ExtremeCloud™ Orchestrator Release Notes

Version 3.5.0

9038090-00 Rev AA
April 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/

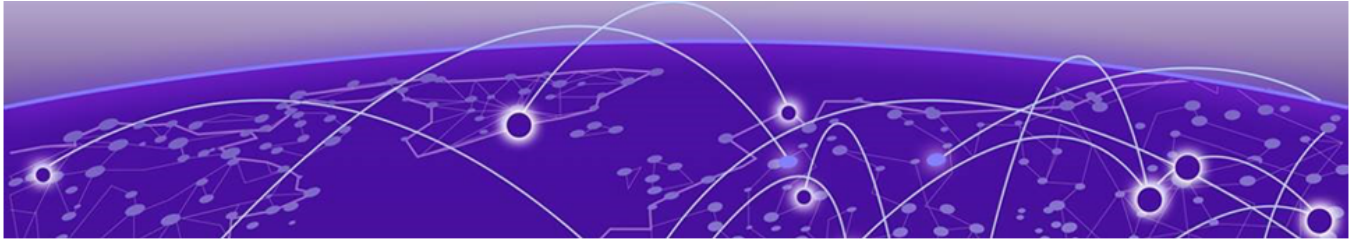
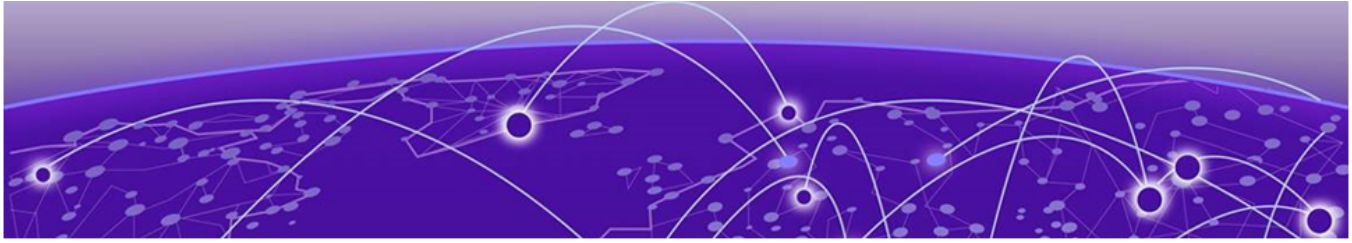


Table of Contents



Release Notes

New In This Release

ExtremeCloud Orchestrator 3.5.0 introduces the following features and resolves issues through defect fixes. For information about XCO deployment, refer to the *ExtremeCloud Orchestrator Deployment Guide, 3.5.0*.

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 or Disable Flooding for IP DHCP Relay	Added a new topic "Enable or Disable Flooding for IP DHCP Relay" that describes the procedure for enabling or disabling flooding for IP DHCP relay. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.5.0*.
Enable or Disable Suppress ARP and Neighbor Discovery (ND)	Added a new topic "Enable or Disable Suppress ARP and Neighbor Discovery (ND)" that describes the procedure for enabling or disabling suppress ARP and neighbor discovery. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.5.0*.

Table 1: Features and Improvements (continued)

Feature	Description
Firmware upgrade status	Added new topics "Firmware Upgrade Status", "User Action Fabric-Wide Firmware=Download (FWDL) History", and "Runtime (Operational) Status-based History" that describe fetching the fabric-wide firmware upgrade status using the CLI. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.5.0*.
License service	• Updated the topic "XCO License Service Management" with information on setting alerts on license expiry and deleting licenses. • Added a new topic "Delete a License" that describes procedure to delete a license. • Added a new topic "License Expiry Alert" that describes alerts when a license is expired. • Updated the topic "Inventory of Alerts" with License Alerts Inventory table. • Added a new topic "License Alerts" that describes alerts on License. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.5.0*.

