



ExtremeCloud™ Orchestrator v3.6.0 Release Notes

New Features, Supported Platforms, and Known Issues

9038974-00 Rev AB
August 2024



Copyright © 2024 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/>

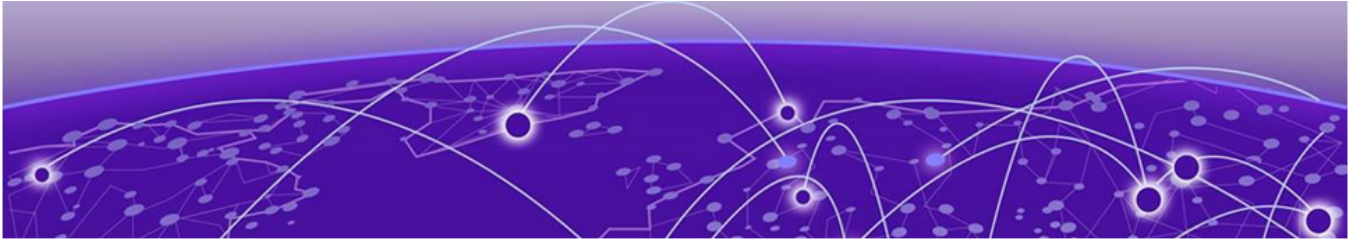


Table of Contents

Release Notes.....	4
Release Information.....	4
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
Known Limitations.....	12
Known Limitations in Fabric Skill.....	12
Known Limitations in Visibility Skill.....	14
Defects Closed with Code Changes	15
Open Defects.....	20
Help and Support.....	23
Subscribe to Product Announcements.....	24



Release Notes

[Release Information](#) on page 4

[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

[Known Limitations](#) on page 12

[Defects Closed with Code Changes](#) on page 15

[Open Defects](#) on page 20

[Help and Support](#) on page 23

Release Information

Release Date: August 2024

The release notes for ExtremeCloud™ Orchestrator version 3.6.0 detail new features, supported platforms, upgrade prerequisites, closed and open defects, and known limitations. New features include retaining route-target configurations on border leaf devices, updated support matrices for fabric and visibility skills, and user interface updates. 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 3.6.0 introduces the following features and resolves issues through defect fixes. For information about XCO deployment, refer to the [ExtremeCloud Orchestrator Deployment Guide, 3.6.0](#).



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
Preserve "retain route-target all" on boarder leaf devices	Added a new topic, "Retain Route Target All on Boarder Leaf Devices" that describes procedure to ignore "retain route target all" configuration present on boarder leaf devices. For more information, refer to the ExtremeCloud Orchestrator CLI Administration Guide, 3.6.0 .
Enable or Disable Database Log Traces	Updated the topic "XCO System Backup and Restoration" with the information on how to "Enable or Disable Database Log Traces" for debugging purposes. For more information, refer to the ExtremeCloud Orchestrator CLI Administration Guide, 3.6.0 .
Support Matrices	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, 3.6.0 .
OS Versions and Security updates	Updated the "OS Versions and Security Updates" topic with the details on removing the locks held on Debian packages. For more information, refer to the ExtremeCloud Orchestrator Deployment Guide, 3.6.0 .
System Hardening for CIS-CAT Assessments	CIS-CAT Assessments system hardening updates. For more information, refer to the ExtremeCloud Orchestrator Security Guide, 3.6.0 .
UI updates	Lag Hash Masking For more information, refer to the ExtremeCloud Orchestrator GUI Administration Guide, 3.6.0 .

For other additional information, see [Defects Closed with Code Changes](#) on page 15.

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	<ul style="list-style-type: none"> • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.5.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
3.6.x	More than 24	Yes	18.04 LTS, 20.04 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	More than 24	Yes	20.04 LTS	<ul style="list-style-type: none"> • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.5.x	More than 24	Yes	20.04 LTS	<ul style="list-style-type: none"> • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.6.x	More than 24	Yes	20.04 LTS	<ul style="list-style-type: none"> • CPU: 4 cores • Storage: 64 GB

Table 3: OVA Deployment Models (continued)

XCO Version	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Virtual Machine
				• 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	<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	20.04 LTS	20.5.2a
3.5.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	20.04 LTS	20.5.2a
3.6.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	20.04 LTS	20.5.2a

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

Table 5: TPVM Software Support (continued)

XCO Version	TPVM Version	SLX-OS Version
3.5.0	4.6.10	20.6.1
3.6.0	4.6.13, 4.6.14	20.6.2, 20.6.2a

