-map-set delete • efa system supportsave For more information, see *ExtremeCloud Orchestrator v4.0.0 Command Reference*.
System Hardening for CIS-CAT Assessments	CIS-CAT Assessments system hardening updates. For more information, see *ExtremeCloud Orchestrator v4.0.0 Security Configuration Guide*.

For other additional information, Closed Defects on page 22.

XCO ONE OS Integration

Extreme ONE OS is a cloud-native, microservices-based network operating system designed for IP fabrics and data center environments.

Note

- The features related to XCO ONE OS and Extreme 8730 support in XCO 4.0.0 are released as Control Released Features.
- For comprehensive feature descriptions, CLI command references, administrative procedures, and API documentation, contact Extreme Networks.

The following features are included as Control Released Features in XCO 4.0.0:

- XCO ONE OS Integration: Lifecycle management support for XCO ONE OS-based devices.
- Extreme 8730 Support: Inventory and fabric integration for the new platform.

- Secure Settings via GNMI: Centralized enforcement of SSH, TLS, and password policies.
- CLI and API Enhancements: Extended command coverage for device and fabric operations.

Note
Config Drift Tracking is not supported.

Table 2: Supported ONE OS features

Feature	Description
Fabric	
Non-Clos Fabric Support	XCO automates both Clos and non-Clos environments. The following are supported for non-Clos fabrics: • Automated provisioning of Layer 2 and Layer 3 services • Tenant-aware networking, including VLANs and VRFs • Simplified configuration workflows via CLI and REST APIs • MCT (Multi-Chassis Trunk) for redundancy XCO uses microservices running on a lightweight Kubernetes cluster (K3s) to orchestrate these functions, whether deployed on TPVM (Third-Party Virtual Machine) or external VMs.
Tenant	
Tenant PO	A port channel, also known as a Link Aggregation Group (LAG) is a communication link between devices. For creation of single-homed or multi-homed port channel for ONE OS devices, you can specify the following parameters: LACP negotiation, LACP timeout, Port Port channel number, MTU, Number of active links required. Speed is not required for port channel creation unlike SLX devices.
BD based L3 EPG Support (Auto-VNI) & VLAN based L3EPG Auto-VNI	An endpoint group is a logical group of endpoints or devices connected to the network. These endpoints are used to deploy Layer-2 or Layer-3 services over the fabric. To create Layer-3 service, you can specify parameters: Group name IP address, port channels, switchport mode, CTAG range, associated VRF, bridge domain, and neighbour discovery preferences.

Table 2: Supported ONE OS features (continued)

Feature	Description
Auto VNI Map Fabric with BD-Based Tenant and L2 EPG	Enables automatic VXLAN Network Identifier (VNI) mapping for tenants in a non-Clos fabric, using Bridge Domain (BD)-based segmentation and Layer 2 Endpoint Groups (EPGs). The following features are supported: • Auto VNI Mapping: ◦ For VLAN-based tenants ◦ For BD-based tenants • BD-Based Tenants: ◦ Multiple tenants can share the same VLAN ◦ Each VLAN is mapped to a unique BD, which then maps to a unique VNI. • L2 EPG: ◦ Allows grouping of endpoints at Layer 2 ◦ Facilitates policy enforcement and traffic segmentation within the same subnet. • Multi-Tenant: ◦ Tenants can have overlapping VLANs (ctags) ◦ Each tenant gets a unique L2VNI and isolated network space. Ideal for multi-tenant data centers where isolation, scalability, and automation are critical.

Table 2: Supported ONE OS features (continued)

Feature	Description
Auto VNI Map Fabric - VLAN Based Tenant, L2 EPG	Enables automatic VNI assignments for VLAN-based tenants in a Clos fabric, with support for Layer 2 Endpoint Groups (EPGs) as part of the Tenant Service integration in XCO. The following features are supported: • Auto VNI Mapping: ◦ For VLAN-based tenants, the VNI is statically derived from the VLAN ID ◦ Simplifies VXLAN configuration by eliminating manual VNI assignment. • L2 EPG: ◦ Groups endpoints within the same VLAN/subnet ◦ Enables policy enforcement and traffic segmentation at Layer 2 • Multi-Tenant Isolation: ◦ Each tenant gets a unique L2VNI ◦ Prevents VLAN overlap across tenants by enforcing one-to-one VLAN-to-VNI mapping ◦ Ideal for multi-tenant data centers where VLAN-based segmentation is preferred, and automation of VXLAN overlays is needed for scalability and consistency.