Table 1: Features and Improvements (continued)

Feature	Description
Additional SNMP Notification Event support from SLX	• Modified the topic "Set Threshold Monitor Options" that describes procedure to set threshold monitor options. • Added a new topic "Additional Threshold Monitor Types" that describes additional threshold monitor entities. • Added a new topic "Re-worked Threshold Monitor Parameters" that describes threshold monitor parameters in XCO 3.5.0. • Added a new topic "CLI Migration" that describes which threshold Monitor settings will be migrated from the previous XCO releases. • Modified the topic "Unset Threshold Monitor Options" that describes procedure to unset threshold monitor options. • Modified the topic "Display Threshold Monitor Settings" that describes procedure to show threshold monitor settings. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.5.0*.
Password expiry notification enhancement	• Added a new topic "SLX Password Expiry Notification" which describes the process for configuring password expiry notification. • Updated the topic "Inventory of Alerts" the Password Expiry Alerts Inventory table. • Updated the topic "Alarm Inventory" with password expiration alarm. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.5.0*.
Galera certificate	Updated the topics "XCO Certificates" and "Galera Certificate" with the Galera certificate details. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.5.0*.

Table 1: Features and Improvements (continued)

Feature	Description
OVA DNS update	Updated the topic "Post OVA Install Procedure for Fabric and Visibility" with OVA DNS updates. For more information, refer to the *ExtremeCloud Orchestrator Deployment Guide, 3.5.0*.
CoreDNS forwarding	Added the topic "Avoiding CrashLoopBackOff State for CoreDNS" that describes enabling CoreDNS forwarding to avoid CrashLoopBackOff state. For more information, refer to the *ExtremeCloud Orchestrator Deployment Guide, 3.5.0*.
UI updates	• Bulk Edit Ports • Bi-directional Match Rule Configuration • Firmware History • 400G Line Card Support for 9920 Devices For more information, refer to the *ExtremeCloud Orchestrator GUI Administration Guide, 3.5.0*.

For other additional information, see Defects Closed with Code Changes on page 18.

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
3.2.x	More than 24	Yes	18.04 LTS and 20.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.3.x	More than 24	Yes	18.04 LTS and 20.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
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 3: OVA Deployment Models

XCO Version	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Virtual Machine
3.2.x	More than 24	Yes	18.04	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.3.x	More than 24	Yes	20.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB

Table 3: OVA Deployment Models (continued)

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 4: TPVM Deployment Models

XCO Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum SLX-OS Version
3.2.x	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820 (20.4.3 and later)	Up to 24	Yes	18.04	20.4.3
3.3.0	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820 (20.4.3 and later)	Up to 24	Yes	20.04 LTS	20.5.2
3.3.1	• 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 4: TPVM Deployment Models (continued)

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 5: TPVM Software Support

XCO Version	TPVM Version	SLX-OS Version
3.1.0	4.5.6	20.4.2a
3.1.1	4.5.8	20.4.3
3.2.0	4.5.10	20.4.3a
3.2.1	4.5.12	20.5.1
3.3.0	4.6.2	20.5.2
3.3.1	4.6.4	20.5.2a
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

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	✔	✔	✔		✔

Table 6: IP Fabric Topology Matrix (continued)

Device	SLX-OS Release	Leaf	Spine	Super Spine	Border Leaf	Small DC Fabric
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, Neutron, and SLX-OS Compatibility

XCO or EFA Version	Neutron Version	SLX-OS Version
2.5.4, 2.5.5	3.1.1-04	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
3.2.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
3.3.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 8: Ubuntu Server Version (continued)

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 9: OVA Deployment Models

XCO Version	Ubuntu Version	Virtual Machine
3.2.x	18.04	Minimum: • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.3.x	20.04 LTS	Minimum: • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB

Table 9: OVA Deployment Models (continued)

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 10: Supported Devices and Software

Device	Supported Software
Extreme 9920	Extreme 9920 software with the NPB application • 21.1.2.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.

