



ExtremeCloud™ Orchestrator v4.0.5 Release Notes

Resolved and Open Issues

9039317-04 Rev AA
August 2026



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

Legal Notice

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

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

Trademarks

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

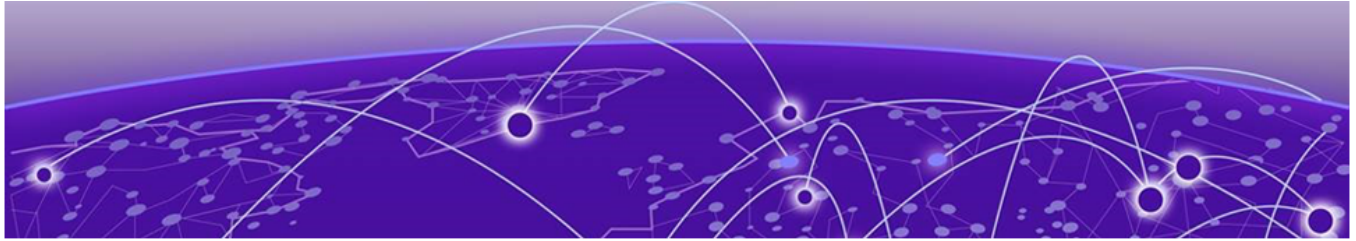
All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

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

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses.

End-user license agreements and open source declarations can be found at: <https://www.extremenetworks.com/support/policies/open-source-declaration/>



Abstract

ExtremeCloud™ Orchestrator v4.0.5 Release Notes supports lifecycle management capabilities, supporting advanced fabric provisioning, multi-tenant networking, and automation features. This release includes critical security patches.



Release Notes

[New In This Release](#) on page 4

[XCO Extreme OS ONE Integration](#) on page 4

[Supported Platforms and Deployment Models for Fabric Skill](#) on page 5

[XCO Upgrade Prerequisites](#) on page 8

[Resolved Issues](#) on page 9

[Open Issues](#) on page 9

[Security Patch](#) on page 9

New In This Release

ExtremeCloud Orchestrator 4.0.5 resolves issues through critical security patches.



Note

- In release 4.0.2, the "ID" field in the Request Body for the RegisterTrapSubscriber REST API is read-only. When registering a Trap Subscriber using REST API, the "ID" field must not be included in the request body. This change does not affect Trap Subscriber registration using CLI.

For more information, see [Security Patch](#) on page 9.

XCO Extreme OS ONE Integration

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



Note

- The features related to XCO OS ONE and Extreme 8730 support in XCO 4.0.x are released as Control Released Features.
- For testing the XCO OS ONE features, and for comprehensive feature descriptions, CLI command references, administrative procedures, and API documentation, contact Extreme Networks.

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

Table 2: 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

Table 2: OVA Deployment Models (continued)

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

Table 3: 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	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	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
4.0.2	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820	Up to 24	Yes	22.04 LTS	SLX-OS 20.7.3a
	OS ONE • Extreme 8730	Up to 24	Yes	22.04 LTS	Controlled Release. Contact Extreme Networks.

Table 3: TPVM Deployment Models (continued)

XCO Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum Network OS Version
4.0.3, 4.0.4, 4.0.5	- SLX 9150 - SLX 9250 - SLX 9740 - Extreme 8520 - Extreme 8720 - Extreme 8820	Up to 24	Yes	22.04 LTS	SLX-OS 20.8.1a
	OS ONE Extreme 8730	Up to 24	Yes	22.04 LTS	Controlled Release. Contact Extreme Networks.

Table 4: 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
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
4.0.3	4.7.17	SLX-OS 20.8.1a

Table 4: TPVM Software Support (continued)

XCO Version	TPVM Version	Minimum Network OS Version
4.0.4	4.7.18	SLX-OS 20.8.1a
4.0.5	4.7.19	SLX-OS 20.8.1a

Table 5: IP Fabric Topology Matrix

Device	SLX-OS/OS ONE Release	Leaf	Spine	Super Spine	Border Leaf	Small DC Fabric
SLX 9150	SLX-OS 20.6.x, 20.7.x, and 20.8.x	Yes	-	-	-	Yes
SLX 9250	SLX-OS 20.6.x, 20.7.x, and 20.8.x	Yes	Yes	Yes	-	Yes
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	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

**Note**

- The hardening script, `extr-granite.py` bundled with EFA 2.6.1 will not automatically modify the above mentioned parameters.
- Direct upgrade from XCO 4.0.0 to 4.0.5 and later is not supported. Contact Extreme Networks for support.
- XCO 4.0.5 defaults to full upgrade mode due to host package updates. No additional parameters, such as `force-full-upgrade`, are required to perform a full upgrade.