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	✓				✓
SLX 9250	20.2.x, 20.3.x, 20.4.x	✓	✓	✓		✓
SLX 9540	20.2.x, 20.3.x, 20.4.x	✓			✓	
SLX 9640	20.2.x, 20.3.x, 20.4.x				✓	
SLX 9740	20.2.x, 20.3.x, 20.4.x		✓	✓	✓	✓
Extreme 8720	20.3.x, 20.4.x	✓	✓	✓	✓	✓
Extreme 8520	20.3.x, 20.4.x	✓			✓	✓
Extreme 8820	20.4.3		✓	✓	✓	✓

Table 7: XCO or EFA, and SLX-OS Compatibility

XCO or EFA Version	SLX-OS Version
2.5.4, 2.5.5	20.3.2d

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 8: Ubuntu Server Version

XCO Version	Ubuntu Version	Virtual Machine
3.4.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
3.5.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
3.6.x	18.04 LTS, 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

Table 9: OVA Deployment Models

XCO Version	Ubuntu Version	Virtual Machine
3.4.x	20.04 LTS	Minimum: <ul style="list-style-type: none"> • CPU: 4 cores

Table 9: OVA Deployment Models (continued)

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

Table 10: 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.

Known Limitations

Note the following caveat for this release of ExtremeCloud Orchestrator.

- If the CLOS setup firmware upgrade encounters the error "Cannot start download before the new image is committed", then create a separate group only for the active XCO node and perform the firmware upgrade.

Known Limitations in Fabric Skill

Follow these caveats and limitations when using Fabric Skill.

Quality of Service (QoS) policy service support

- The XCO-driven application of policy is dynamic and can vary depending on the port's role, whether it belongs to a fabric, tenant, port channel, or tenant endpoint group.



Tip

As a best practice, avoid running user-driven policy operations in parallel with fabric, tenant, port channel, and tenant endpoint group operations.

To ensure that the fabric, tenant, port channel, and tenant endpoint group configurations are effective, run the **show** command before proceeding with the policy operations, and vice-versa.

- Before running the force operations, including deletion, ensure that you unbind the policies (QoS) from all the relevant targets (fabric, tenant, port, port channel, and tenant endpoint group) to avoid stale policies (QoS) in the system.
- Before executing the QoS policy bind commands, remove any conflicting or additional OOB (Out of Band) QoS configurations from the switches to ensure that the correct policies are applied to the ports.
- There is no support for a lossless hardware profile. Therefore, you must switch the configuration on SLX devices to a lossy hardware profile before provisioning QoS policies from XCO.
- There is no support for egress QoS maps. While XCO allows the configuration of egress QoS maps, as a best practice, do not configure any egress QoS maps from XCO due to limitations in SLX support of egress QoS maps.

VRF delete from EPG and re-adding VRF to EPG fails intermittently

Symptom	Condition	Workaround
Endpoint group (EPG) update vrf-add operation fails with the reason as VRF to be added has conflicting VRF on the switch.	Run EPG update vrf-add , vrf-delete , and vrf-add operation CLI in quick succession: <ol style="list-style-type: none"> 1. Update EPG for operation vrf-add. 2. Update EPG for operation vrf-delete. 3. Update the same EPG again with operation vrf-add for the same VRF which was deleted in step 2. 	Wait of 30 seconds between the EPG update vrf-add and vrf-delete operations on the same EPG.

REST operations are not retried (as applicable) during the service boot

Symptom	Condition	Workaround
REST operations are not retried (as applicable) during the service boot up.	After publishing the necessary events on the message bus, the status for the REST operations are not set automatically.	Manually set the status for all REST operations.

RBAC: XCO shows "export EFA_TOKEN" command suggestion when a tenant user logs in

Symptom	Condition	Workaround
XCO shows an export EFA_TOKEN message after a tenant user with RBAC logs in to the system.	When a user is created with the default login shell as sh.	XCO supports only bash shell for login or any other CLI commands. Ensure that bash is specified as the default login shell for all XCO user accounts.