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: 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.eyJjb21tb25fbmFtZSI6IkVGQSBUb2tlbiBTZXJ2aWNlIiwidWFzIjpbeyJ0YXJnZXQiOiJFRkEiLCJyb2xlIjoiVlIyLVRudEFkbWluIn1dLCJvcmciOiJFeHRyZW1lIE5ldHdvcmtzIiwidmVyIjoiMS4wIiwiaWQiOiIiLCJleHAiOjE2NDUyNDcxNDIsImp0aSI6IjZjMjA4ZDUxLTkwNzgtMTFlYy1iZjk5LWNhNzk1MDY1YzIwNyIsImlhdCI6MTY0NTE2MDc0MiwiaXNzIjoiRUZBIFRva2VuIFNlcnZpY2UiLCJuYmYiOjE2NDUxNjA3NDIsInN1YiI6InVzZXIyIn0.b7m5PINijeEdNSqnTeE2ZhUrqKLKQAu079vXyBIdgHbXKt9ULfa03vMU1jfBO1qFb1-x0oHmsAQ0pSsF5JLeMaMzMflLf78ktZO8U5IePq72vM5en35IR-DNLyoGIZBeFeG6ZbBMoETzz5vf9OuefgQID3YdjcALr7yllCgDmLVFlgson77yCBpkTK15xm

```
1GRbtL7JKXZzShBE7E3kdW7N71MdM85Gc3r4l-c8sfz7eo06gKrfTq9wXCv4_LVzR6-
KRSg6NyLq363WEpcK1A2Hs0Wo3T9TpquYHNaCWA5I1QTsG-
RHFdg4kxZP2fQpUp6Bgy1s6k59PVPn4-M-a8lA— Time Elapsed: 4.619465187s ——
```

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

Symptom	Condition	Workaround
Tenant2 delete is successful whereas deleting Tenant1 took more than 15 minutes and failed with the following message: Error : service is not available or internal server error has occurred, please try again later Tenant service was running. Tenant1 was not available after the error.	When you try to delete tenants in a single rack small data center deployment configured with scale tenant config	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.

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 3.5.0.

Defects Closed with Code Changes in ExtremeCloud Orchestrator 3.5.0

Parent Defect ID:	XCO-7899	Issue ID:	XCO-7899
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	BGP peer delete with MP-BGP support enabled for additional path advertise fails with netconf error - '%Error: 'additional-paths advertise' is configured, cannot remove 'additional-paths select' command'.		
Condition:	If the MP-BGP neighbor is associated to additional path select, then the deletion of the bgp neighbor fails with the following netconf error - '%Error: 'additional-paths advertise' is configured, cannot remove 'additional-paths select' command'		
Workaround:	There is no workaround for this issue.		
Recovery:	Run the peer delete command again and it gets deleted on the second attempt.		

Parent Defect ID:	XCO-8735	Issue ID:	XCO-8735
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	Inventory and device page shows different firmware version.		
Condition:	Post firmware upgrade, inventory and device page shows different firmware version.		
Workaround:	Post device discovery, device page shows correct firmware version.		

Parent Defect ID:	XCO-8829	Issue ID:	XCO-8829
Product:	XCO	Reported in Release:	XCO 3.2.1
Symptom:	New firmware-host registry fails when single quote is used in the password.		

Parent Defect ID:	XCO-8829	Issue ID:	XCO-8829
Condition:	Single quote is used in the password.		
Workaround:	Use the password without single quote.		

Parent Defect ID:	XCO-9137	Issue ID:	XCO-9137
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	EFA upgrade from release 2.7.2 to 3.3.0		
Condition:	DNS was removed before upgrade.		
Workaround:	DNS configuration should not be changed between upgrades.		
Recovery:	If DNS config is removed after upgrade to XCO 3.3.0, use update_dns.sh script to disallow DNS using following steps. 1. bash update-dns.sh --dns-action disallow 2. Get the core dns pod name using k3s kubectl get pods -n kube-system 3. Restart core dns pod using k3s kubectl delete pod <coredns pod name> -n kube-system 4. Wait for few mins or restart all XCO pods using the following commands: **sudo efactl stop** **sudo efactl start**		

Parent Defect ID:	XCO-9216	Issue ID:	XCO-9216
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	Multiple subscription on devices leads to memory leak.		
Condition:	Memory leak occurs when one of the devices is in unhealthy state.		

