ExtremeCloud™ Orchestrator Release Notes v3.7.0

New Features, Supported Platforms, and Known Issues

9039078-00 Rev AA
December 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/

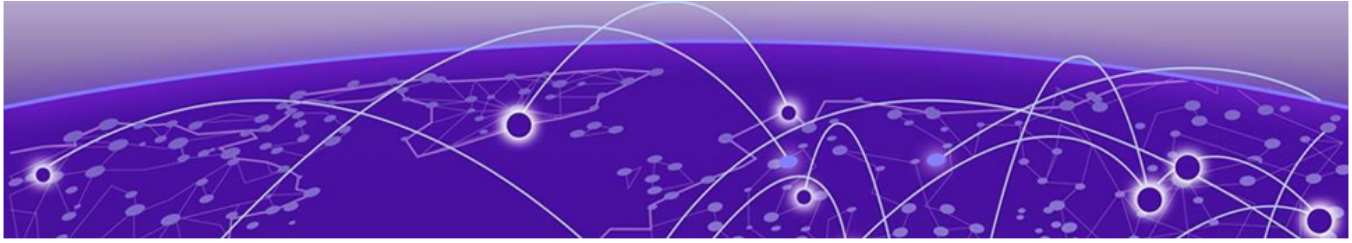
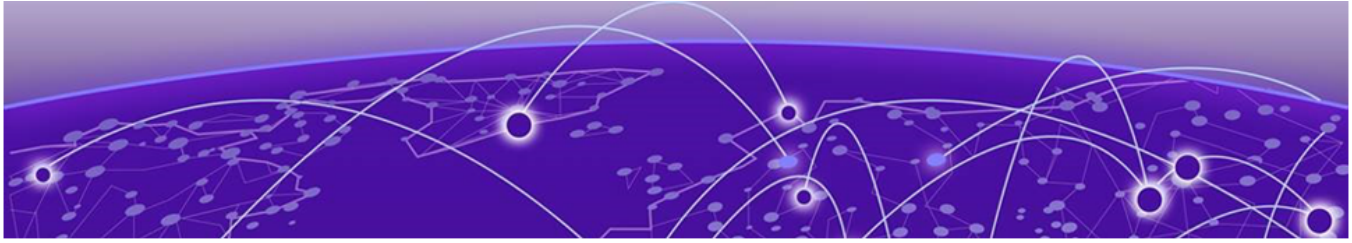


Table of Contents



Release Notes

Release Information

Release Date: December 2024

The release notes for ExtremeCloud™ Orchestrator version 3.7.0 detail new features, supported platforms, upgrade prerequisites, closed and open defects, and known limitations. New features include enabling passwordless SSH or SCP for backup and log file operations, configuring description for the device interface, upgrading Ubuntu OS and TPVM, and user interface enhancements. Supported deployment models include server, OVA, and TPVM across various versions. The document outlines upgrade prerequisites and known limitations for fabric and visibility skills, such as issues with policy applications and REST operations. Numerous defects were addressed, including BGP peer deletion errors and firmware version discrepancies, while open defects involve issues like device discovery limitations and configuration drift in dynamic peers. For support, users are directed to Extreme Networks' various customer service channels.

New In This Release

ExtremeCloud Orchestrator 3.7.0 introduces the following features and resolves issues through defect fixes. 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.

Table 1: Features and Improvements

Feature	Description
Enable passwordless SSH or SCP for backup and log file operations	• Added a new topic, "Configure Remote Settings" that describes the procedure to configure remote server settings using CLI and API. • Added a new topic, "PasswordLess SSH or SCP Support for Secure and Efficient Backup and Supportsave Transfers" that describes the procedure to enable passwordLess SSH or SCP for secure backup and supportsave transfers. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.7.0*.
Set or unset description for the device interface	Added a new topic, "Configure Description on Device Interface" that describes the procedure to set or unset the description for the interface on devices.` For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.7.0*.
Support matrix	Updated the support matrices for supported platforms and deployment models for fabric and visibility skills. For more information, refer to the *ExtremeCloud Orchestrator Deployment Guide, 3.7.0*.
Upgrade Ubuntu OS and TPVM	Added new topics: • Upgrade of Ubuntu OS of XCO Installed Server • Upgrade TPVM of XCO Installed Server For more information, refer to the *ExtremeCloud Orchestrator Deployment Guide, 3.7.0*.