Table 2: Supported ONE OS features (continued)

Feature	Description
Virtual Routing and Forwarding (VRF)	Enables Tenant Service to integrate with VRF instances, allowing for multi-tenant Layer 3 segmentation within a non-Clos fabric. The following features are supported: • Tenant-Specific VRFs: ◦ Allows assignment of one or more VRFs to each tenant for isolated routing domains. ◦ Prevents route leakage and ensures traffic separation • Distributed and Centralized Routing: ◦ Allows configuration of VRFs for distributed routing on leaf switches or centralized routing on border nodes. • Lifecycle Management: ◦ Create, update, show, and delete VRFs via CLI or REST APIs ◦ Integrated with XCO inventory and policy engine ◦ Ideal for multi-tenant data centers or service provider environments where Layer 3 isolation is required between tenants. ◦ Scalable and secure routing without needing multiple physical routers.
Inventory	
Network Essentials: NTP	Ensures all devices in the fabric maintain synchronized time—a critical requirement for logging, monitoring, and security. The following features are supported: • Inventory Integration: XCO tracks and manages NTP server configurations across devices in its inventory. • Flexible Targeting: Apply NTP settings to specific devices or entire fabrics. • Persistent Configuration: NTP settings are stored in the XCO database for consistency across reboots and updates.

Table 2: Supported ONE OS features (continued)

Feature	Description
Network Essentials: Interface	Enables comprehensive visibility and management of network interfaces across devices in the XCO inventory as part of the Network Essentials module, which provides foundational services for fabric orchestration. The following features are supported: • Interface Listing: CLIs list interfaces on a device • Filter by interface Type: ◦ physical, loopback, ve, po, or all • State Monitoring: ◦ Admin State: up, down, or all ◦ Operational State: up, down, or all • Redundant Management Interface Listing: ◦ Option to list RM-enabled interfaces using --rmelist • Displays interface details: ◦ Device IP ◦ Interface name and type ◦ Admin and operational status ◦ Ensures that device configurations are synchronized with XCO and allows quick detection of drift or mis-configurations.
Support Maintenance Mode	Allows temporary restriction or modification to customer support tools and services during planned maintenance activities, system upgrades, or critical backend operations. This mode: • Ensures system stability during updates • Displays customizable maintenance messages to users • Automatically restores full support functionality post-maintenance • Logs maintenance activities for compliance and review Ideal for rolling out new support features or performing backend updates without disrupting live support.

Table 2: Supported ONE OS features (continued)

Feature	Description
Switch Firmware upgrade	Allows firmware upgrades on deployed fabrics (non-Clos, multi-rack, 3-Clos, 5-Clos) without traffic loss. Supports targeted upgrades using a prepared device list. Optimizes the upgrade process using Maintenance Mode (MM), Drift and Reconcile (DRC), and reboot options based on image build types.
Device and Network Level Settings	Introduces enhanced configuration capabilities at both the device and network levels: • Activates maintenance mode for device upgrades, initiates on-demand health checks, and configures single or periodic configuration backups. • Provides upcoming certificate and password expiry alerts. • Helps configure route load sharing maximum paths, unicast reverse path forwarding, MCT bring up delay.
Device Secure Settings	Enables security configurations on onboarded devices, whether part of a fabric or standalone in the XCO inventory. The following settings are supported: • Min-tls-version • Mac-algorithm • Key-exchange-algorithm • Cipher • Telnet • Max-password-age • Force-default-password-change
Device Password Expiry and Clear	Allows configuration of password expiry attributes on Extreme ONE OS devices. • Password expiry alerts are generated ahead of the expiration date, based on predefined thresholds. • Alert levels include: ◦ Info ◦ Minor ◦ Major ◦ Critical These levels help users take timely action to update passwords and maintain device security.

