ExtremeCloud™ Orchestrator v4.1.0 Release Notes

New Features, Supported Platforms, and Known Issues

9041115-00 Rev AA
September 2026

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

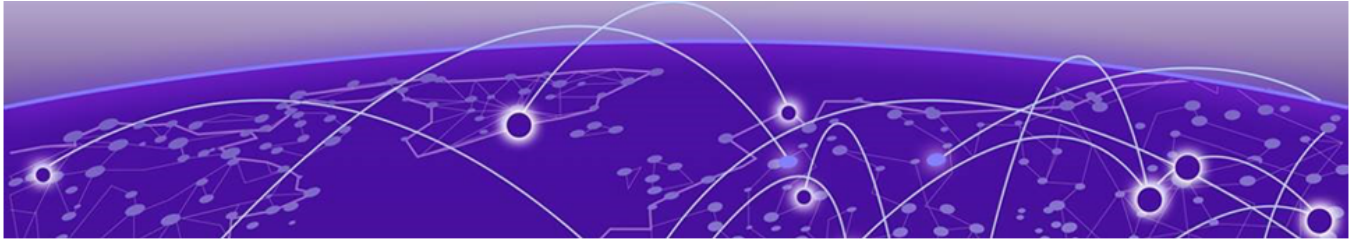
Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

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/



Abstract

ExtremeCloud™ Orchestrator v4.1.0 Release Notes supports lifecycle management capabilities, supporting advanced fabric provisioning, multi-tenant networking, and automation features. This release delivers new features and enhancements and resolves issues through defect fixes.

Release Notes

New In This Release

ExtremeCloud Orchestrator 4.1.0 includes the following features and enhancements and resolves issues through defect fixes.

Note

- XCO 4.1.0 release supports fresh installations only.
- The features related to XCO-OS ONE and Extreme 8730 support in XCO 4.1.0 are released as Control Released Features.
- For comprehensive XCO-OS ONE feature descriptions, CLI command references, administrative procedures, and API documentation, contact Extreme Networks.

Table 1: Features and Enhancements

Feature	Description
Infra Enhancements	Includes cross-cutting hardening, CVE remediation, and operational enhancements including Go version upgrades, base image internalization, file permission hardening, Kubernetes node failover fixes, and support utility improvements.
Inter-AS Support	Uses MPLS L3VPN to extend Layer 3 connectivity between an XCO-managed fabric and external gateways. By leveraging a shared BGP VPNv4/VPNv6 session, it enables the exchange of routes for many tenant VRFs over a single scalable control-plane connection rather than maintaining individual BGP sessions for each VRF.
Certificate Management Enhancements	Automates certificate enrollment, provisioning, and renewal using CMPv2 protocol. Supports third party certificates for RELP client.

Table 1: Features and Enhancements (continued)

Feature	Description
Multiple IP Address Related Enhancements	Tracks multiple IPs per interface separately from device-reported IPs. Automatically reconciles and removes stale IPs during config pushes, preventing duplicate BGP sessions and fabric health degradation from cable swaps and link flaps.
Fabric Health Enhancements	Addresses identified gaps in fabric health management
Software BFD Session Control	Enables fabric-wide policy to run BFD sessions in software on underlay L3 ports for Jericho2-based platforms (SLX 9740, Extreme 8820), achieving failover in seconds when control plane freezes.
Secure Service Credentials	Replaces all Base64-encoded and static credentials with encrypted secrets, OTP, time-limited tokens, or derived keys. Implements automatic credential rotation and secure loading without persistent plain text storage.

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 2: 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

Table 2: Server Deployment Models (continued)

XCO Version	Managed SLX Devices	Multi-Fabric Support	Ubuntu Server Version	Virtual Machine
4.0.2	More than 24	Yes	22.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
4.1.0	More than 24	Yes	22.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB

Table 3: 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.x	More than 24	Yes	22.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
4.1.0	More than 24	Yes	22.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB

Table 4: 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 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820	Up to 24	Yes	20.04 LTS	SLX-OS 20.5.2a
3.7.x	• SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820	Up to 24	Yes	22.04 LTS	SLX-OS 20.6.3a

Table 4: TPVM Deployment Models (continued)

XCO Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum Network OS Version
3.8.x	• 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
4.0.2	• SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820	Up to 24	Yes	22.04 LTS	SLX-OS 20.7.3a
	• Extreme 8730, Extreme 8720 (OS ONE)	Up to 24	Yes	22.04 LTS	Controlled Release. Contact Extreme Networks
4.1.0	• SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820	Up to 24	Yes	22.04 LTS	SLX-OS 20.8.2
	Extreme 8730, Extreme 8720	Up to 24	Yes	22.04 LTS	Controlled Release. Contact Extreme Networks