Table 1: Features and Improvements (continued)

Feature	Description
System Hardening for CIS-CAT Assessments	CIS-CAT Assessments system hardening updates. For more information, refer to the *ExtremeCloud Orchestrator Configuration Guide, 3.7.0*.
UI updates	• Network Essentials enhancements • Sync Firmware Version For more information, refer to the *ExtremeCloud Orchestrator GUI Administration Guide, 3.7.0*.

For other additional information, see Defects Closed with Code Changes on page 12.

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 2: 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

Table 2: Server Deployment Models (continued)

XCO Version	Managed SLX Devices	Multi-Fabric Support	Ubuntu Server Version	Virtual Machine
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

Table 3: 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
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 4: 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	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
	• Extreme 8720 • Extreme 8820 (20.4.3 and later)				
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 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

Table 6: IP Fabric Topology Matrix

Device	SLX-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 6: IP Fabric Topology Matrix (continued)

Device	SLX-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 7: 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 7: 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 8: 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 8: 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 9: 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 in ExtremeCloud Orchestrator 3.7.0.

Parent Defect ID:	XCO-9190	Issue ID:	
Product:	XCO Visibility Skill	Reported in Release:	XCO 3.3.0
Symptom:	GUI Library matches shows 2 devices when only 1 device discovered.		
Condition:	Remove all the devices and discover only one device.		
Workaround:	Discover device and remove all duplicate hash matches entries from match table for the device.		
Recovery:	Remove all duplicate hash matches entries from match table for the device.		

Parent Defect ID:	XCO-9734	Issue ID:	
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.4.0
Symptom:	REST request random failure was noticed by customer with "401 Unauthorized error" while reusing the authentication token.		
Condition:	XCO uses single TCP persistent connection for all REST requests and re-uses the same authentication token for subsequent REST calls . But there is a restriction in SLX http server side while using the same authentication token in single persistent connection. Where it can have maximum number of 100 requests in a persistent connection. Once it reaches the maximum request, SLX http server closes its connection and rejects all subsequent REST requests with "401 Unauthorized" error for that token.		
Recovery:	Retrigger the failed configuration again will succeed.		

Parent Defect ID:	XCO-9983	Issue ID:	
Product:	XCO Visibility Skill	Reported in Release:	XCO 3.5.0
Symptom:	Faulty card state is shown as online.		
Condition:	When the card type is changed to invalid type, card state will be shown as online/active though the card is in faulty state.		
Workaround:	Set the correct card type based on the card present in device.		
Recovery:	Delete and re-discover the device		

Parent Defect ID:	XCO-10073	Issue ID:	
Product:	XCO Visibility Skill	Reported in Release:	XCO 3.5.0
Symptom:	Statistics are not displayed/updated in XCO device overview page		
Condition:	When SLX (9140/9240) device is discovered with IPv6 address.		

Parent Defect ID:	XCO-10073	Issue ID:	
Workaround:	Discover the SLX device with IPv4 address.		
Recovery:	Delete the device which is discovered with IPv6 address and re-discover with IPv4 address.		

Parent Defect ID:	XCO-10234	Issue ID:	
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.3.1
Symptom:	Duplicate entries for auth-type HOST are seen in 'efa auth authentication preference show'		
Condition:	Duplicate entries for auth-type HOST are seen in 'efa auth authentication preference show'		

Parent Defect ID:	XCO-10366	Issue ID:	
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.5.0
Symptom:	TPVM upgrade from 4.6.7 to 4.6.11 fails intermittently		
Condition:	Upgrade TPVM from 4.6.7 to 4.6.11		
Workaround:	Upgrade TPVM sequentially.		
Recovery:	Upgrade TPVM sequentially.		

