ExtremeCloud™ Orchestrator v3.7.1 Release Notes

New Features, Supported Platforms, and Known Issues

9039078-01 Rev AA
March 2024

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/

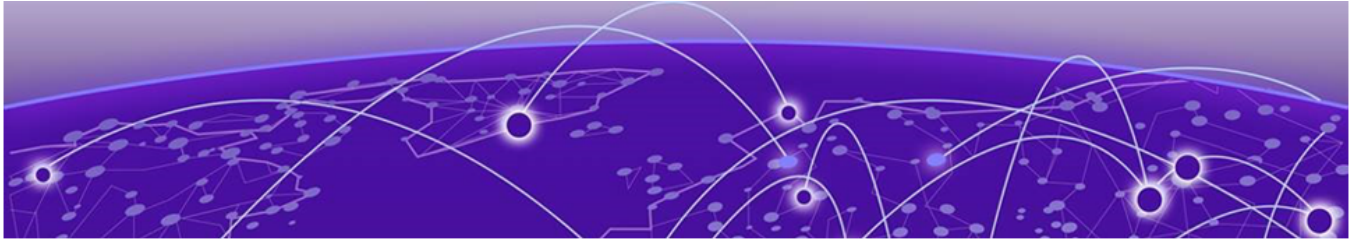
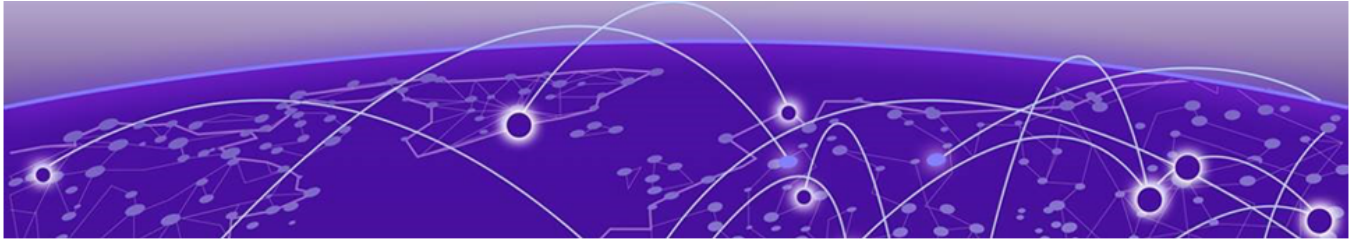
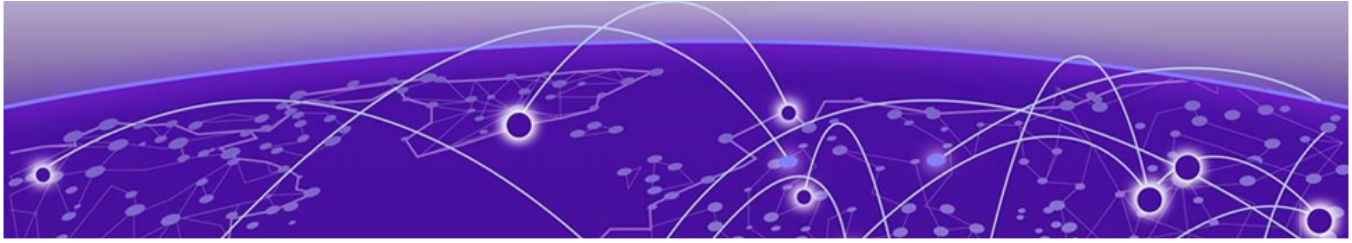


Table of Contents



Abstract

ExtremeCloud Orchestrator version 3.7.1 is a security patch release that includes updates to several components to address multiple vulnerabilities. Supported deployment models for fabric and visibility skills include server, Open Virtual Appliance (OVA), and TPVM across various versions. The document outlines upgrade prerequisites, such as ensuring no DNS configuration exists under TPVM config and resolv.conf, and maintaining management connectivity from SLX and TPVM to the external build server image during the upgrade process. Defects were closed with code changes, and there are no open defects in this release.