Table 2: Supported ONE OS features (continued)

Feature	Description
Inventory Switch LCM	Device certificates are installed and configured during ONE OS device registration in XCO.
Switch Health Management (SHM) and DRC	By default, health check functionality is disabled when Extreme ONE OS devices are registered. You can enable health checks on the device using the following operations: • **health-check-enable** • **health-check-interval** • **health-check-heartbeat-miss-threshold** XCO is configured to automatically back up device configurations every 6 minutes by default. XCO also supports Drift and Reconcile (DRC) at the device level. It compares the current device configuration with the expected configuration stored in XCO. If a drift is detected, XCO reconciles the configuration to restore the intended state. APIs are available to initiate drift and reconcile requests.
Switch System Support Save	Collects the system support save of the Inventory, Tenant, and Fabric service logs, and their associated database dumps.
Infrastructure	
TPVM Single Node	Deploys TPVM on ONE OS devices using IAH microservices. After deploying TPVM, you can install XCO using the same process as SLX-based TPVM deployments, with only minor differences in CLI commands. By default, XCO TPVM needs: • CPU: 2 cores • RAM: 4 GB • Disk: ◦ Rootfs – 10GB as per TPVM.img ◦ /apps – as per platform • 2 SSD devices: ◦ Available size 128 GB or 256 GB ◦ Default /apps size 50 GB • 1 SSD devices: ◦ Default /apps size – 30GB

Table 2: Supported ONE OS features (continued)

Feature	Description
TPVM Multinode	Deploys TPVM in a multinode configuration to achieve HA capabilities. To set up TPVM in multinode mode: 1. Deploy TPVM on two separate ONE OS devices. 2. Enable passwordless SSH between the two TPVM instances. This setup allows XCO to deploy required binaries and packages across both nodes without prompting for credentials.
TPVM Upgrade	Currently, only incremental TPVM upgrades are supported for the XCO 4.0.0 release.
Notification Services	Sends notifications to external entities: • Events: Derived from syslog messages from managed devices. • Alerts: Triggered by unexpected conditions in XCO services. • Alarms: Stateful notifications raised and cleared by the system. • Tasks: User-initiated or scheduled operations (e.g., device registration, fabric creation). XCO 4.0.0 ONE OS integration supports: • Alarms • Events • Fault Health Checks Supported Alerts and Alarms: 1. Port Flaps – Frequent interface up/down transitions. 2. Device Health – Monitors device operational status. 3. Certification Expiry – Notifies before certificates expire. 4. Password Expiry – Alerts for upcoming password expiration. 5. Fabric Health – Tracks network fabric status and integrity.

Table 2: Supported ONE OS features (continued)

Feature	Description
Simple Network Management Protocol (SNMP) Notifications	SNMP traps are alert messages sent from a remote SNMP-enabled device to a central collector, the SNMP Manager. Trap messages are the main form of communication between SNMP monitoring tools: • SNMP Agent • SNMP Manager XCO functions as the SNMP Manager for all EXTREME ONE OS devices and agents. Once a device is registered, XCO auto-configures it to send SNMP v3 traps. XCO receives traps from all devices in its inventory and acts as an SNMP proxy, forwarding SNMP v2 and v3 traps to an external trap receiver, if configured. Trap messages are the primary communication method between SNMP Agents and Managers, used to alert the SNMP Manager of events on remote devices.
Network Essentials: SNMP	XCO supports configuring the following SNMP components on EXTREME ONE OS devices: • SNMP Communities • SNMP Users • SNMP Host
SupportSave	The **efa system supportsave** script collects logs, database snapshots, pod logs, deployment details, and system support-save data. It compresses all collected information into a ZIP file for easy sharing with the Extreme support team during troubleshooting. The script captures: • Logs from XCO microservices • Host-level service logs • A snapshot of the database

Table 2: Supported ONE OS features (continued)

Feature	Description
Policy	
Compact Fabric Quality of Service (QoS) - Phase 1	XCO supports configuring QoS settings on Ethernet interfaces and Port Channels, including: • DSCP trust • PCP and DSCP ingress/egress maps Policy application is dynamic and adapts to the port role, whether part of a fabric, tenant, port channel, or tenant endpoint group.