Resolved Issues

The following issue is resolved with code in this release of the software.

Issue ID	Description
XCO-19576	XCO GUI Displays "MUI X Invalid License Key" Error on Services pages after upgrading to XCO 4.0.4.

Open Issues

Unless explicitly closed in this release, previously reported open defects remain open.

Security Patch

The following table lists the updated security components and vulnerabilities addressed in this release.

Component	CVE
K3S Services	CVE-2025-47913
	CVE-2025-47914
	CVE-2025-58181
	CVE-2025-68121
	CVE-2026-24051
	CVE-2026-25679
	CVE-2026-27139
	CVE-2026-27142
	CVE-2026-32280
	CVE-2026-32281
	CVE-2026-32282
	CVE-2026-32283
	CVE-2026-32288
	CVE-2026-32289
	CVE-2026-33186
	CVE-2026-33811
	CVE-2026-39820
	CVE-2026-39823
	CVE-2026-39825
	CVE-2026-39826
	CVE-2026-39827
	CVE-2026-39828
	CVE-2026-39829
	CVE-2026-39830
	CVE-2026-39831
	CVE-2026-39832
	CVE-2026-39833
	CVE-2026-39834
	CVE-2026-39835
	CVE-2026-39836
	CVE-2026-39883
	CVE-2026-40179
	CVE-2026-42151
	CVE-2026-42154
	CVE-2026-42499
	CVE-2026-42508
	CVE-2026-44903
	CVE-2026-46595
	CVE-2026-46597
	CVE-2026-46598
	CVE-2026-54761
	CVE-2026-54762
	CVE-2026-54763

Component	CVE
	CVE-2026-54764 CVE-2026-54765 GHSA-3G6V-2R68-PRFC GHSA-45GG-VH54-H5M9 GHSA-4MR2-FC2P-W63C GHSA-5CGQ-3RG8-M6CV GHSA-5CV4-JP36-H3MW GHSA-78MQ-XCR3-XM33 GHSA-89GR-R52H-F8RX GHSA-8RM2-7QQF-34QM GHSA-9H8M-3FM2-QJRQ GHSA-9M57-25V3-79X9 GHSA-F5WC-C3C7-36MC GHSA-FW8G-CG8F-9J28 GHSA-HFVC-G4FC-PQHX GHSA-JPPX-RXC9-JMRX GHSA-P77J-4MVH-X3M3 GHSA-Q4H4-GMJ2-QVW2 GHSA-QPW4-5X99-6VJP GHSA-RM3J-F69W-WQMQ GHSA-VFFH-X6R8-XX99 GHSA-VCWF-H737-FF37 GHSA-W879-237Q-WC7R GHSA-WG65-39GG-5WFJ GHSA-X527-X647-Q7GG GO-2026-4337 GO-2026-4601 GO-2026-4602 GO-2026-4603 GO-2026-4865 GO-2026-4870 GO-2026-4946 GO-2026-4947 GO-2026-4971 GO-2026-4977 GO-2026-4980 GO-2026-4981 GO-2026-4982 GO-2026-4986
Containers	CVE-2026-50219 CVE-2026-53422 CVE-2026-54886 CVE-2026-54887 CVE-2026-54891

Component	CVE
	CVE-2026-55950 CVE-2026-55952 CVE-2026-56131 CVE-2026-56132 CVE-2026-56403 CVE-2026-56404 CVE-2026-56405 CVE-2026-56406 CVE-2026-56407 CVE-2026-56408 CVE-2026-56409 CVE-2026-56410 CVE-2026-56411 CVE-2026-56412
Host Packages	CVE-2026-10879 CVE-2026-32286 CVE-2026-34743 CVE-2026-39822 CVE-2026-40467 CVE-2026-40468 CVE-2026-40469 CVE-2026-40553 CVE-2026-41889 CVE-2026-42496 CVE-2026-42505 CVE-2026-46600 CVE-2026-56852 CVE-2026-8376 CVE-2026-9698 GHSA-J88V-2CHJ-QFWX GHSA-JQCQ-XJH3-6G23 GO-2026-5856



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.