ExtremeCloud™ Orchestrator Release Notes

Version 3.3.0

9037864-00 Rev AB
January 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: www.extremenetworks.com/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/

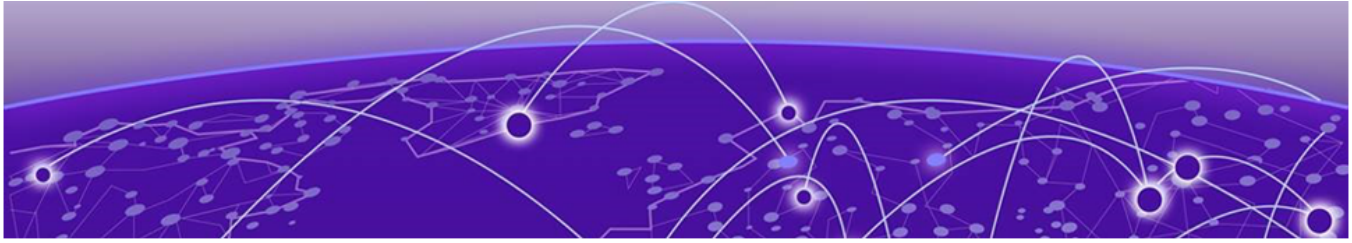
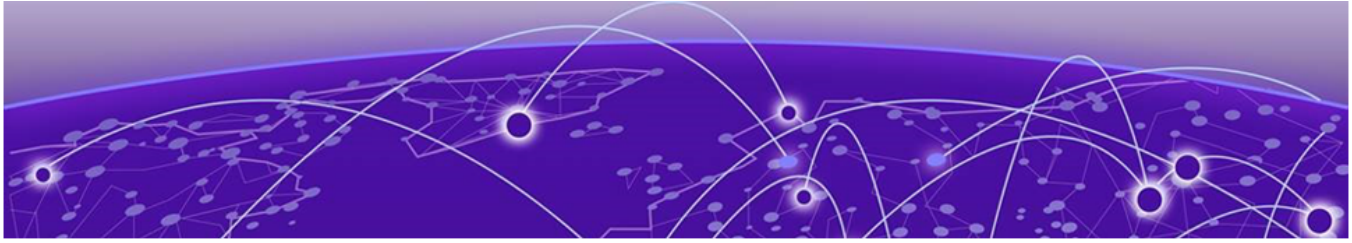


Table of Contents



Release Notes

New In This Release

ExtremeCloud Orchestrator 3.3.0 provides several new features and improvements. For information about XCO deployment, refer to the *ExtremeCloud Orchestrator Deployment Guide, 3.3.0*.

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
Fabric Service Enhancements	View Device Error in Clos and Non-Clos Fabric describes the process to view device errors. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.3.0*.
	Router ID and VTEP Loopback IP Allocation in Clos and Non-Clos Fabric describes the IP allocation scheme for Router ID and VTEP Loopback process to allocate IP to Router ID and VTEP Loopback IP. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.3.0*.
	Allocate IP using Uniform Granular Scheme and Allocate IP using Uniform Loopback Scheme describe the IP allocation scheme for Router ID and VTEP Loopback. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.3.0*.
	Static ICL in Small Data Center describes the static ICL in small data center. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.3.0*.
	Configure Static and Dynamic ICL describes the static ICL in small data center. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.3.0*.
	Dynamic ICL to Static ICL Conversion describes the static ICL in small data center. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.3.0*.
	Static ICL to Dynamic ICL Conversion describes the static ICL in small data center. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.3.0*.
Health support for fabric service	Fabric Health Alerts For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.3.0*.
	Inventory of Alerts updated with fabric health alerts. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.3.0*.
	Alarms Commands update. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.3.0*.
	Alarm Inventory update. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.3.0*.
Manage SLX IP options	Disable IP Option For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.3.0*.

