



ExtremeCloud™ Orchestrator v3.8.5 Release Notes

New Features, Supported Platforms, and Known Issues

9039188-05 Rev AA
January 2025



Copyright © 2025 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/>

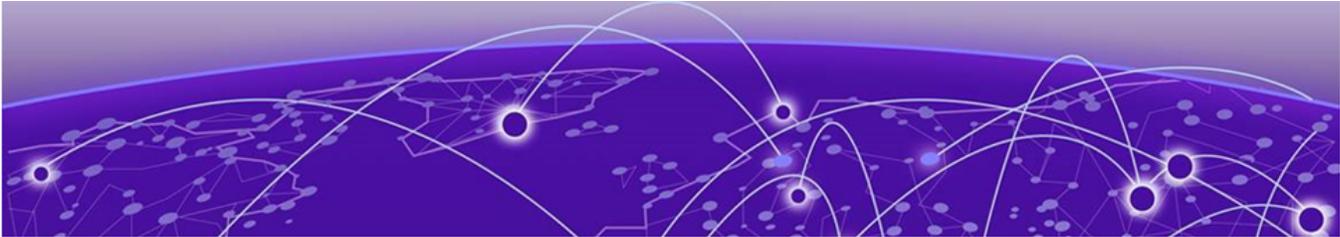
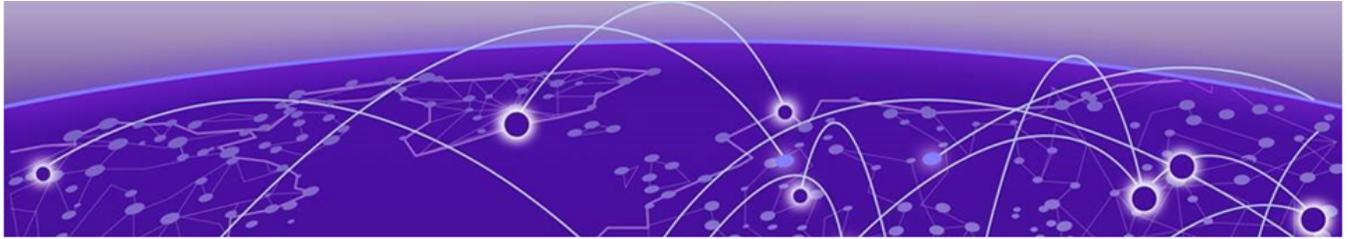


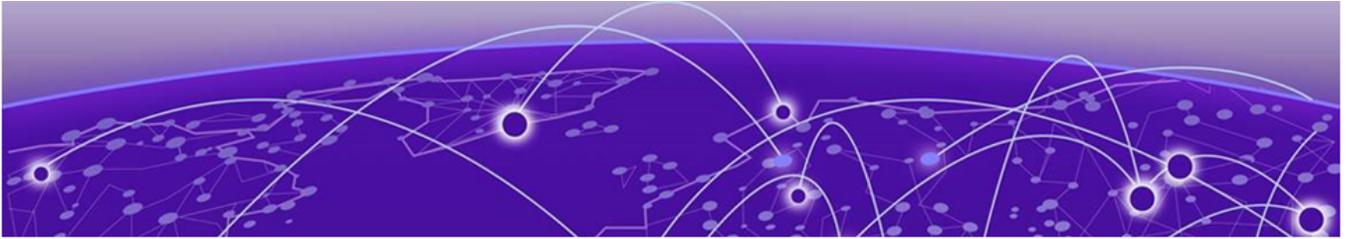
Table of Contents

Abstract.....	iv
Release Notes.....	5
New In This Release.....	5
Supported Platforms and Deployment Models for Fabric Skill.....	7
Supported Platforms and Deployment Models for Visibility Skill.....	10
XCO Upgrade Prerequisites.....	11
Open Issues.....	12
Security Patch	14
Help and Support.....	15
Subscribe to Product Announcements.....	15



Abstract

The release notes for ExtremeCloud™ Orchestrator version 3.8.5 presents a security-focused maintenance release that delivers critical updates to core orchestration components and addresses multiple CVEs. The document outlines supported deployment models—including Server, OVA, and TPVM—across validated Ubuntu and SLX-OS versions, with compatibility matrices for SLX and Extreme hardware platforms. Upgrade procedures emphasize DNS cleanup and persistent management connectivity. Visibility skill support, SSH hardening guidance, and hostname compliance rules are also covered. Additionally, this release introduces feature support for Max-Path Fabric Setting, MCT Keep Alive Configuration, and RMA from SLX 9250 to SLX 8720. The content is tailored for technically proficient users managing multi-fabric orchestration in high-availability environments.