Parent Defect ID:	XCO-10548	Issue ID:	
Product:	XCO Visibility Skill	Reported in Release:	XCO 3.5.0
Symptom:	Inventory reports excel sheet have latest and correct information but not the Inventory GUI Page.		
Condition:	Perform firmware upgrade from device itself.		
Workaround:	Discover the device again.		
Recovery:	Discover the device again.		

Parent Defect ID:	XCO-10558	Issue ID:	
Product:	XCO Visibility Skill	Reported in Release:	XCO 3.6.0
Symptom:	Post import the csv that has multiple SLXs and at various locations mentioned. Upload successful discovery in the inventory list we see the location names are given only one name.		
Condition:	Import devices using cvs file with different locations.		

Parent Defect ID:	XCO-10558	Issue ID:	
Workaround:	Add device one by one using Add device button.		
Recovery:	Add device one by one using Add device button from XCO GUI.		

Parent Defect ID:	XCO-10560	Issue ID:	
Product:	XCO Visibility Skill	Reported in Release:	XCO 3.6.0
Symptom:	XCO GUI discovered SLX9240 but failed to install syslog certificate		
Condition:	When SLX only has ipv6 address configured		
Workaround:	Use IPv4 address.		
Recovery:	Configure device with IPv4 address and discover from XCO GUI.		

Parent Defect ID:	XCO-10578	Issue ID:	
Product:	XCO Visibility Skill	Reported in Release:	XCO 3.5.0
Symptom:	A discrepancy is seen for 'efa device secure settings' Max Password Age and Force Default Password Change between the security guide and default values		
Condition:	A discrepancy is seen for 'efa device secure settings' Max Password Age and Force Default Password Change between the security guide and default values		

Parent Defect ID:	XCO-10628	Issue ID:	
Product:	XCO Visibility Skill	Reported in Release:	XCO 3.6.0
Symptom:	XCO GUI Library filters are not working for matches and policies		
Condition:	Search the ACL by name.		
Workaround:	Search Matches and policies by "Device type".		

Parent Defect ID:	XCO-10732	Issue ID:	
Product:	XCO Visibility Skill	Reported in Release:	XCO 3.6.0
Symptom:	XCO GUI inventory download page missing MLX firmware version with line cards SN and part numbers.		
Condition:	Fetch inventory Summary details from XCO inventory page.		

Parent Defect ID:	XCO-10749	Issue ID:	
	XCO Fabric Skill	Reported in Release:	XCO-3.6.0

Parent Defect ID:	XCO-10749	Issue ID:	
Product:			
Symptom:	IPV4 MTU config is not pushed to device thought the XCO EPG update command though the command executed successfully		
Condition:	IPV4 MTU config is not pushed to device thought the XCO EPG update command though the command executed successfully		

Parent Defect ID:	XCO-10799	Issue ID:	
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.6.0
Symptom:	XCO reports "TPVM Instance failed to come up" though the TPVM is upgraded successfully		
Condition:	XCO reports "TPVM Instance failed to come up" though the TPVM is upgraded successfully		

Parent Defect ID:	XCO-10813	Issue ID:	
Product:	XCO Common	Reported in Release:	XCO 3.3.1
Symptom:	XCO upgrade fails with error 'Device does not exist'		
Condition:	XCO upgrade fails with error 'Device does not exist'		

Parent Defect ID:	XCO-10830	Issue ID:	
Product:	XCO Visibility Skill	Reported in Release:	XCO 3.6.0
Symptom:	MLX device with specific patches 6300bc was not discovered using XCO GUI 3.6.		
Condition:	MLX device should be configured with 6300bc.		
Workaround:	Configured MLX device with other versions ex:- 6300a and then discover.		
Recovery:	Configured MLX device with other versions ex:- 6300a and then discover.		