Table 1: Features and Improvements (continued)

Feature	Description
Multi Protocol BGP configuration	Multi Protocol BGP details on static and dynamic peer. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.3.0*.
	Configure Multi Protocol BGP on Tenant Static BGP Peer describes multi protocol BGP configuration. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.3.0*.
Infra and deployment enhancements	Updated the "Non-Interactive Mode" and "Single CLI on Server for Single Node" topics with more options of source deployment. sh script. For more information, refer to the *ExtremeCloud Orchestrator Deployment Guide, 3.3.0*.
Support update	Updated the support matrices for XCO 3.3.0 supported platforms and deployment models. For more information, refer to the *ExtremeCloud Orchestrator Deployment Guide, 3.3.0*.
TPVM 4.6.0 (Ubuntu 20.04) support	Updated the "Upgrade Ubuntu on the XCO Host - Single Node or Multi Node" topic for the latest Ubuntu version. For more information, refer to the *ExtremeCloud Orchestrator Deployment Guide, 3.3.0*.
Update password for TPVM assessments	Procedure to update password for Extreme user on TPVM assessments. For more information, refer to the *ExtremeCloud Orchestrator Security Guide, 3.3.0*.
TPVM and CIS-CAT updates	Changes to TPVM and CIS-CAT assessor versions for system hardening assessments. For more information, refer to the *ExtremeCloud Orchestrator Security Guide, 3.3.0*.
Security hardening updates	Security hardening script for Ubuntu Linux host servers. For more information, refer to the *ExtremeCloud Orchestrator Security Guide, 3.3.0*.
UI enhancements	The ExtremeCloud Orchestrator GUI has the following updates: • Locations map view to show multiple locations • Fabric device attributes • Firmware upgrade procedure For more information, refer to the *ExtremeCloud Orchestrator GUI Administration Guide, 3.3.0*.

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
3.1.x	More than 24	Yes	16.04, 18.04, and 20.04	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.2.x	More than 24	Yes	18.04 and 20.04	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.3.0	More than 24	Yes	18.04 and 20.04	• 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
3.1.x	More than 24	Yes	18.04	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.2.x	More than 24	Yes	18.04	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.3.0	More than 24	Yes	20.04 LTS	• 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
3.1.x	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820 (20.4.3 and later)	Up to 24	Yes	18.04	20.4.2
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

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

Table 5: TPVM Software Support (continued)

XCO Version	TPVM Version	SLX-OS Version
3.2.1	4.5.12	20.5.1
3.3.0	4.6.2	20.5.2

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, 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
3.1.x	18.04 and 20.04	Minimum: • CPU: 4 cores • Storage: 128 GB • RAM: 8 GB Recommended: • CPU: 16 cores • Storage: 200 GB • RAM: 32 GB
3.2.x	18.04 and 20.04	Minimum: • CPU: 4 cores • Storage: 128 GB • RAM: 8 GB Recommended: • CPU: 16 cores • Storage: 200 GB • RAM: 32 GB
3.3.0	18.04 and 20.04	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
3.1.x	18.04	Minimum: • CPU: 4 cores

Table 9: OVA Deployment Models (continued)

XCO Version	Ubuntu Version	Virtual Machine
		• Storage: 64 GB • RAM: 8 GB
3.2.x	18.04	Minimum: • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.3.0	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.

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 nit 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 a **`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.