Here's a sample token. Copy/Paste this in your shell:

export

```
EFA_TOKEN=eyJhbGciOiJSUzI1NiIsImtpZCI6IjEuMCIsInR5cCI6IkpXVCJ9.eyJjb21tb25fbmFtZSI6IktVQSBub2t1biBTZXJ2aWNlIiwidWFzIjpbeyJ0YXJnZXQiOiJFRkeiLCJyb2x1Ijoiv1IyLVRudEFkbWluInldLCJvcmeCI6IjFeHRyZW11IE5ldHdvcmtzIiwidmVyIjoimS4wIiwiaWQiOiIiLCJleHAiOjE2NDUyNDcxNDIsImp0aSI6IjZmja4ZDUxLTkwNzgtMTFlYy1iZjk5LWNhNzk1MDY1YzIwNyIsImh0CI6MTY0NTE2Mdc0MiwiaXNzIjoiuRUZBIFRva2VuIFNlcncZpY2UiLCJmYyIjE2NDUyNDUxNjA3NDIsInN1YiI6InVzZXIyIn0.b7m5PINijeEdNSqntE2ZzUrqrKLQAu079vXyBI dgHbXKt9ULfa03vMU1jfbO1qFb1-x0oHmsAQ0pSsF5JLeMaMzMf1Lf78ktZ08U5IePq72vM5en35IR-DNLyoGIZBeFeG6ZbBMoETzz5vf9OuefgQID3YdjcAlr7y1lCgDmLVFlgson77yCBpkTK15xm
```

```
1GRbtL7JKXZzShBE7E3kdW7N71MdM85Gc3r41-c8sfz7eo06gKrfTq9wXCv4_LVzR6-
KRSg6NyLq363WEpcK1A2Hs0Wo3T9TpquYHNaCWA5I1QTsG-
RHFdg4kxZP2fQpUp6Bgy1s6k59PVPn4-M-a81A- Time Elapsed: 4.619465187s —
```

XCO CLI or REST request with scale config takes longer than 15 minutes fails

Symptom	Condition	Workaround
<p>Tenant2 delete is successful whereas deleting Tenant1 took more than 15 minutes and failed with the following message:</p> <p>Error : service is not available or internal server error has occurred, please try again later</p> <p>Tenant service was running.</p> <p>Tenant1 was not available after the error.</p>	<p>When you try to delete tenants in a single rack small data center deployment configured with scale tenant config</p>	<p>Any CLI or REST tenant operations, and any fabric operations taking more than 15 minutes, will timeout at the client side. The operation completes in the background. Run the efa tenant show command to view the actual state of the operation.</p>

Known Limitations in Visibility Skill

Follow these caveats and limitations when using the Visibility Skill.

LAG created when port channel deployment fails

Any changes to ExtremeCloud Orchestrator configuration are reverted when a port channel deployment fails. However, a link aggregation group (LAG) is created on the device. The LAG is immediately deleted, but you can see the creation and deletion of a LAG in the device logs.

MLX UDA profile must be associated with an ingress group if the policy contains a UDA match

(MLX only) When you create an ingress group and associate it with an ingress policy, you must also associate the group with a UDA profile if the ingress policy contains a UDA match. For more information, see [ExtremeCloud Orchestrator GUI Admin Guide](#).

Firmware upgrade requires an absolute path to image locations

In the **Absolute Path** field, enter the complete file path to the location of the firmware image. The following are sample file paths for the various supported devices.

- Extreme 9920 (absolute path to the binary file): /root/NPB-21.2.1.0.bin
- SLX (absolute directory path where supported image files are located): /root/slxos18s.1.03/slxos18s.1.03a
- MLX (path to the manifest file): XMR-MLX/MLX_npb_06200_mnf.txt

For more information, see [ExtremeCloud Orchestrator GUI Admin Guide](#).

Device discovery

XCO deployed in packet broker mode supports device discovery notifications only for packet broker devices.

Listener policy byte count is incorrect when truncation is enabled

On the Extreme 9920 device, the byte count for truncated packets is the actual byte count seen by the egress ACL before truncation.

Defects Closed with Code Changes

The following defects were closed in ExtremeCloud Orchestrator 3.6.0.

Parent Defect ID:	XCO-4128	Issue ID:	XCO-4128
Product:	XCO – Visibility Skill	Reported in Release:	XCO 3.0.0
Symptom:	Port-channel partial configuration are present on device for SLX NPB devices		
Condition:	Port-channel configuration failed from UI, on device still the partial configuration is present.		
Workaround:	Make sure that all the configuration information are correctly populated from UI so that configuration will not fail on device.		
Recovery:	Login to SLX CLI and delete the given port channel and select refresh configuration on XCO UI from the device action list.		