Release Notes

[New In This Release](#) on page 5

[Supported Platforms and Deployment Models for Fabric Skill](#) on page 7

[Supported Platforms and Deployment Models for Visibility Skill](#) on page 10

[XCO Upgrade Prerequisites](#) on page 11

[Open Issues](#) on page 12

[Security Patch](#) on page 14

New In This Release

ExtremeCloud Orchestrator 3.8.5 introduces the following features and enhancements, resolves issues through defect fixes, and includes a critical security patch. For

information about XCO deployment, refer to the *ExtremeCloud Orchestrator Deployment Guide, 3.8.0*.



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.

Table 1: Features and enhancements

Feature	Description
Max-Path Fabric Setting	Default max-path fabric setting is supported on active fabric. For more information, see <i>ExtremeCloud Orchestrator CLI Administration Guide, 3.8.5</i> .
MCT Keep Alive Configuration	MCT keep alive configuration is supported on both active and inactive fabrics. For more information, see <i>ExtremeCloud Orchestrator CLI Administration Guide, 3.8.5</i> .
RMA from SLX 9250 to SLX 8720	Standardizes procedure for replacing SLX 9250 switches with SLX 8720, addressing both reachable and unreachable device scenarios. Includes steps to remove RME and breakout configurations from the XCO database to ensure a seamless RMA process. For more information, see <i>ExtremeCloud Orchestrator CLI Administration Guide, 3.8.5</i> .

For more information, see:

- [Open Issues](#) on page 12
- [Security Patch](#) on page 14

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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.7.x, 3.8.x	More than 24	Yes	22.04 LTS	<ul style="list-style-type: none"> • 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 SLX-OS Version
3.4.x, 3.5.x, 3.6.x	<ul style="list-style-type: none"> • SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 	Up to 24	Yes	20.04 LTS	20.5.2a

Table 4: TPVM Deployment Models (continued)

XCO Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum SLX-OS Version
	<ul style="list-style-type: none"> Extreme 8720 Extreme 8820 (20.4.3 and later) 				
3.7.x	<ul style="list-style-type: none"> 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
3.8.x	<ul style="list-style-type: none"> SLX 9150 SLX 9250 SLX 9740 Extreme 8520 Extreme 8720 Extreme 8820 (20.4.3 and later) 	Up to 24	Yes	22.04 LTS	20.7.1

Table 5: 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
3.8.0	4.7.4	20.7.1a
3.8.1	4.7.5	20.7.1a
3.8.2	4.7.7, 4.7.9	20.7.1ab, 20.7.2ab
3.8.3	4.7.8	20.7.1ab

Table 5: TPVM Software Support (continued)

XCO Version	TPVM Version	SLX-OS Version
3.8.4	4.7.10	20.7.2ab
3.8.5	4.7.12	20.7.3a

Table 6: IP Fabric Topology Matrix

Device	SLX-OS Release	Leaf	Spine	Super Spine	Border Leaf	Small DC Fabric
SLX 9150	20.5.x, 20.6.x, 20.7.x	Yes				Yes
SLX 9250	20.5.x, 20.6.x, 20.7.x	Yes	Yes	Yes		Yes
SLX 9540	20.5.x, 20.6.x, 20.7.x	Yes			Yes	
SLX 9640	20.5.x, 20.6.x, 20.7.x				Yes	
SLX 9740	20.5.x, 20.6.x, 20.7.x		Yes	Yes	Yes	Yes
Extreme 8720	20.5.x, 20.6.x, 20.7.x	Yes	Yes	Yes	Yes	Yes
Extreme 8520	20.5.x, 20.6.x, 20.7.x	Yes			Yes	Yes
Extreme 8820	20.5.x, 20.6.x, 20.7.x		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 7: Ubuntu Server Version