Parent Defect ID:	XCO-9284	Issue ID:	XCO-9284
Product:	XCO	Reported in Release:	XCO 3.4.0
Symptom:	Copy default-config to startup-config with maintenance mode enabled will remove all config including QoS policies on a device. Further, running DRC does not properly re-install all QoS configuration.		
Condition:	Copy default-config startup-config with maintenance mode enabled.		
Recovery:	Remove the device from inventory and then re-register the device.		

Parent Defect ID:	XCO-9291	Issue ID:	XCO-9291
	XCO	Reported in Release:	XCO 3.4.0

Parent Defect ID:	XCO-9291	Issue ID:	XCO-9291
Product:			
Symptom:	The fabric internal ports QoS profile is not getting applied on fabric internal ports when leaf devices are converted from single-homed to multi-homed by adding a new leaf device.		
Condition:	The fabric internal ports QoS profile is not getting applied on fabric internal ports when leaf devices are converted from single-homed to multi-homed by adding a new leaf device.		
Workaround:	User can issue unbind of fabric internal port QoS profile and rebind the fabric internal port QoS profile using the following commands: Unbind Fabric internal ports QoS profile: **efa policy qos profile unbind --name <profile_name> --fabric <fabric_name> --port fabric-internal** Bind Fabric internal ports QoS profile: **efa policy qos profile bind --name <profile_name> --fabric <fabric_name> --port fabric-internal**		
Recovery:	User can issue unbind of fabric internal port QoS profile and rebind the fabric internal port QoS profile using the following commands: Unbind Fabric internal ports QoS profile: **efa policy qos profile unbind --name <profile_name> --fabric <fabric_name> --port fabric-internal** Bind Fabric internal ports QoS profile: **efa policy qos profile bind --name <profile_name> --fabric <fabric_name> --port fabric-internal**		

Parent Defect ID:	XCO-9331	Issue ID:	XCO-9331
Product:	XCO	Reported in Release:	XCO 3.4.0
Symptom:	If a tenant interface level QoS profile binding exists on a port channel and the port channel is removed from the device using OOB (Out Of Band) triggering, DRC will not re-install the tenant level interface binding.		
Condition:	Removing a port channel from a device using OOB (Out of Band) triggers DRC.		

Parent Defect ID:	XCO-9331	Issue ID:	XCO-9331
Workaround:	When the port channel is restored by the DRC process on the device the user will need to re-apply/rebind the desired QoS profile on the tenant interface (port channel) using **efa policy qos profile bind --name <profile_name> --tenant <tenant_name> --po <port channel ID>**		
Recovery:	When the port channel is restored by the DRC process on the device the user will need to re-apply/rebind the desired QoS profile on the tenant interface (port channel) using **efa policy qos profile bind --name <profile_name> --tenant <tenant_name> --po <port channel ID>**		

Parent Defect ID:	XCO-9336	Issue ID:	XCO-9336
Product:	XCO	Reported in Release:	XCO 3.4.0
Symptom:	Inventory device delete is not removing QoS config on the spine device.		
Condition:	Device deletion from inventory which has QoS configuration.		
Workaround:	User needs to unbind the policies (QoS) from all the relevant targets (fabric/tenant/port/po) before running the inventory device delete.		
Recovery:	User needs to unbind the policies (QoS) from all the relevant targets (fabric/tenant/port/po). After this, the user needs to delete the leftover QoS configuration from SLX.		

Parent Defect ID:	XCO-9362	Issue ID:	XCO-9362
Product:	XCO	Reported in Release:	XCO 3.4.0
Symptom:	The fabric internal ports QoS profile is not getting applied on intended ports: 1. When a new device is being added to CLOS fabric and fabric is configured. 2. When a new rack is added to non-CLOS fabric and fabric is configured.		
Condition:	Pre-condition: Fabric internal ports QoS profile is already applied on a fabric (CLOS or non-CLOS). Issue will be seen: 1. When a new device is being added to CLOS fabric and fabric is configured. 2. When a new rack is added to non-CLOS fabric and fabric is configured.		