Release Notes

New In This Release

ExtremeCloud Orchestrator 3.7.1 is a security patch release. For information about XCO deployment, refer to the *ExtremeCloud Orchestrator Deployment Guide, 3.7.0*.

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.

For other additional information, see Security Patch on page 15 and Defects Closed with Code Changes on page 13.

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 support 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	More than 24	Yes	18.04 LTS and 20.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.5.x	More than 24	Yes	18.04 LTS and 20.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.6.x	More than 24	Yes	18.04 LTS, 20.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.7.x	More than 24	Yes	20.04 LTS and 22.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
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: OVA Deployment Models

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

Table 2: OVA Deployment Models (continued)

XCO Version	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Virtual Machine
3.6.x	More than 24	Yes	20.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.7.x	More than 24	Yes	22.04 LTS	• 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 SLX-OS Version
3.4.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	20.5.2a
3.5.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	20.5.2a

Table 3: TPVM Deployment Models (continued)

XCO Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum SLX-OS Version
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	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	20.6.3a

Table 4: TPVM Software Support

XCO Version	TPVM Version	SLX-OS Version
3.4.0	4.6.6	20.5.3a
3.4.1	4.6.7	20.5.3a
3.4.2	4.6.8	20.5.3a
3.5.0	4.6.10	20.6.1
3.6.0	4.6.13, 4.6.14	20.6.2, 20.6.2a
3.7.0	4.6.17, 4.7.0	20.6.3a
3.7.1	4.6.19, 4.7.2	20.6.3a

Table 5: IP Fabric Topology Matrix

Device	SLX-OS Release	Extreme ONE OS Release	Leaf	Spine	Super Spine	Border Leaf	Small DC Fabric
SLX 9150	20.2.x, 20.3.x, 20.4.x		Yes				Yes
SLX 9250	20.2.x, 20.3.x, 20.4.x		Yes	Yes	Yes		Yes
SLX 9540	20.2.x, 20.3.x, 20.4.x		Yes			Yes	

Table 5: IP Fabric Topology Matrix (continued)

Device	SLX-OS Release	Extreme ONE OS Release	Leaf	Spine	Super Spine	Border Leaf	Small DC Fabric
SLX 9640	20.2.x, 20.3.x, 20.4.x					Yes	
SLX 9740	20.2.x, 20.3.x, 20.4.x			Yes	Yes	Yes	Yes
Extreme 8720	20.3.x, 20.4.x		Yes	Yes	Yes	Yes	Yes
Extreme 8520	20.3.x, 20.4.x		Yes			Yes	Yes
Extreme 8820	20.4.3			Yes		Yes	Yes

Supported Platforms and Deployment Models for Visibility Skill

Support includes Server, OVA, and supported devices and software.

Note

- Upgrade from XVM (Extreme Visibility Manager) to XCO is not supported.
- XCO supports only a fixed set of special characters for hostnames. Any additional characters configured in MLX or SLX are reconciled in XCO and can be edited or deleted. Any configuration name must start with an alphanumeric character and can contain a-z A-Z 0-9 _ -.

Table 6: Ubuntu Server Version

XCO Version	Ubuntu Version	Virtual Machine
3.4.x	18.04 LTS and 20.04 LTS	Minimum: • CPU: 4 cores • Storage: 128 GB • RAM: 8 GB Recommended: • CPU: 16 cores • Storage: 200 GB • RAM: 32 GB
3.5.x	18.04 LTS and 20.04 LTS	Minimum: • CPU: 4 cores • Storage: 128 GB • RAM: 8 GB Recommended: • CPU: 16 cores • Storage: 200 GB • RAM: 32 GB

Table 6: Ubuntu Server Version (continued)