EFA Token command message

Please type this in your shell:

```
export
EFA_TOKEN=eyJhbGciOiJSUzI1NiIsImtpZCI6IjEuMCIsInR5cCI6IkpXVCJ9.eyJjb21tb
25fbmFtZSI6IkVGQSBUb2tlbiBTZXJ2aWNlIiwidWFzIjpbeyJ0YXJnZXQiOiJFRkEiLCJyb
2xlIjoiVlIyLVRudEFkbWluIn1dLCJvcmciOiJFeHRyZW1lIE5ldHdvcmtzIiwidmVyIjoiM
S4wIiwiaWQiOiIiLCJleHAiOjE2NDUyNDcxNDIsImp0aSI6IjZjMjA4ZDUxLTkwNzgtMTFlY
y1iZjk5LWNhNzk1MDY1YzIwNyIsImlhdCI6MTY0NTE2MDc0MiwiaXNzIjoiRUZBIFRva2VuI
FNlcnZpY2UiLCJuYmYiOjE2NDUxNjA3NDIsInN1YiI6InVzZXIyIn0.b7m5PINijeEdNSqnT
eE2ZhUrqKLKQAu079vXyBIdgHbXKt9ULfa03vMU1jfBO1qFb1-
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/TierraOS--NPB.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 resolved in ExtremeCloud Orchestrator 3.3.0.

Parent Defect ID:	XCO-3458	Issue ID:	XCO-3458
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	Port breakout fails for SLX devices with "generic message error". On device new split ports are created.		
Recovery:	Login to SLX CLI and remove the breakout of port using the following steps: Run following commands: configuration terminal hardware connector <slot/interface> breakout mode <4x10g/4x25g> no breakout e.g. if the port 0/50 got this issue, following are the commands to run after login to CLI Freedom7-Bng# configure t Entering configuration mode terminal Freedom7-Bng(config)# hardware Freedom7-Bng(config-hardware)# connector 0/50 Freedom7-Bng(config-connector-0/50)# breakout mode 4x10 Freedom7-Bng(config-connector-0/50)# no breakout		

Parent Defect ID:	XCO-3472	Issue ID:	XCO-3472
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	XCO IP/VIP change is not updated on device for telemetry/streaming and syslog		
Condition:	Once XCO is installed and devices are discovered in Visibility installation, if the XCO node IP/VIP changes, those are not updated on device for receiving the statistics and syslog.		
Workaround:	Change XCO's IP/VIP before discovering the devices.		
Recovery:	Required to delete and add all devices again after the IP/VIP of XCO is changed.		

Parent Defect ID:	XCO-4180	Issue ID:	XCO-4180
Product:	XCO	Reported in Release:	EFA 3.0.0
Symptom:	Http Login/Logout Raslogs repeatedly observed on device side, after CLI execution.		
Condition:	During Ntp create/delete operation, few repeated logs are observed on device.		

Parent Defect ID:	XCO-4180	Issue ID:	XCO-4180
Workaround:	On device side we can configure Raslog to suppress/Ignore logs. logging raslog message SEC-1206 suppress //to supress logging raslog console CRITICAL //to discard other types and show only critical		
Recovery:	It is a non-functional issue and has no impact on the overall system operations.		

Parent Defect ID:	XCO-5931	Issue ID:	XCO-5931
Product:	XCO	Reported in Release:	EFA 3.0.1
Symptom:	Firmware Not Committed" but "Firmware Download Show Overall Status" shows "Device Update In Progress		
Condition:	For the firmware download workflow, it will perform the FWDL on each device as prescribed by the grouping and then finally do a "quick" device update (device links only) for all devices that have participated in the FWDL. The purpose of the device links only update is to ensure the fabric configurations are in-sync after the FWDL workflow has completed since devices were rebooted to activate the new firmware. In this customer case they only did a FWDL of a single device, but the workflow is the same... a device links only update will be performed at the end. The firmware download show command contains the individual device's status in the table and the "Overall Status" at the bottom reflects EFA's overall status of the FWDL workflow which includes the Device links only update.		
Workaround:	The user must poll for the Overall Status Completion to proceed for another FWDL workflow prepare/execute.		
Recovery:	Not applicable.		

Parent Defect ID:	XCO-6192	Issue ID:	XCO-6192
Product:	XCO	Reported in Release:	EFA 3.0.0
Symptom:	Unable to login to XCO.		

Parent Defect ID:	XCO-6429	Issue ID:	XCO-6429
Product:	XCO	Reported in Release:	EFA 3.1.1
Symptom:	ACL hits displayed on stats table while it should maintain its position during stats update		

Parent Defect ID:	XCO-6429	Issue ID:	XCO-6429
Condition:	ACL hits dynamically keep moving around and it can't track of hits.		