Parent Defect ID:	XCO-9362	Issue ID:	XCO-9362
Workaround:	User can issue unbind of fabric internal port QoS profile and rebind the fabric internal port QoS profile using the following commands: Unbind Fabric internal QoS profile: **efa policy qos profile unbind --name <profile_name> --fabric <fabric_name> --port fabric-internal** Bind Fabric internal QoS profile: **efa policy qos profile bind --name <profile_name> --fabric <fabric_name> --port fabric-internal**		
Recovery:	User can issue unbind of fabric internal port QoS profile and rebind the fabric internal port QoS profile using the following commands: Unbind Fabric internal QoS profile: **efa policy qos profile unbind --name <profile_name> --fabric <fabric_name> --port fabric-internal** Bind Fabric internal QoS profile: **efa policy qos profile bind --name <profile_name> --fabric <fabric_name> --port fabric-internal**		

Parent Defect ID:	XCO-9381	Issue ID:	XCO-9381
Product:	XCO	Reported in Release:	XCO 2.7.2
Symptom:	9740 devices with breakout port configured, DRC fails for even numbered port.		
Condition:	If XCO is upgraded from previous version to 3.2.0 version.		
Workaround:	Perform fresh install followed by reconfiguration of breakout ports and its respective configuration.		

Parent Defect ID:	XCO-9420	Issue ID:	XCO-9420
Product:	XCO	Reported in Release:	XCO 3.3.1
Symptom:	When standby TPVM is down, 'efa health show' shows the status as 'Red'.		
Condition:	When standby TPVM is down, 'efa health show' status must be 'Orange'.		
Workaround:	N/A		
Recovery:	N/A		

Parent Defect ID:	XCO-9659	Issue ID:	XCO-9659
Product:	XCO	Reported in Release:	XCO 3.4.0
Symptom:	Duplicate qos-profile entries listed in "efa policy qos-profile list" command		

Parent Defect ID:	XCO-9659	Issue ID:	XCO-9659
Condition:	•Create Qos-profile efa policy qos map create --type dscp-tc-map --name qosMapPort2 --rule "dscp[20],tc[2],dp[2]" efa policy qos service-policy-map create --name servicePolicyPort --rule "strict-priority[5],dwrr[0;0;100],class[default]" efa policy qos profile create --name profile2 --trust dscp --dscp-tc qosMapPort2 --service-policy "name[servicePolicyPort],dir[out]" •Create Tenant efa tenant create --name "vpod01" --type private --vlan-range 100 --vrf-count 0 --port 10.20.48.110[0/4] •Attach the qos-profile to Tenant efa policy qos profile bind --name profile2 --tenant vpod01 •List the qos-profile to make sure binding exist at Tenant level efa policy qos profile list --ip 10.20.48.110 --interface "Ethernet 0/4" •Now add the same port to the Tenant again efa tenant update --operation=port-add --port 10.20.48.110[0/4] --name vpod01 •Now check qos-profile list whether duplicate entry is listed efa policy qos profile list --ip 10.20.48.110 --interface "Ethernet 0/4"		
Workaround:	Avoid adding same port to Tenant when already exist		
Recovery:	Detach qos-profile from Tenant and Re-attach it again		

Parent Defect ID:	XCO-9664	Issue ID:	XCO-9664
Product:	XCO	Reported in Release:	XCO 3.3.1
Symptom:	During XCO upgrade on fabric with mct nodes, database restore resulted in bringing down port-channel 64 with sudden impact on mct cluster.		
Condition:	1. Create a CLOS or Non-CLOS fabric with atleast one leaf node pairs (i.e. MCT pair) 2. Have only two icl links between the mct pair and connect these interfaces in criss-cross fashion i.e. 0/55 to 0/56 and 0/56 to 0/55 and configure fabric. 3. Take a database backup with above scenario and change the criss-cross links to normal links i.e. 0/55 to 0/55 and 0/56 to 0/56 followed by fabric configure. 4. While upgrading XCO, apply the database backup created during criss-cross links and do DRC before fabric configure. 5. With above database restore in one of old releases, stale entries were persisted into database for criss-cross even though the mistake was rectified and changed to direct links. 6. Restore the database with stale entries for next XCO upgrade.		