Parent Defect ID:	XCO-4129	Issue ID:	XCO-4129
Product:	XCO – Visibility Skill	Reported in Release:	XCO 3.0.0
Symptom:	Disable of vn-tag header strip and enabling of 802.1BR header strip fails from XCO GUI for SLX NPB		
Condition:	When vn-tag header strip is enabled on an interface, disabling the vn-tag header strip and enabling the 802.1BR header strip in a single operation fails from XCO GUI.		
Workaround:	Disable the vn-tag header strip in first operation (save the port update) and then edit port again for enabling 802.1BR header strip option.		
Recovery:	N/A		

Parent Defect ID:	XCO-9844	Issue ID:	XCO-9844
Product:	XCO – Fabric Skill	Reported in Release:	XCO 3.3.1
Symptom:	The EPG created with a VRF containing duplicate static routes within the system. When another EPG is created using the same VRF, an error occurs due to a discrepancy between the device-configured static routes and those stored in the database. As the database should not contain duplicate static route entries for the VRF.		

Parent Defect ID:	XCO-9844	Issue ID:	XCO-9844
Condition:	Steps to reproduce: <ol style="list-style-type: none"> 1. Create VRF without any duplicate static routes. 2. Create EPG with the VRF. 3. Update VRF with duplicate static routes. 4. Create another EPG with same VRF. 		
Workaround:	Ensure that duplicate static routes are not provided when updating the VRF.		
Recovery:	Use the 'static-route-delete' operation to eliminate any duplicate static routes during the update of the VRF. Then, re-add the static routes using the 'static-route-add' operation, ensuring that no duplicates are present.		

Parent Defect ID:	XCO-9997	Issue ID:	XCO-9997
Product:	XCO – Fabric Skill	Reported in Release:	XCO 3.5.0
Symptom:	After successful reconciliation, the DRC status shown as "cfg-refreshed" when dynamic peer is drifted.,		
Condition:	<ol style="list-style-type: none"> 1. Dynamic Peers with both family IPv4 and IPv6 are created. 2. One of the address family dynamic peers is drifted. 3. After reconciling, other family dynamic peer is in cfg-refreshed. 		
Recovery:	The address-family which in "cfg-refreshed state", after reconcile, issue "no address-family" of VRF and once again issue the drift-reconcile command, the App State will be back in "cfg-in-sync" state.		

Parent Defect ID:	XCO-10050	Issue ID:	XCO-10050
Product:	XCO – Fabric Skill	Reported in Release:	XCO 3.3.1
Symptom:	Fabric devices are in cfg-refreshed state due to drift identified in interface description as part of events notification.		
Condition:	Users overwrite the description of the interface which is configured by fabric service.		
Recovery:	efa inventory device drift-reconcile --execute <ip> --reconcile		

Parent Defect ID:	XCO-10051	Issue ID:	XCO-10051
Product:	XCO – Fabric Skill	Reported in Release:	XCO 3.6.0
Symptom:	App-state for device shows cfg-refresh-error in 'efa fabric show'.		

Parent Defect ID:	XCO-10051	Issue ID:	XCO-10051
Condition:	The LLDP neighbor data is not added to the inventory database when length of chassis ID for a device is more than 50 characters.		
Workaround:	Modify the chassis name with less than 50 characters of length.		

Parent Defect ID:	XCO-10052	Issue ID:	XCO-10052
Product:	XCO – Fabric Skill	Reported in Release:	XCO 3.3.1
Symptom:	Fabric devices are in cfg-refreshed state due to drift identified in out of box peer-group configuration.		
Condition:	Users configure the peer-group on devices and mapped to the lowest neighbour Ip and without configure l2vpn properties includes (peer-as-check, encapsulation and next unchanged)		
Recovery:	Users configure the peer-group on devices and mapped to the highest compare with fabric configured neighbour Ip. neighbor 200.250.x.x peer_group <overlay>		

Parent Defect ID:	XCO-10093	Issue ID:	XCO-10093
Product:	XCO - Common	Reported in Release:	XCO 3.5.0
Symptom:	The firmware rollback is restricted with an error message "Firmware download for Device IP: 10.32.81.146 is not in uncommitted status" on 9920 devices		
Condition:	Firmware rollback triggered for 9920 devices		
Workaround:	Perform the firmware upgrade workflow with the intended firmware version of the rollback		

Parent Defect ID:	XCO-10102	Issue ID:	XCO-10102
Product:	XCO – Fabric Skill	Reported in Release:	XCO 3.3.1
Symptom:	Unable to update an EPG with a new port-channel due to an error related to MAC ACL		
Condition:	Unable to update an EPG with a new port-channel due to an error related to MAC ACL		

Parent Defect ID:	XCO-10105	Issue ID:	XCO-10105
	XCO – Visibility Skill	Reported in Release:	XCO 3.5.0

