



ExtremeCloud™ Orchestrator v4.1.1 Release Notes

New Features, Supported Platforms, and Known Issues

9041115-01 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

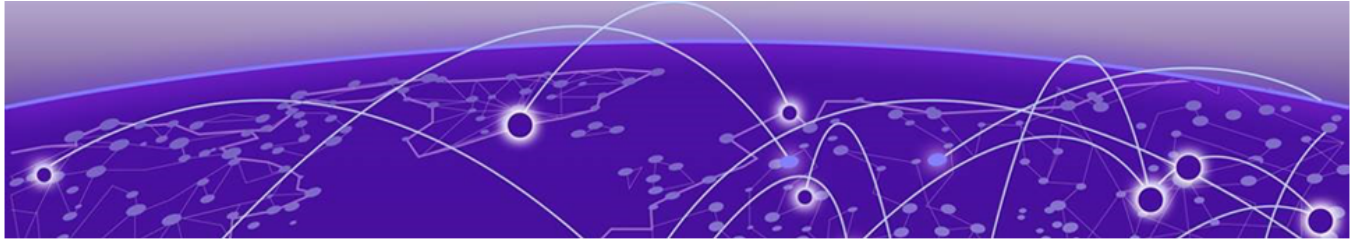
Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

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>

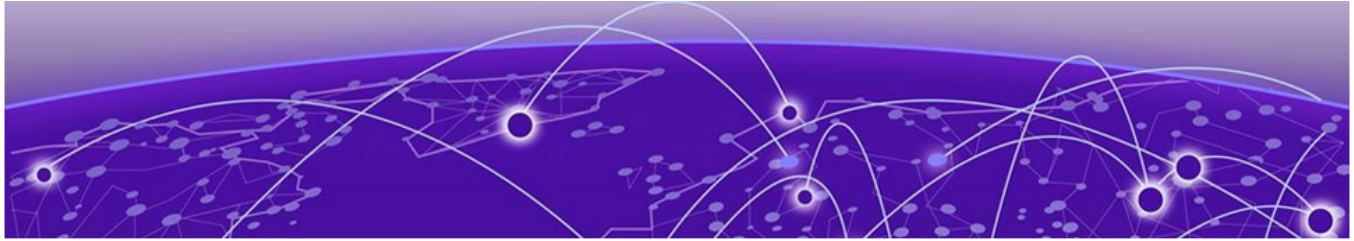
Open Source Declarations

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/>



Abstract

ExtremeCloud™ Orchestrator v4.1.1 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

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

[XCO Upgrade Prerequisites](#) on page 7

[Security Patch](#) on page 8

New In This Release

ExtremeCloud Orchestrator 4.1.1 resolves issues through critical security patches.



Note

- In OS ONE environments, XCO 4.1.1 supports fresh installations only. Upgrades from previous versions are not supported.
- The features related to XCO-OS ONE and Extreme 8730 support in XCO 4.1.1 are released as Control Released Features.
- For comprehensive XCO-OS ONE 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
3.7.x, 3.8.x	More than 24	Yes	20.04 LTS and 22.04 LTS	<ul style="list-style-type: none"> • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
4.x.x	More than 24	Yes	22.04 LTS	<ul style="list-style-type: none"> • 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
3.7.x, 3.8.x, 4.x.x	More than 24	Yes	22.04 LTS	<ul style="list-style-type: none"> • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB

Table 3: TPVM Deployment Models

XCO Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum Network OS Version
3.7.x	<ul style="list-style-type: none"> • SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820 	Up to 24	Yes	22.04 LTS	SLX-OS 20.6.3a
3.8.x	<ul style="list-style-type: none"> • 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 3: TPVM Deployment Models (continued)

XCO Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum Network OS Version
4.0.2	<ul style="list-style-type: none"> SLX 9740 Extreme 8520 Extreme 8720 Extreme 8820 	Up to 24	Yes	22.04 LTS	SLX-OS 20.7.3a
	OS ONE: <ul style="list-style-type: none"> Extreme 8730 Extreme 8720 	Up to 24	Yes	22.04 LTS	Controlled Release. Contact Extreme Networks.
4.0.3, 4.0.4, 4.0.5	<ul style="list-style-type: none"> SLX 9740 Extreme 8520 Extreme 8720 Extreme 8820 	Up to 24	Yes	22.04 LTS	SLX-OS 20.8.1a
	OS ONE: <ul style="list-style-type: none"> Extreme 8730 Extreme 8720 	Up to 24	Yes	22.04 LTS	Controlled Release. Contact Extreme Networks.
4.1.0, 4.1.1	<ul style="list-style-type: none"> SLX 9740 Extreme 8520 Extreme 8720 Extreme 8820 	Up to 24	Yes	22.04 LTS	SLX-OS 20.8.2
	OS ONE: <ul style="list-style-type: none"> Extreme 8730 Extreme 8720 	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
3.7.0	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