Parent Defect ID:	XCO-9664	Issue ID:	XCO-9664
Workaround:	In case of criss-coss connection with restore case, with out DRC execute efa fabric configure to have correct entries populated and old entries to be removed.		
Recovery:	Remove stale entries in database manually and execute fabric configure to restore PO64 up.		

Parent Defect ID:	XCO-9753	Issue ID:	XCO-9753
Product:	XCO	Reported in Release:	XCO 3.3.1
Symptom:	Ping-target configuration is missing in “efa version” output.		
Condition:	Trigger "efa version" in multi-node setup when ping-target is already configured.		
Workaround:	Refer to the /apps/etc/efa/efa.conf file which holds the configured ping targets details. EFA_DEPLOYMENT_PING_TARGET_ENABLED=yes EFA_DEPLOYMENT_HA_HEALTH_CHECK_IPS=<List of IP addresses>		

Parent Defect ID:	XCO-9772	Issue ID:	XCO-9772
Product:	XCO	Reported in Release:	XCO 3.4.1
Symptom:	EFA policy route-map-match delete option allows for non-existing matches for community-list. It supposed to deny the command with a does not exist error.		
Condition:	Use non-existing community-list name while deleting the matches using EFA policy route-map-match delete option.		
Workaround:	Use correct community-list name while deleting the matches using EFA policy route-map-match delete option.		
Recovery:	N/A		

Parent Defect ID:	XCO-9794	Issue ID:	XCO-9794
Product:	XCO	Reported in Release:	XCO 3.3.1
Symptom:	JWT certificate renewal fails after XCO upgrade.		

Parent Defect ID:	XCO-9794	Issue ID:	XCO-9794
Condition:	Kustomization YAML files were not copied to the installation directory after upgrade. These files are needed for certificate generation.		
Workaround:	Move the "kustomization.yaml" files to the correct locations as shown below: SERVER: /opt/efa/certs/cert /opt/efa/certs/key TPVM: /apps/efa/certs/cert /apps/efa/certs/key		

Parent Defect ID:	XCO-10000	Issue ID:	XCO-10000
Product:	XCO	Reported in Release:	XCO 3.4.1
Symptom:	Binding QosProfile to Pport-channel ID applies to all port-channels when more than one port-channel is using the same identical port-channel ID.		
Condition:	No option to bind QosProfile to specific port-channel name when more than one port-channel is using the same identical port-channel ID.		
Workaround:	Use unique Po ID for each port-channel to ensure that QosProfile binding to Po ID will not overlap with each other.		
Recovery:	N/A		

Defects Closed without Code Changes

No defects were closed without code changes in ExtremeCloud Orchestrator 3.5.0.

Parent Defect ID:	XCO-6964	Issue ID:	XCO-6964
Reason Code:	Already implemented		
Product:	XCO	Reported in Release:	XCO 3.2.0
Symptom:	Upgrade was successful but a failed message displays at the end of upgrade. message is "Status: Failed"		
Condition:	Upgrade XCO with latest build. Issue is seen only on customer setup.		

Parent Defect ID:	XCO-9178	Issue ID:	XCO-9178
Reason Code:	Not reproducible		
Product:	XCO	Reported in Release:	XCO 3.4.0
Symptom:	When a device is removed from fabric which has QoS configuration, not all QoS configuration is removed from the device and EFA.		
Condition:	Device is deleted from fabric		
Workaround:	User needs to unbind the policies (QoS) from all the relevant targets (fabric/tenant/port/po) before executing the fabric device delete to avoid the stale policies (QoS) in the system.		

Parent Defect ID:	XCO-9195	Issue ID:	XCO-9195
Reason Code:	Working as designed		
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	XCO 3.3.0 VM GUI won't allow library copy for matches.		
Condition:	Go to the Library page using the XCO GUI and try to make a copy using the edit option.		

Parent Defect ID:	XCO-9217	Issue ID:	XCO-9217
Reason Code:	Already implemented		
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	CLI for "efactl restart" throwing retrying and failed messages on customer setup only.		
Condition:	Run the CLI "efactl restart" command on GTAC setup and user can see the failed pop-up trace even those pods restart completed successfully.		