XCO Version	Ubuntu Version	Virtual Machine
3.4.x, 3.5.x, 3.6.x	18.04 LTS and 20.04 LTS	Minimum: <ul style="list-style-type: none">• CPU: 4 cores• Storage: 128 GB• RAM: 8 GB Recommended: <ul style="list-style-type: none">• CPU: 16 cores• Storage: 200 GB• RAM: 32 GB
3.7.x, 3.8.x	20.04 LTS and 22.04 LTS	Minimum: <ul style="list-style-type: none">• CPU: 4 cores• Storage: 128 GB• RAM: 8 GB Recommended: <ul style="list-style-type: none">• CPU: 16 cores• Storage: 200 GB• RAM: 32 GB

Table 8: OVA Deployment Models

XCO Version	Ubuntu Version	Virtual Machine
3.4.x, 3.5.x, 3.6.x	20.04 LTS	Minimum: <ul style="list-style-type: none">• CPU: 4 cores• Storage: 64 GB• RAM: 8 GB
3.7.x, 3.8.x	22.04 LTS	Minimum: <ul style="list-style-type: none">• CPU: 4 cores• Storage: 64 GB

Table 8: OVA Deployment Models (continued)

XCO Version	Ubuntu Version	Virtual Machine
		<ul style="list-style-type: none"> RAM: 8 GB

Table 9: Supported Devices and Software

Device	Supported Software
Extreme 9920	Extreme 9920 software with the NPB application <ul style="list-style-type: none"> 21.1.2.x 21.2.1.x 21.2.2.x
Extreme Routing MLX Series	<ul style="list-style-type: none"> NetIron 6.3.00 patches
Extreme Switching SLX 9140	<ul style="list-style-type: none"> SLX-OS 18s.1.03 patches
Extreme Switching SLX 9240	<ul style="list-style-type: none"> 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.

Open Issues

The following issues are open in this release.

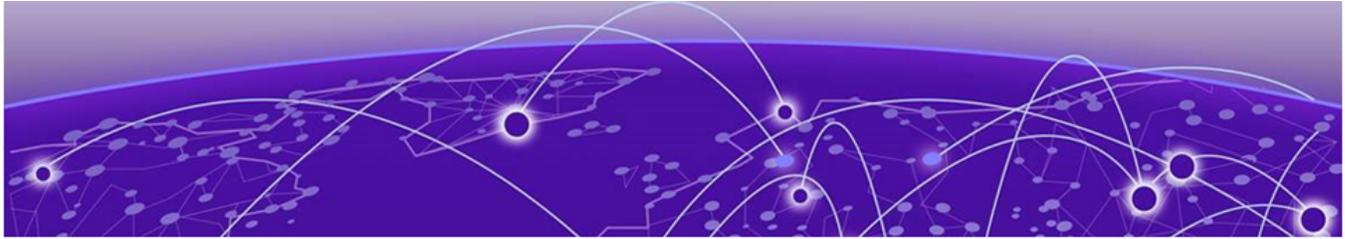
Issue ID	Description
XCO-15741	<p>Symptom: Fabric service fails to execute DB queries and becomes unresponsive due to stale or broken DB connection. Logs show: Error 1047 (08S01): WSREP has not yet prepared node for application use.</p> <p>Condition: Occurs when the DB node is not ready for application use (WSREP is not in primary/ready state), and the Fabric service continues to hold an old database session instead of establishing a new one.</p> <p>Workaround: Restart the Fabric service using the <code>efactl restart-service fabric</code> command.</p> <p>Recovery: The startup script, XCO/scripts/k3s-deployment/app_efa_template.yaml is updated to check WSREP readiness before starting the Fabric service, preventing the stale DB handle issue. No fix applied in Fabric code.</p>
XCO-15683	<p>Symptom: The <code>efa certificate device expiry show</code> command returns the "Sync comparison error for HTTPS certificate" error.</p> <p>Workaround: Reinstall the HTTPS certificate for the affected fabric using the <code>efa certificate device install --cert-type https --fabric=<fabric-name> --force</code> command.</p> <p>Note: This operation restarts the HTTP service on SLX devices, and services will be unavailable until the process is complete.</p>
XCO-15641	<p>Symptom: Tenant service restart count increases when services are listed. This does not impact functionality. During the upgrade, tenant service restarts are observed and restart count is increased.</p> <p>Condition: Occurs when XCO is upgraded to the newer version.</p>
XCO-15632	<p>Symptom: When DRC is triggered simultaneously for all MCT devices after a system restore, DRC may fail on one or more devices during MCT cluster configuration reconciliation.</p> <p>Workaround: Run DRC for the failed devices.</p>