Parent Defect ID:	XCO-10885	Issue ID:	
Product:	XCO Visibility Skill	Reported in Release:	XCO 3.6.0
Symptom:	SLX9240 IPV6 discovery failing in XCO3.6 GUI due to IPV6 short form.		
Condition:	SLX9240 device should be configured with IPV6 short form.		

Parent Defect ID:	XCO-10885	Issue ID:	
Workaround:	Configure device with IPv6 long form, while trying multiple devices		
Recovery:	Configure device with IPv6 long form and discover devices.		

Parent Defect ID:	XCO-11024	Issue ID:	
Product:	XCO Visibility Skill	Reported in Release:	XCO 3.6.0
Symptom:	In case of no port speed, the field was disabled under the Edit Port configuration page on XCO GUI.		
Condition:	Device port configured with no port speed .		
Workaround:	Configure the port speed and discover the device.		
Recovery:	Configure the port speed and discover the device.		

Parent Defect ID:	XCO-11378	Issue ID:	
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.6.0
Symptom:	XCO API returns "HTTP/2 502 - Bad Gateway" for vrf-delete operation		
Condition:	XCO API returns "HTTP/2 502 - Bad Gateway" for vrf-delete operation		

Open Defects

There following defects are open in ExtremeCloud Orchestrator 3.7.0.

Parent Defect ID:	XCO-8191	Issue ID:	
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.3.0
Symptom:	If you run concurrent epg update commands operation as port-group-add or vrf-add on bridge-domain EPGs that are associated with more than one ctag, one or some of the commands may fail with error "Save for device failed".		
Condition:	This is observed more often when more than 3 concurrent EPG port-group-add commands with non-conflicting ports and non-overlapping ctag-range are executed. Occasionally, configuration information that is pushed by one command is not used properly to prepare command recipe for another, causing the failure of one command.		

Parent Defect ID:	XCO-8191	Issue ID:	
Workaround:	Rerunning the failing command will succeed. The error is intermittent and does not cause permanent changes. XCO state information is not affected at any point.		
Recovery:	No recovery is required as no state change is done as part of this failure.		

Parent Defect ID:	XCO-9307	Issue ID:	
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.4.0
Symptom:	After the upgrade from 3.5.0 to 3.6.0, removing all the configuration from XCO/devices and restoring the 3.5.0 backup followed by manual DRC failed to push the configurations to the devices		
Condition:	After the upgrade from 3.5.0 to 3.6.0 and when the user removes the configurations. Backup and restore work fine right after the upgrade without removing the configurations.		

Parent Defect ID:	XCO-9363	Issue ID:	
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.4.0
Symptom:	After removing the tenant using the --force option, Fabric binding is not applied on the physical interfaces which were part of the port-channel/physical interfaces.		
Condition:	Issue is observed when user issues the command 'efa tenant delete --name <tenant_name> --force'		
Workaround:	User needs to unbind the policies (QoS) from all the relevant targets (fabric/tenant/port/port channel/tenant endpoint group) before executing the force operations including delete to avoid the stale policies(QoS) in the system.		

Parent Defect ID:	XCO-9769	Issue ID:	
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.4.1
Symptom:	Unable to delete the prefix list from Policy Service , even though it is not binded in tenant service		
Condition:	After deleting the ipv6 prefix from bgp-peer in tenant service, not able to delete prefix-list from policy service		
Recovery:	Please issue the following CLI command: efa inventory device update --ip <>		

Parent Defect ID:	XCO-9942	Issue ID:	
	XCO Fabric Skill	Reported in Release:	XCO 3.5.0

Parent Defect ID:	XCO-9942	Issue ID:	
Product:			
Symptom:	Few PO's will remain on SLX Devices and Few PO's will remain in XCO database after executing EPG delete and PO delete in quick succession. [Two commands executed at same time]		
Condition:	Few PO's will remain on SLX Devices and Few PO's will remain in XCO database after executing EPG delete and PO delete in quick succession. [Two commands executed at same time]		
Workaround:	Delete EPG and wait for the profile to be applied on the po's and then delete po's after making sure EPG delete is complete.		
Recovery:	GO to SLX device and Remove the PO's manually and do inventory device update.		