Parent Defect ID:	XCO-9224	Issue ID:	XCO-9224
Reason Code:	Design limitation		
Product:	XCO	Reported in Release:	XCO 3.4.0
Symptom:	QoS application is not taking place after changing interface switch port modes or changing the interface from L2 to L3 or vice-a-versa through OOB (out of band) means.		
Condition:	Modifying the switchport mode followed by executing auto DRC.		
Recovery:	Remove all OOB Interface configuration and restore the configuration to the original EFA configured values and re-run DRC.		

Parent Defect ID:	XCO-9341	Issue ID:	XCO-9341
Reason Code:	Insufficient Information		
Product:	XCO	Reported in Release:	XCO 3.2.1
Symptom:	App state for one of the border leaf shows 'cfg-refresh-error'.		
Condition:	Due to some reason if mariadb restarts on active XCO node, "Error : dial tcp <xco-ip>:3306: connect: connection refused; invalid transaction; invalid transaction" is seen for 'efa fabric show' command. After db connection is successful, the app state for one of the border leaf shows 'cfg-refresh-error'.		
Recovery:	To update the app-state for the device, use the following recovery steps: 1. On SLX: shut MCT ports. 2. On XCO: efa inventory device update –ip <device-ip> 3. On SLX:, no shut MCT ports 4. On XCO: efa inventory device update –ip <device-ip>		

Parent Defect ID:	XCO-9354	Issue ID:	XCO-9354
Reason Code:	Feature or function is not supported		
Product:	XCO	Reported in Release:	XCO 3.3.1
Symptom:	Threshold monitor configuration for monitor types (lif, bfd-session, vxlan-tunnel, mac-table) failed when we configure thru XCO to SLX device (starting from SLX version - 20.5.3).		
Condition:	Use XCO 3.3.1 and SLX version 20.5.3 and try below cases, 1. Set monitor threshold for lif, bfd-session, vxlan-tunnel, mac-table thru XCO failed only when we use count/interval fields. 2. Unset monitor threshold for lif, bfd-session, vxlan-tunnel, mac-table thru XCO failed. Here Unset logic tries to clear all fields including count/interval fields by default.		
Workaround:	1. Set monitor threshold for types lif, bfd-session, vxlan-tunnel, & mac-table thru XCO without count/interval fields. 2. Unset can't be done by XCO. Instead it can be unset directly in SLX using the following commands: **`no threshold-monitor <monitor-type>`** Or use XCO 3.3.1 with SLX version 20.5.2a for functioning without any issues.		

Open Defects

There following defects are open in ExtremeCloud Orchestrator 3.5.0.

Parent Defect ID:	XCO-3445	Issue ID:	XCO-3445
Product:	XCO	Reported in Release:	EFA 3.0.0
Symptom:	DRC will not identify the drift and hence will not reconcile the drifted configuration		
Condition:	Below are the steps to reproduce the issue: 1. Configure multi rack Non-CLOS fabric. 2. Manually remove the below set of configurations on device under router-bgp no neighbor 172.x.x.x password xxxx no neighbor 172.x.x.x update-source loopback 1 no neighbor 172.x.x.x peer-group overlay-ebgp-group address-family l2vpn evpn no retain route-target all 3. Execute "efa inventory drift-reconcile execute --ip <device-ip>"		
Recovery:	Manually reconfigure the removed configurations from the device		

Parent Defect ID:	XCO-3471	Issue ID:	XCO-3471
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	Stale BGP Peer-group entry configured under router BGP on SLX Border leaf and Spine devices with none of the BGP neighbors linked with the Peer group.		
Condition:	1. Create a 3-stage CLOS fabric, add devices with MCT leaf, spine, and border-leaf and configure the fabric 2. Convert the 3-stage CLOS fabric to a 5-stage CLOS fabric using the fabric migrate command "efa fabric migrate --type "3-to-5-stage" --source-fabric <source-fabric> --destination-3-stage-leaf-spine-pod <pod-name> --destination-3-stage-border-leaf-pod <pod-name>" 3. Add super-spine POD devices to the migrated 5-stage CLOS fabric 4. Disconnect the BorderLeaf to Spine links and reconnect the BorderLeaf to Super-Spine links 5. Configure the migrated 5-stage CLOS fabric		
Recovery:	Manually delete the stale BGP peer-groups from both the Border Leaf and Spine devices		