Parent Defect ID:	XCO-10105	Issue ID:	XCO-10105
Product:			
Symptom:	'gofaultmanager-service' went into crashLoopbackoff in visibility skill XCO setup		
Condition:	'gofaultmanager-service' went into crashLoopbackoff in visibility skill XCO setup		

Parent Defect ID:	XCO-10127	Issue ID:	XCO-10127
Product:	XCO – Fabric Skill	Reported in Release:	XCO 3.5.0
Symptom:	Standby node showing 'down' after node reboot		
Condition:	Trigger SLX reload using below command where the active XCO node is running and check the node status after reboot (when it becomes standby) echo c >/proc/sysrq-trigger		
Workaround:	N/A		
Recovery:	Reboot both active and standby nodes to recover from the situation		

Parent Defect ID:	XCO-10131	Issue ID:	XCO-10131
Product:	XCO – Fabric Skill	Reported in Release:	XCO 3.5.0
Symptom:	'efa inventory device firmware-download show' data is misaligned with the headings		
Condition:	'efa inventory device firmware-download show' data is misaligned with the headings		

Parent Defect ID:	XCO-10140	Issue ID:	XCO-10140
Product:	XCO – Fabric Skill	Reported in Release:	XCO 3.5.0
Symptom:	After 20-30 reloads of active node Standby showing Down		
Condition:	After 20-30 reloads of active node Standby showing Down		

Parent Defect ID:	XCO-10151	Issue ID:	XCO-10151
	XCO – Fabric Skill	Reported in Release:	XCO 3.5.0

Parent Defect ID:	XCO-10151	Issue ID:	XCO-10151
Product:			
Symptom:	DRC fails after reboot of spine hosting active EFA causing it to stay in MM		
Condition:	DRC fails after reboot of spine hosting active EFA causing it to stay in MM		

Parent Defect ID:	XCO-10160	Issue ID:	XCO-10160
Product:	XCO – Fabric Skill	Reported in Release:	XCO 3.5.0
Symptom:	efa inventory device threshold-monitor set should failed if value is -1		
Condition:	efa inventory device threshold-monitor set should failed if value is -1		

Parent Defect ID:	XCO-10171	Issue ID:	XCO-10171
Product:	XCO – Fabric Skill	Reported in Release:	XCO 3.2.1
Symptom:	Unable to create IPv6 prefix list with specific IPV6 IP addresses.		
Condition:	Unable to create IPv6 prefix list with specific IPV6 IP addresses.		

Parent Defect ID:	XCO-10177	Issue ID:	XCO-10177
Product:	XCO – Fabric Skill	Reported in Release:	XCO 3.5.0
Symptom:	Qos profile settings is missing for PO 64 (ICL Port-channel) after switch replacement (non-CLOS).		
Condition:	Qos profile settings is missing for PO 64 (ICL Port-channel) after switch replacement (non-CLOS)		

Parent Defect ID:	XCO-10184	Issue ID:	XCO-10184
Product:	XCO – Fabric Skill	Reported in Release:	XCO 3.1.2
Symptom:	XCO API request fail for IPV6 DHCP Relay		
Condition:	XCO API request fail for IPV6 DHCP Relay		

Open Defects

The following defects are open in ExtremeCloud Orchestrator 3.6.0.

Parent Defect ID:	XCO-8191	Issue ID:	XCO-8191
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 can fail with the following 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.		
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-9190	Issue ID:	XCO-9190
Product:	XCO - Common	Reported in Release:	XCO 3.3.0
Symptom:	VM GUI Library matches shows 2 devices when only 1 device is 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-9307	Issue ID:	XCO-9307
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-9307	Issue ID:	XCO-9307
Workaround:	N/A		
Recovery:	N/A		

Parent Defect ID:	XCO-9363	Issue ID:	XCO-9363
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:	XCO-9769
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:	Run the following CLI command: efa inventory device update --ip <>		

Parent Defect ID:	XCO-9942	Issue ID:	XCO-9942
Product:	XCO – Fabric Skill	Reported in Release:	XCO 3.5.0
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 run at the 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 run at the same time).		

Parent Defect ID:	XCO-9942	Issue ID:	XCO-9942
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-9983	Issue ID:	XCO-9983
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 or 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-10067	Issue ID:	XCO-10067
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 commands Bind Fabric internal ports QoS profile: efa policy qos profile bind --name <profile_name> --fabric <fabric_name> --port fabric-internal		

Parent Defect ID:	XCO-10073	Issue ID:	XCO-10073
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:	XCO-10073
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-10430	Issue ID:	XCO-10430
Product:	XCO - Common	Reported in Release:	XCO 3.6.0
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.		

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.