XCO Version	Ubuntu Version	Virtual Machine
3.6.x	18.04 LTS, 20.04 LTS	Minimum: • CPU: 4 cores • Storage: 128 GB • RAM: 8 GB Recommended: • CPU: 16 cores • Storage: 200 GB • RAM: 32 GB
3.7.x	20.04 LTS, 22.04 LTS	Minimum: • CPU: 4 cores • Storage: 128 GB • RAM: 8 GB Recommended: • CPU: 16 cores • Storage: 200 GB • RAM: 32 GB

Table 7: OVA Deployment Models

XCO Version	Ubuntu Version	Virtual Machine
3.4.x	20.04 LTS	Minimum: • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.5.x	20.04 LTS	Minimum: • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB

Table 7: OVA Deployment Models (continued)

XCO Version	Ubuntu Version	Virtual Machine
3.6.x	20.04 LTS	Minimum: • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.7.x	22.04 LTS	Minimum: • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB

Table 8: Supported Devices and Software

Device	Supported Software
Extreme 9920	Extreme 9920 software with the NPB application • 21.1.2.x • 21.2.1.x • 21.2.2.x
Extreme Routing MLX Series	• NetIron 6.3.00 patches
Extreme Switching SLX 9140	• SLX-OS 18s.1.03 patches
Extreme Switching SLX 9240	• SLX-OS 18s.1.03 patches

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.

Defects Closed with Code Changes

The following defects were closed with code changes in ExtremeCloud Orchestrator 3.7.1.

Parent Defect ID:	XCO-11647		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.8.0
Symptom:	The existing rabbitmq:3.8.0 (alpine 3.20.3) has known security vulnerabilities and hence need to change this combination to the latest recommended release.		
Condition:	These problems exist in the earlier package combination and they are resolved in the latest recommended package combination rabbitmq:3.7.1 (alpine 3.21.3).		

Parent Defect ID:	XCO-11940		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.8.0
Symptom:	Alpine container version 3.18.6 used with traefik package is old and with some known security vulnerabilities. Need to upgrade the alpine base image to the latest release.		
Condition:	These problems exist in alpine container 3.18.6. These issues are resolved in latest alpine container 3.21.2.		

Parent Defect ID:	XCO-11941		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.8.0
Symptom:	The libraries used in existing traefik package version 2.10.7 have some known security vulnerabilities and it could possibly cause issues in customer deployment. Need to upgrade the package to the latest release.		
Condition:	These issues exist in traefik version 2.10.7 and they are resolved in latest version 2.11.18 of traefik package.		

Parent Defect ID:	XCO-11942		
	XCO Fabric Skill	Reported in Release:	XCO 3.8.0

Parent Defect ID:	XCO-11942		
Product:			
Symptom:	The go version and libraries used in coredns version 1.10.1 are old and contain known security vulnerabilities. Need to update the package to the latest version 1.12.0 to resolve the issues.		
Condition:	The problem exists in coredns version 1.10.1 and latest libraries are used in updated version 1.12.0		

Parent Defect ID:	XCO-11944		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.8.0
Symptom:	The local-path-provisioner package 0.0.28 used in XCO is old which uses older cypto, net, protobuf and stdlib libraries. These older libraries have some known vulnerabilities which could possibly exploited in the customer deployment environment.		
Condition:	These vulnerabilities exist in older 0.0.28 package. These issues are resolved in newer 0.0.30 package of local-path-provisioner.		

Open Defects

There are no open defects in ExtremeCloud Orchestrator 3.7.1.

Security Patch

The following table lists the updated security components and vulnerabilities addressed in ExtremeCloud Orchestrator 3.7.1.