Parent Defect ID:	XCO-8191	Issue ID:	XCO-8191
Product:	XCO	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.		
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-8550	Issue ID:	XCO-8550
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	IPV6 deployment failing with default GW errors even IPv6 XCO server can reach to default Gateway.		
Condition:	IPv6 deployment is failed in below condition. Failed condition- default proto static metric 1024 nexthop via 2600:3c01:e000:e2::2 dev eth0 weight 1 expecting the below pattern - fe80::/64 dev veth0a9acd23 proto kernel metric 256 pref medium default via 2620:100:c:e085:20c:29ff:fee1:3ec1 dev ens160 metric 1024 pref medium		
Workaround:	User has to add the default route using below command- sudo ip -6 route add default via <IPv6 address of default gw> dev <exit interface> example: sudo ip -6 route add default via fc00::5:204:96ff:fed6:f288 dev eth0		

Parent Defect ID:	XCO-9190	Issue ID:	XCO-9190
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	VM GUI Library matches shows 2 devices when only 1 device discovered.		
Condition:	Remove all the devices and discover only one device.		

Parent Defect ID:	XCO-9307	Issue ID:	XCO-9307
Product:	XCO	Reported in Release:	XCO 3.4.0
Symptom:	After the upgrade from 3.4.2 to 3.5.0, removing all the configuration from XCO devices and restoring the 3.4.2 backup followed by manual DRC failed to push the configurations to the devices.		
Condition:	After the upgrade from 3.4.2 to 3.5.0, when the user removes the configurations, back and restore followed by manual DRC failed to push the configurations to the devices. However, backup and restore function works fine right after the upgrade without removing the configurations.		
Workaround:	No		
Recovery:	No		

Parent Defect ID:	XCO-9363	Issue ID:	XCO-9363
Product:	XCO	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-9844	Issue ID:	XCO-9844
Product:	XCO	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: 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 the 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-9942	Issue ID:	XCO-9942
Product:	XCO	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]		
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-9997	Issue ID:	XCO-9997
Product:	XCO	Reported in Release:	XCO 3.5.0
Symptom:	After successful reconciliation, the DRC status shown as "cfg-refreshed" when dynamic peer is drifted.,		

Parent Defect ID:	XCO-9997	Issue ID:	XCO-9997
Condition:	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, please 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	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	Reported in Release:	XCO 3.6.0
Symptom:	App-state for device shows cfg-refresh-error in 'efa fabric show'.		
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	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-10067	Issue ID:	XCO-10067
	XCO	Reported in Release:	XCO 3.5.0

Parent Defect ID:	XCO-10067	Issue ID:	XCO-10067
Product:			
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 the following 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 the following 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-10069	Issue ID:	XCO-10069
Product:	XCO	Reported in Release:	XCO 3.5.0
Symptom:	Fabric devices are in cfg-refreshed state due to LLDP Link down (LD) event.		
Condition:	LD event is triggered		
Recovery:	Configure fabric using CLI "efa fabric configure –name <fabric_name> "		

Parent Defect ID:	XCO-10073	Issue ID:	XCO-10073
Product:	XCO	Reported in Release:	XCO 3.5.0
Symptom:	Statistics and Syslog are not displayed or updated in XCO device overview and view logs pages respectively.		
Condition:	When SLX (9140/9240) device is discovered with IPv6 address.		
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-10093	Issue ID:	XCO-10093
Product:	XCO	Reported in Release:	XCO 3.5.0
Symptom:	The firmware rollback is restricted with an error message "Firmware download for Device IP is not in uncommitted status" on 9920 devices		

Parent Defect ID:	XCO-10093	Issue ID:	XCO-10093
Condition:	Firmware rollback triggered for 9920 devices		
Workaround:	Perform the firmware upgrade using firmware host with the intended firmware version of the rollback.		
Recovery:	None		

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.