Workaround:	Sequence number is implemented and rest of the things will be fixed in next release.		

Parent Defect ID:	XCO-6466	Issue ID:	XCO-6466
Product:	XCO	Reported in Release:	EFA 3.1.1
Symptom:	Full IPv4/IPv6 address are not seen for policy rules.		
Condition:	When user launch troubleshoot and monitor page to select the rules.		
Workaround:	Mouse over tip is provided so that user can get the complete address.		
Recovery:	NA		

Parent Defect ID:	XCO-6510	Issue ID:	XCO-6510
Product:	XCO	Reported in Release:	XCO 3.2.0
Symptom:	The "Network Essentials" option is listed as a device action for the NPB device and a blank page is opened when the user clicks on that.		
Condition:	NPB device is discovered in XCO and user clicks on the device action (for the NPB device) from the inventory page.		
Workaround:	Do not select the networks essentials for NPB devices from device inventory page.		

Parent Defect ID:	XCO-6629	Issue ID:	XCO-6629
Product:	XCO	Reported in Release:	XCO 3.2.0
Symptom:	Cannot scroll to see more than 37 rows while in troubleshooting/ monitor in XCO Packet skill version 3.2.0.		

Parent Defect ID:	XCO-6792	Issue ID:	XCO-6792
Product:	XCO	Reported in Release:	XCO 3.2.0
Symptom:	XCO doesn't recover after OOB management network failure simulation - double fault testing		

Parent Defect ID:	XCO-6937	Issue ID:	XCO-6937
	XCO	Reported in Release:	XCO 3.2.0

Parent Defect ID:	XCO-6937	Issue ID:	XCO-6937
Product:			
Symptom:	Monitor/Troubleshooting page, could not scroll through tables to view an entire table		

Parent Defect ID:	XCO-6950	Issue ID:	XCO-6950
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	[Packet Broker] 9920 - The 'Interface Name' field on the Ingress Policy Stats Table does not appear to be working. No information available!		

Parent Defect ID:	XCO-7097	Issue ID:	XCO-7097
Product:	XCO	Reported in Release:	XCO 3.2.0
Symptom:	XCO 3.2.0 inventory-service crashing during ‘efa fabric device add-bulk’		

Parent Defect ID:	XCO-7223	Issue ID:	XCO-7223
Product:	XCO	Reported in Release:	EFA 3.0.1
Symptom:	After upgrade, SLX 9250 Spine2 stuck in failed state when executed "efa inventory drift-reconcile".		

Parent Defect ID:	XCO-7345	Issue ID:	XCO-7345
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	insecuretls flags in XCO-3.1.0, it sets the value to true by default and by setting “–insecuretls false”.		

Parent Defect ID:	XCO-7718	Issue ID:	XCO-7718
Product:	XCO	Reported in Release:	EFA 2.7.2
Symptom:	drifted configuration on EFA is still showing as drifted after tenant drift reconcile		

Parent Defect ID:	XCO-7797	Issue ID:	XCO-7797
Product:	XCO	Reported in Release:	XCO 3.2.1
Symptom:	Certificate expiry notification persists after renewal.		

Defects Closed without Code Changes

The following defects were closed without code changes in ExtremeCloud Orchestrator 3.3.0.

Parent Defect ID:	XCO-3438	Issue ID:	XCO-3438
Reason Code:	Cannot Fix		
Product:	XCO	Reported in Release:	EFA 2.7.0
Symptom:	When endpoint group create or update operation REST requests of multiple endpoint groups each with 50+ ctags are issued concurrently, one or two of the requests can fail with "Error 1452: Cannot add or update a child row: a foreign key constraint fails" or with an error indicating database timeout or an error indicating failure of network property delete.		
Condition:	When multiple endpoint group requests are processed concurrently, some of the database requests initiated by EFA can cause database to end one of the request with the above mentioned error		
Workaround:	Execute the commands sequentially		
Recovery:	EFA database and SLX device configurations are always not affected by this error and hence no recovery is required. The failed commands shall be rerun sequentially to successful completion of the expected operations		

Parent Defect ID:	XCO-5171	Issue ID:	XCO-5171
Reason Code:	Not Reproducible		
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	EFA status takes longer time to settle after SLX power cycle.		

Parent Defect ID:	XCO-5235	Issue ID:	XCO-5235
Reason Code:	Already Implemented		
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	High Memory utilization by litestream process		
Condition:	Condition not known.		

Parent Defect ID:	XCO-5235	Issue ID:	XCO-5235