Components	Previous Version	Latest Version	Vulnerabilities
local-path-provisioner	0.0.28	0.0.30	• CVE-2024-45337 • CVE-2023-48795 • CVE-2024-45338 • CVE-2023-45288 • CVE-2024-24786 • CVE-2024-24790 • CVE-2023-45288 • CVE-2024-34156 • CVE-2023-39326 • CVE-2023-45289 • CVE-2023-45290 • CVE-2024-24783 • CVE-2024-24784 • CVE-2024-24785 • CVE-2024-24789 • CVE-2024-24791 • CVE-2024-34155 • CVE-2024-34158 • CVE-2024-45336 • CVE-2024-45341
local-path-provisioner	0.0.28	0.0.30	• CVE-2024-4741 • CVE-2024-5535 • CVE-2024-6119 • CVE-2024-9143 • CVE-2024-4741 • CVE-2024-5535 • CVE-2024-6119 • CVE-2024-9143

Components	Previous Version	Latest Version	Vulnerabilities
Coredns	1.10.1	1.12.0	• CVE-2024-51744 • CVE-2024-45339 • CVE-2024-45337 • CVE-2023-48795 • CVE-2022-41723 • CVE-2023-39325 • CVE-2024-45338 • CVE-2023-3978 • CVE-2023-44487 • CVE-2023-45288 • CVE-2023-44487 • CVE-2024-24786 • CVE-2024-24538 • CVE-2024-24540 • CVE-2024-24790 • CVE-2022-41722 • CVE-2022-41723 • CVE-2022-41724 • CVE-2022-41725 • CVE-2023-24534 • CVE-2023-24536 • CVE-2023-24537 • CVE-2023-24539 • CVE-2023-29400 • CVE-2023-29403 • CVE-2023-39325 • CVE-2023-45283 • CVE-2023-45288 • CVE-2024-34156 • CVE-2023-24532 • CVE-2023-29406 • CVE-2023-29409 • CVE-2023-39318 • CVE-2023-39319 • CVE-2023-39326 • CVE-2023-45284 • CVE-2023-45289 • CVE-2023-45290 • CVE-2024-24783 • CVE-2024-24784 • CVE-2024-24785 • CVE-2024-24789 • CVE-2024-24791 • CVE-2024-34155 • CVE-2024-34158 • CVE-2024-45336 • CVE-2024-45341

Components	Previous Version	Latest Version	Vulnerabilities
raetrafik	2.10.7	2.11.18	• CVE-2024-35255 • CVE-2024-41110 • CVE-2023-28840 • CVE-2023-28841 • CVE-2023-28842 • CVE-2024-24557 • CVE-2024-29018 • CVE-2024-28180 • GHSA-2c7c-3mj9-8fqh • CVE-2024-51744 • CVE-2024-6104 • CVE-2024-22189 • CVE-2023-49295 • CVE-2024-53259 • CVE-2024-45337 • CVE-2023-48795 • CVE-2024-45338 • CVE-2023-45288 • CVE-2024-24786 • CVE-2024-24790 • CVE-2023-45288 • CVE-2024-34156 • CVE-2023-45289 • CVE-2023-45290 • CVE-2024-24783 • CVE-2024-24784 • CVE-2024-24785 • CVE-2024-24789 • CVE-2024-24791 • CVE-2024-34155 • CVE-2024-34158 • CVE-2024-45336 • CVE-2024-45341

Components	Previous Version	Latest Version	Vulnerabilities
mirrored-library-traefik	2.10.7	2.11.18	• CVE-2023-42363 • CVE-2023-42364 • CVE-2023-42365 • CVE-2023-42366 • CVE-2023-42363 • CVE-2023-42364 • CVE-2023-42365 • CVE-2023-42366 • CVE-2024-4603 • CVE-2024-4741 • CVE-2024-5535 • CVE-2024-6119 • CVE-2024-2511 • CVE-2024-9143 • CVE-2024-4603 • CVE-2024-4741 • CVE-2024-5535 • CVE-2024-6119 • CVE-2024-2511 • CVE-2024-9143 • CVE-2023-42363 • CVE-2023-42364 • CVE-2023-42365 • CVE-2023-42366
erlang	25.3.2.15	27.2.4	• CVE-2024-12254 • CVE-2024-9287 • CVE-2024-12254 • CVE-2024-9287

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.