Table 5: 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
3.8.3	4.7.8	SLX-OS 20.7.1.ab
3.8.4	4.7.10	SLX-OS 20.7.2ab
3.8.5	4.7.12	SLX-OS 20.7.3a

Table 5: TPVM Software Support (continued)

XCO Version	TPVM Version	Minimum Network OS Version
3.8.6	4.7.13	SLX-OS 20.7.3a
3.8.7	4.7.14	SLX-OS 20.7.3a
3.8.8	4.7.15	SLX-OS 20.7.3ab
4.0.2	4.7.15	SLX-OS 20.8.1
4.1.0	4.7.19, 4.7.20	SLX-OS 20.8.2

Table 6: IP Fabric Topology Matrix

Device	SLX-OS/OS ONE Release	Leaf	Spine	Super Spine	Border Leaf	Small DC Fabric
SLX 9540	SLX-OS 20.6.x, 20.7.x, and 20.8.x	Yes	-	-	Yes	-
SLX 9640	SLX-OS 20.6.x, 20.7.x, and 20.8.x	-	-	-	Yes	-
SLX 9740	SLX-OS 20.6.x, 20.7.x, and 20.8.x	-	Yes	Yes	Yes	Yes
Extreme 8720	SLX-OS 20.6.x, 20.7.x, and 20.8.x	Yes	Yes	Yes	Yes	Yes
Extreme 8520	SLX-OS 20.6.x, 20.7.x, and 20.8.x	Yes	-	-	Yes	Yes
Extreme 8820	SLX-OS 20.6.x, 20.7.x, and 20.8.x	Yes	Yes	-	Yes	Yes
Extreme 8730, Extreme 8720	Controlled Release. Contact Extreme Networks	-	-	-	-	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

Resolved Issues

The following issues are resolved in this release of the software.

Issue ID	Description
XCO-19768	BFD static route delete/add failure (XCO 4.0.2)
XCO-19441	Duplicate "MigrationComplete" entries cause upgrade failure (3.8.5→4.0.2)
XCO-18771	Stale NFS file handle error in EFA command outputs
XCO-18722	XCO deployment fails during MariaDB installation
XCO-18664	Threshold-monitor output formatting regression (XCO 4.0.2)
XCO-18367	EFA enters cfg-refreshed state post-installation
XCO-18355	EFA SDI upgrade fails from 3.11.3→3.12 and 3.8.8→4.0.2
XCO-18276	Drifted virtual equipment with config refresh error
XCO-18199	Rollback fails during inventory DB migration (4.0.2→3.8.6)
XCO-18148	BGP peer-group creation fails with service unavailability error
XCO-18091	EPG creation fails due to ClientID allocation conflict
XCO-18050	Fabric device upgrade fails with device not prepared under fabric error
XCO-17814	EFA fabric health degrades after leaf device reload
XCO-17800	BGP process failure causes EFA crash and traffic loss
XCO-17747	EVPN IRB virtual equipment drift after scaling config in non-CLOS
XCO-17677	EFA upgrade takes significantly longer than expected
XCO-17402	Devices stuck in firmware download state
XCO-17357	EFA status returns empty after corrupt image upgrade failure
XCO-17340	BFD neighbor configuration not applied on SLX after fabric setting update
XCO-17339	EFA fabric creation fails due to unhealthy fabric
XCO-17231	SQL injection vulnerability in XCO API
XCO-17213	Credentials leaked in XCO logs
XCO-16738	EFA upgrade takes significantly longer than expected
XCO-16569	EFA health shows red/black due to duplicate DRC entries
XCO-16017	Backup restore hangs on EFA fabric show (3.50→3.8.2)
XCO-15837	Fabric nodes enter cfg-refreshed state (EFA 3.2.1)
XCO-15247	Binding policy errors with redundant-management configuration