Parent Defect ID:	XCO-10067	Issue ID:	
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.5.0
Symptom:	After adding border-leaf to the fabric, fabric-internal profile is not getting applied on the MCT port-channel.		
Condition:	After adding new devices(leaf/border-leaf) to the fabric followed by fabric configure, fabric-internal profile is not getting applied on the MCT Port-channel of the newly added devices(leaf/border-leaf).		
Workaround:	User can issue rebind the fabric internal port QoS profile using below command: Bind Fabric internal ports QoS profile: efa policy qos profile bind --name <profile_name> --fabric <fabric_name> --port fabric-internal.		
Recovery:	User can issue rebind the fabric internal port QoS profile using below command: Bind Fabric internal ports QoS profile: efa policy qos profile bind --name <profile_name> --fabric <fabric_name> --port fabric-internal.		

Parent Defect ID:	XCO-10430	Issue ID:	
	XCO Common	Reported in Release:	XCO 3.6.0

Parent Defect ID:	XCO-10430	Issue ID:	
Product:			
Symptom:	In the firmware history page, the previous and target versions are interchanged during the firmware restore operation. The same issue is also seen in the firmware history CLI response.		
Condition:	firmware restore operation on a 9920 device or a fabric SLX device from the GUI or CLI.		

Parent Defect ID:	XCO-10566	Issue ID:	
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.4.1
Symptom:	Configuring switchport mode trunk fails with netconf rpc error: 'Config not allowed as it will exceed system max allowed AC LIFs..',		
Condition:	Network Policy Error: Configuring switchport mode trunk on 27 failed due to netconf rpc [error] '%Error: Config not allowed as it will exceed system max allowed AC LIFs..' is seen while creating EPGs with high CTAG range and port channels		
Workaround:	When the EPG creation fails for high CTAG range, create it incrementally using medium/less CTAG ranges until the available limit is reached.		

Parent Defect ID:	XCO-10727	Issue ID:	
Product:	XCO Visibility Skill	Reported in Release:	XCO 3.6.0
Symptom:	Start/Stop packet capture for 9920or SLX device and observe the behavior.		
Condition:	Start packet capture for device 9920 or SLX.		
Workaround:	Do not stop packet capture when pcap capture count reached to max limit 25 in case of 9920 device.		

Parent Defect ID:	XCO-10980	Issue ID:	
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.7.0
Symptom:	Description is not setting on the fabric ports, after set-description command.		
Condition:	When set-description command is used for setting the description for fabric ports, the description is not setting on the fabric ports interface.		

Parent Defect ID:	XCO-11047	Issue ID:	
	XCO Fabric Skill	Reported in Release:	XCO 3.7.0

Parent Defect ID:	XCO-11047	Issue ID:	
Product:			
Symptom:	After upgrade and DRC, the description is not retained on interface		
Condition:	When the XCO is upgraded, description is not retained after DRC is done.		

Parent Defect ID:	XCO-11053	Issue ID:	
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.6.0
Symptom:	The command 'efa inventory device setting update' accepts same range of values for the --crypto-cert-expiry levels Info, Minor, Major and Critical		
Condition:	While running the command 'efa inventory device setting update', the flags --crypto-cert-expiry-info, --crypto-cert-expiry-minor, --crypto-cert-expiry-major and --crypto-cert-expiry-critical accepts values of range 0-90.		

Parent Defect ID:	XCO-11138	Issue ID:	
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.7.0
Symptom:	GoNotification pod will be missing from k3s after renewal of k3s server certificate even if it is not disabled before the command execution.		
Condition	Executing "efa certificate server renew" will lead the system to end up in an issue state.		
Recovery:	Execute the commnad "efa system service enable notification"		

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.