Supported Platforms and Deployment Models for Fabric Skill

Support includes Server, Open Virtual Appliance (OVA), and TPVM deployment models, supported TPVM versions, supported SLX-OS software versions, and supported SLX devices.

Note

- OVA deployment model does not support HA.
- As a best practice, refer to the following Extreme validated support matrices for supported platforms and deployment models information.

Table 3: Server Deployment Models

XCO Version	Managed SLX Devices	Multi-Fabric Support	Ubuntu Server Version	Virtual Machine
3.4.x, 3.5.x, 3.6.x	More than 24	Yes	18.04 LTS and 20.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.7.x, 3.8.x	More than 24	Yes	20.04 LTS and 22.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
4.0.0	More than 24	Yes	20.04 LTS and 22.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB

Table 4: OVA Deployment Models

XCO Version	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Virtual Machine
3.4.x, 3.5.x, 3.6.x	More than 24	Yes	20.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.7.x, 3.8.x	More than 24	Yes	22.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
4.0.0	More than 24	Yes	22.04 LTS	• CPU: 4 cores • Storage: 64 GB

Table 4: OVA Deployment Models (continued)

XCO Version	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Virtual Machine
				• RAM: 8 GB

Table 5: TPVM Deployment Models

XCO Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum Network OS Version
3.4.x, 3.5.x, 3.6.x	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820 (20.4.3 and later)	Up to 24	Yes	20.04 LTS	SLX-OS 20.5.2a
3.7.x	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820 (20.4.3 and later)	Up to 24	Yes	22.04 LTS	SLX-OS 20.6.3a
3.8.x	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820 (20.4.3 and later)	Up to 24	Yes	22.04 LTS	SLX-OS 20.7.1

Table 5: TPVM Deployment Models (continued)

XCO Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum Network OS Version
4.0.0	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820 (20.4.3 and later)	Up to 24	Yes	22.04 LTS	SLX-OS 20.7.2
	• Extreme 8730 (ONE OS)	Up to 24	Yes	22.04 LTS	ONE OS 22.2.0.0

Table 6: TPVM Software Support

XCO Version	TPVM Version	Minimum Network OS Version
3.4.0	4.6.6	SLX-OS 20.5.3a
3.4.1	4.6.7	SLX-OS 20.5.3a
3.4.2	4.6.8	SLX-OS 20.5.3a
3.5.0	4.6.10	SLX-OS 20.6.1
3.6.0	4.6.13, 4.6.14	SLX-OS 20.6.2, SLX-OS 20.6.2a
3.7.0	4.6.17, 4.7.0	SLX-OS 20.6.3a
3.8.0	4.7.4	SLX-OS 20.7.1a
3.8.1	4.7.5	SLX-OS 20.7.1a
3.8.2	4.7.7	SLX-OS 20.7.1ab
4.0.0	4.7.7	SLX-OS 20.7.2, ONE OS 22.2.0.0

Table 7: IP Fabric Topology Matrix

Device	Minimum Network OS Release	Leaf	Spine	Super Spine	Border Leaf	Small DC Fabric
SLX 9150	SLX-OS 20.5.x, 20.6.x, and 20.7.x	Yes				Yes
SLX 9250	SLX-OS 20.5.x, 20.6.x, and 20.7.x	Yes	Yes	Yes		Yes
SLX 9540	SLX-OS 20.5.x, 20.6.x, and 20.7.x	Yes			Yes	

Table 7: IP Fabric Topology Matrix (continued)