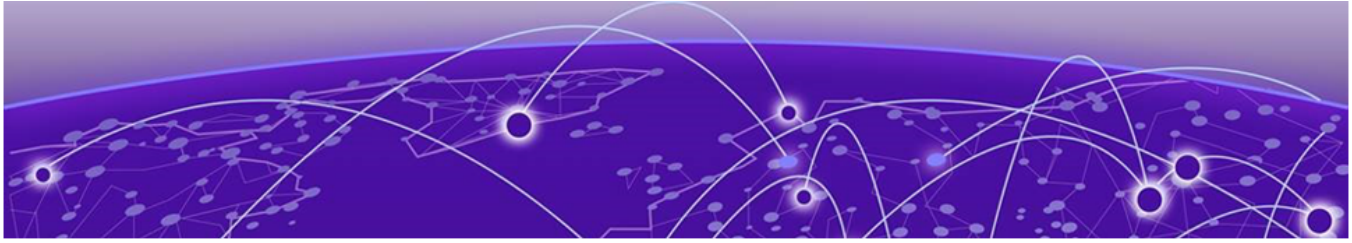
Issue ID	Description
XCO-15148	Admin state up fails on compute leaf (XCO 4.0.1)
XCO-15063	RabbitMQ issues during tenant config provisioning/unprovisioning
XCO-14867	Fabric nodes move to default fabric after backup/restore
XCO-14685	Upgrade fails due to module manager disable timeout
XCO-14643	SLX-OS upgrade stuck at Device Reload Completed
XCO-14259	BIN_DIR variable not set in server deployments
XCO-14235	EFA fabric error with QoS trust DSCP configuration
XCO-14184	EFA shows SLXOS update state as failed
XCO-14161	BL switches stuck in cfg-refreshed state due to BGP
XCO-14143	max-password-age update instructions updated in documentation
XCO-14099	Security banner not displayed correctly after TPVM upgrade from 4.7.3
XCO-13965	EFA security banner fails to handle '%' character
XCO-13964	Security banner is not displayed for non-extreme users during EFA CLI access
XCO-13914	EFA configuration missing on last SLX after restore
XCO-13841	gosnmp-service crashes after active-to-standby failover
XCO-13700	Certificate copy fails from active to standby TPVM
XCO-13326	Interfaces unexpectedly bind to unbound QoS profiles
XCO-12891	SLX-OS 20.7.1 upgrade causes standby TPVM failure
XCO-11638	EFA commands experience abnormal execution delays

Open Issues

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

Issue ID	Description
XCO-20319	**Reported in Release** XCO 4.1.0 **Symptom** A multi-node upgrade from XCO 4.0.x to 4.1.0 fails during the Installing k3s container orchestration phase with the error: "`Cannot enable cgroup controller 'cpuset' in subtree_control. This will prevent k3s from starting.`" The installer then rolls back the partial installation. **Condition** When the upgrade is initiated from the standby TPVM node, the attempt to enable the cpuset cgroup controller fails with an `EINVAL` error due to an unsupported cgroup v2 hierarchy configuration. **Workaround:** Run the efa deployment commands from the SLX device hosting the active TPVM node.
XCO-20278	**Reported in Release** XCO 4.1.0 **Symptom** When a port-channel (PO)-level QoS profile is unbound, the operation may report a partial failure with the error "`%Error: Map does not Exist.`" The underlying tenant-level QoS profile may temporarily appear in a `cfg-refreshed` state until the configuration is restored. **Condition** This issue occurs when a tenant-level QoS profile is overridden by a different PO-level QoS profile that uses a different QoS map and the PO includes all tenant-bound interfaces on the device. **Workaround:** Ensure that at least one tenant-bound port or port-channel remains outside the PO associated with the higher-priority QoS profile. **Recovery** No manual intervention is required. The system automatically recovers within approximately 5 minutes and restores the tenant-level QoS configuration, returning the profile binding from `cfg-refreshed` to `cfg-in-sync`. If faster recovery is required, manually trigger a Draft Reconciliation (DRC).

Issue ID	Description
XCO-19901	**Reported in Release** XCO 4.1.0 **Symptom** The CMPv2 Status page incorrectly displays `Auto Renew` as `true` after auto-renew is disabled using the `efa certificate cmpv2 apply --auto-renew false` command. **Condition** This issue occurs after disabling CMPv2 auto-renewal with the `efa certificate cmpv2 apply --auto-renew false` command and then checking the status using `efa certificate cmpv2 status`. **Workaround:** This issue was resolved in XCO 4.2.0. Upgrade to the next release to obtain the fix.
XCO-19832	**Reported in Release** XCO 4.1.0 **Symptom** After an XCO upgrade or restart, the Fabric application state temporarily changes from `cfg-sync` to `cfg-refresh`. The issue resolves automatically without traffic loss. **Condition** This issue occurs after upgrading or restarting XCO, including upgrades from 4.0.2 to 4.1.0 and 3.8.x to 4.0.2. **Recovery** The issue resolves automatically within approximately 5 minutes in large fabrics (more than 15 devices), with no traffic impact.
XCO-19624	**Reported in Release** XCO 4.1.0 **Symptom** Dual-homed Port-Channel creation intermittently fails due to a race condition during DRC. **Condition** This issue can occur under the following conditions: 1. A non-Clos fabric is deployed and reports a healthy state. 2. Both MCT peer devices are reset to their default configuration. 3. A Drift Reconciliation (DRC) is triggered on one of the devices. 4. During DRC processing, Inventory generates `inv.Mct_cluster` add or update events. 5. The Tenant service does not process these events, preventing MCT cluster information from being added to the Tenant database. 6. This issue does not occur consistently. As a result, dual-homed port-channel creation fails. **Recovery:** Remove and re-add the affected device to the fabric.



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.