Issue ID	Description
XCO-15600	<p>Symptom: When XCO is upgraded from version 3.8.X to another 3.8.X/Y build, the permissions for /apps/efadata/certs, /apps/efadata/misc, and /apps/efadata/efa_logs change. As a result, error messages appear as shown.</p> <p>Condition:</p> <pre>(efa:extreme)extreme@node-1b:~\$ efa fabric show Failed to fire hook: can't rename log file: rename /apps/efa_logs/efa-client.log / apps/efa_logs/efa- client-2025-11-14T04-58-41.562.log: permission denied Failed to fire hook: can't rename log file: rename / apps/efa_logs/efa-client.log / apps/efa_logs/efa- client-2025-11-14T04-59-04.451.log: permission denied</pre> <p>Recovery:</p> <pre>chown root:efa /apps/efa_logs chown root:efa /apps/efadata/certs chown root:efa /apps/efadata/misc</pre> <p>Run the following commands to validate:</p> <pre>ls -lrt /apps/ total 48 drwx----- 2 root root 16384 Nov 27 00:02 lost+found drwxr-xr-x 3 root root 4096 Nov 27 01:28 etc drwxr-xr-x 3 root root 4096 Nov 27 01:32 opt drwxr-xr-x 3 root root 4096 Nov 27 01:40 rancher drwxrwx--- 19 root efa 4096 Nov 27 01:44 efa drwxr-xr-x 10 root efa 4096 Nov 27 01:49 efadata drwxr-xr-x 3 root root 4096 Nov 27 01:49 bin drwxr-xr-x 3 extreme root 4096 Nov 27 02:02 k3s-db drwxrwxr-x 32 root efa 4096 Nov 30 00:00 efa_logs ls -lrt /apps/efadata total 32 drwxr-xr-x 2 root root 4096 Nov 27 01:32 galera drwxr-x--- 2 root efa 4096 Nov 27 01:38 active drwxr-xr-x 3 systemd-network efa 4096 Nov 27 01:45 rabbitmq drwxr-xr-x 2 root root 4096 Nov 27 01:50 tmp drwxr-xr-x 11 root efa 4096 Nov 27 02:08 certs drwxr-x--- 20 mysql efa 4096 Nov 27 04:58 mysql drwxrwxrwx 2 root efa 4096 Dec 1 05:11 sfm drwxr-x--- 9 root efa 4096 Dec 1 17:00 misc</pre>
XCO-15582	<p>Symptom: Router BGP drift for peer-group and MCT neighbor configurations may occur during fabric creation on some devices.</p> <p>Workaround: Run DRC on all devices where configuration drift is detected.</p>

Issue ID	Description
XCO-15575	<p>Symptom: Drift (auto/manual) is detected for max-paths when performed after updating fabric settings but before running fabric configure.</p> <p>Workaround: Run the <code>efa fabric configure</code> command to push the configuration to the device.</p>
XCO-15572	<p>Symptom: Updating fabric settings with <code>efa fabric setting update max-path</code> triggers a configuration refresh (cfg-refresh) for BGP on some SLX devices.</p> <p>Condition: Changing the max-path setting before deep discovery completes triggers BGP drift. In this condition, BGPU persists and the device enters the <code>cfg-refresh</code> state.</p> <p>Workaround: Run the <code>efa fabric configure</code> command to push the fabric settings and clear the configuration generation reasons.</p>

Security Patch

Component	Previous Version	Latest Version	Vulnerabilities
Others	NA	NA	CVE-2025-8194 CVE-2025-54386 CVE-2025-4673 GHSA-fv92-fjc5-jj9h CVE-2025-6069 GHSA-2464-8j7c-4cjm CVE-2025-8291 GHSA-v6h2-p8h4-qcjl CVE-2025-47952 GHSA-q82r-2j7m-9rv4 GHSA-4vq8-7jfc-9cjp CVE-2025-58050 CVE-2025-64756 CVE-2025-10966 CVE-2025-5889



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.