Device	Minimum Network OS Release	Leaf	Spine	Super Spine	Border Leaf	Small DC Fabric
SLX 9640	SLX-OS 20.5.x, 20.6.x, and 20.7.x				Yes	
SLX 9740	SLX-OS 20.5.x, 20.6.x, and 20.7.x		Yes	Yes	Yes	Yes
Extreme 8720	SLX-OS 20.5.x, 20.6.x, and 20.7.x	Yes	Yes	Yes	Yes	Yes
Extreme 8520	SLX-OS 20.5.x, 20.6.x, and 20.7.x	Yes			Yes	Yes
Extreme 8820	SLX-OS 20.5.x, 20.6.x, and 20.7.x		Yes		Yes	Yes
Extreme 8730	ONE OS 22.2.0.0					Yes (2 Nodes)

XCO Upgrade Prerequisites

Prerequisites for XCO upgrade process with the default gateway changed:

1. Ensure that no DNS configuration exists under TPVM config and resolv.conf.
2. Presence of management connectivity from SLX and TPVM to external build server image, wherein image is available during SLX and TPVM upgrade process.

If file/etc/sshd/sshd_config is modified to non-default values, then manually readjust the following parameters:

- MaxStartups 30:30:100
- MaxAuthTries 6
- LoginGraceTime 120

Note
The hardening script, extr-granite.py bundled with EFA 2.6.1 will not automatically modify the above mentioned parameters.

Closed Defects

The following defects are closed in this release of the software.

Issue ID	Description
XCO-13057	"Sync comparison error" is displayed while checking HTTPS certificate on EFA.
XCO-13158	'efa system supportsave --fabric-name' command occasionally produces unexpected output.
XCO-13101	System displays inconsistent error messages for the 'efa inventory device setting update' command when using the crypto-cert-expiry and password-expiry flags.
XCO-13217	Sensitive information stored in plain text in the logs.
XCO-12967	The "http status: 401 Unauthorized" error is displayed when running XCO commands.
XCO-13161	A delay is experienced while deleting ipv6 prefix-list.
XCO-12981	The certificate import fails during device registration.
XCO-10574	XCO CLI incorrectly displays "Devices x.x.x.x are going through firmware download" due to an uncleared flag.
XCO-11734	XCO Health Status is "Yellow".

Open Defects

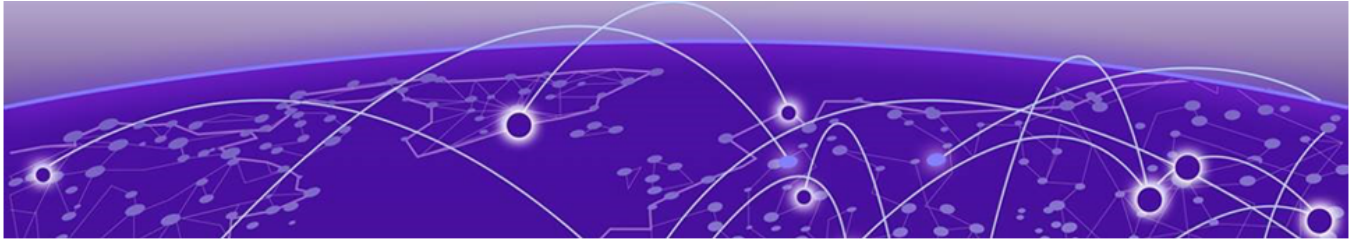
The following defects are open in this release of the software.

Issue ID	Description	
XCO-14407	Tenant service experiences multiple restarts during execution of the CNIS test case: Efa Data Consistency Double Fault Device.	
XCO-10929	XCO takes approximately 45 minutes to complete DRC and transition the node out of MM following an SLX reload.	

Security Patch

The following table lists the updated security components and vulnerabilities addressed in ExtremeCloud Orchestrator 4.0.0.

Component	Previous Version	Latest Version	Vulnerabilities
Others	NA	NA	• CVE-2025-4517 • CVE-2025-4138 • CVE-2025-4330 • CVE-2025-4435 • CVE-2024-12718 • CVE-2025-23166 • CVE-2025-4947 • CVE-2025-5025 • CVE-2025-23165 • CVE-2025-46712 • CVE-2025-4516



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.