Table 4: TPVM Software Support (continued)

XCO Version	TPVM Version	Minimum Network OS Version
4.0.2	4.7.15	SLX-OS 20.8.1
4.0.3	4.7.17	SLX-OS 20.8.1a
4.0.4	4.7.18	SLX-OS 20.8.1a
4.0.5	4.7.19	SLX-OS 20.8.1a
4.1.0	4.7.19, 4.7.20	SLX-OS 20.8.2
4.1.1	4.7.21	SLX-OS 20.8.2

Table 5: IP Fabric Topology Matrix

Device	SLX-OS/OS ONE Release	Leaf	Spine	Super Spine	Border Leaf	Small DC Fabric
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:

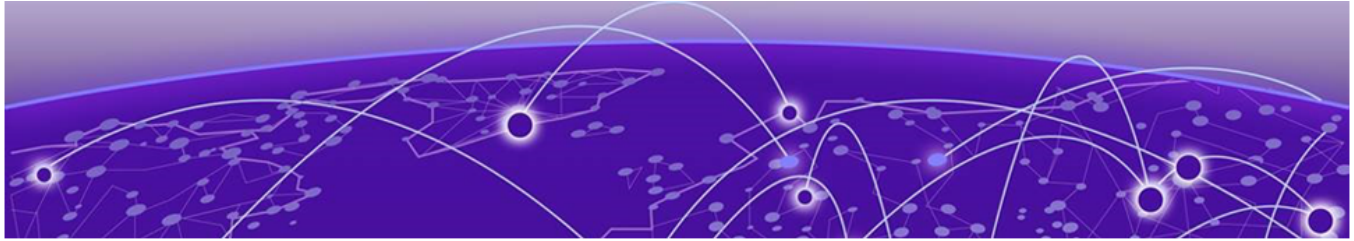
- MaxStartups 30:30:100
- MaxAuthTries 6
- LoginGraceTime 120

Security Patch

Component	Vulnerabilities
K3S Services	CVE-2025-47911 CVE-2025-58190 CVE-2026-25680 CVE-2026-25681 CVE-2026-27136 CVE-2026-27145 CVE-2026-33814 CVE-2026-34180 CVE-2026-34181 CVE-2026-34182 CVE-2026-34183 CVE-2026-39824 CVE-2026-42502 CVE-2026-42504 CVE-2026-42506 CVE-2026-42507 CVE-2026-42764 CVE-2026-42766 CVE-2026-42767 CVE-2026-42768 CVE-2026-42769 CVE-2026-42770 CVE-2026-45445 CVE-2026-45446 CVE-2026-45447 CVE-2026-71324 CVE-2026-71325 CVE-2026-71326 CVE-2026-71327 CVE-2026-7383 CVE-2026-85594 CVE-2026-85595 CVE-2026-85596 CVE-2026-85597 CVE-2026-88004 CVE-2026-88007 CVE-2026-88008 CVE-2026-88009 CVE-2026-88011 CVE-2026-88012 CVE-2026-88877

Component	Vulnerabilities
	CVE-2026-88878 CVE-2026-88879 CVE-2026-9076 GHSA-3CCP-42PG-HGV6 GHSA-62FC-8686-HFMQ GHSA-6765-C87H-8MRF GHSA-7GHQ-V6JF-G56C GHSA-F52W-8J3H-J724 GHSA-FGJJ-PX3W-67XX GHSA-QQJF-53CJ-PWVV GHSA-RF44-J88R-HH8C GHSA-V67P-PHPQ-FC8X GHSA-W4V4-9RW7-5326 GO-2026-4918 GO-2026-5037 GO-2026-5038 GO-2026-5039
Containers	CVE-2026-13608 CVE-2026-18924 CVE-2026-19931 CVE-2026-55951 CVE-2026-59696 CVE-2026-66046 CVE-2026-66357 CVE-2026-66835 CVE-2026-69664 CVE-2026-70399 CVE-2026-70405 CVE-2026-70409 CVE-2026-71380 CVE-2026-71562 CVE-2026-73270 CVE-2026-73276 CVE-2026-73812 CVE-2026-74835 CVE-2026-74994 CVE-2026-75538 CVE-2026-76641 CVE-2026-76956 CVE-2026-76957 CVE-2026-80229 CVE-2026-80230 CVE-2026-80231 CVE-2026-80255

Component	Vulnerabilities
	CVE-2026-80256 CVE-2026-82208 CVE-2026-82209 CVE-2026-89156 CVE-2026-89157 CVE-2026-89158 CVE-2026-89160 CVE-2026-89161 CVE-2026-89162
Host Packages	CVE-2026-12087 CVE-2026-13221 CVE-2026-13595 CVE-2026-15534 CVE-2026-19487 CVE-2026-19546 CVE-2026-19654 CVE-2026-27456 CVE-2026-53613 CVE-2026-53615 CVE-2026-57432 CVE-2026-57433 CVE-2026-61548



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.