Workaround:	Not Applicable		
Recovery:	Following steps need to be followed. 1. Check for litestream process on active using ps aux | grep litestream 2. Use following command to restart. systemctl restart litestream.		

Parent Defect ID:	XCO-5795	Issue ID:	XCO-5795
Reason Code:	Insufficient Information		
Product:	XCO	Reported in Release:	XCO 3.2.0
Symptom:	The data in the previous page has the ethernet interfaces as well as other interfaces even though the page is supposed to contain only the Ethernet interfaces		
Condition:	Below are the steps to reproduce the issue: 1. In the XCO GUI Device Inventory view, the user selects the "Network Essentials" options from the row action menu. 2. The user navigates to page next page 2. And then comes back to the previous page		

Parent Defect ID:	XCO-6464	Issue ID:	XCO-6464
Reason Code:	Already Implemented		
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	DC_APP_Events_Q_Notification messages stacking up causing Disk Space issues in RabbitMQ directory		

Parent Defect ID:	XCO-6465	Issue ID:	XCO-6465
Reason Code:	Already Implemented		
Product:	XCO	Reported in Release:	EFA 3.1.1
Symptom:	Pods from Active node of EFA went down and recovered after some time.		

Parent Defect ID:	XCO-6468	Issue ID:	XCO-6468
	Not Reproducible		

Parent Defect ID:	XCO-6468	Issue ID:	XCO-6468
Reason Code:			
Product:	XCO	Reported in Release:	EFA 3.0.0
Symptom:	Why after recovering from EFA-8779, one EFA server recovered but other remained down and to finally recover it, we had to redeploy EFA.		

Parent Defect ID:	XCO-6574	Issue ID:	XCO-6574
Reason Code:	Question Answered		
Product:	XCO	Reported in Release:	XCO 3.2.0
Symptom:	Post EFA upgrade, EFA not able to communicate Switches.		

Parent Defect ID:	XCO-6630	Issue ID:	XCO-6630
Reason Code:	Not a Software Defect		
Product:	XCO	Reported in Release:	XCO 3.2.0
Symptom:	XCO- MGMT subinterface IP address is not contained in netstat -tuplen | grep 443.		

Parent Defect ID:	XCO-6759	Issue ID:	XCO-6759
Reason Code:	Not Applicable		
Product:	XCO	Reported in Release:	EFA 3.1.1
Symptom:	TPVM incremental downgrade is failing.		

Parent Defect ID:	XCO-6886	Issue ID:	XCO-6886
Reason Code:	Already Implemented		
Product:	XCO	Reported in Release:	EFA 2.7.2
Symptom:	vrf deletion Error : Cannot delete the VRF vrf_VPN01562_354373 as it is configured on the device(s).		

Parent Defect ID:	XCO-6954	Issue ID:	XCO-6954
Reason Code:	Working as Designed		
Product:	XCO	Reported in Release:	XCO 3.2.0
Symptom:	SNMP configuration not in sync with EFA		

Parent Defect ID:	XCO-7475	Issue ID:	XCO-7475
	Not Reproducible		

Parent Defect ID:	XCO-7475	Issue ID:	XCO-7475
Reason Code:			
Product:	XCO	Reported in Release:	XCO 3.2.1
Symptom:	UC1: XCO deletes IPv4/v6 addresses from Ve interfaces after Leaf reboot & DRC		

Parent Defect ID:	XCO-7612	Issue ID:	XCO-7612
Reason Code:	Not a Software Defect		
Product:	XCO	Reported in Release:	XCO 3.2.1
Symptom:	Configuration pushed using execute-cli is removed by XCO during DRC		

Parent Defect ID:	XCO-8144	Issue ID:	XCO-8144
Reason Code:	Not a Software Defect		
Product:	XCO	Reported in Release:	XCO 3.2.1
Symptom:	XCO 3.2.1: EFA manage firmware-downlad status as a “failed” after upgrade.		

Open Defects

The following defects are open in ExtremeCloud Orchestrator 3.3.0.

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		

Parent Defect ID:	XCO-3445	Issue ID:	XCO-3445
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-4127	Issue ID:	XCO-4127
Product:	XCO	Reported in Release:	EFA 3.0.0
Symptom:	Ports are not listed in the port-channel creation for SLX NPB devices		
Condition:	Even though the ports are not used in any other configurations, the ports are not listed in the port-channel creation. For these ports, speed is set to auto-negotiation, and ports are not connected with cable.		

Parent Defect ID:	XCO-4127	Issue ID:	XCO-4127
Workaround:	For breakout ports, make sure that cables are connected so that port speed will be updated.		
Recovery:	N/A		

Parent Defect ID:	XCO-4128	Issue ID:	XCO-4128
Product:	XCO	Reported in Release:	EFA 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	Reported in Release:	EFA 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:	NA		

Parent Defect ID:	XCO-4146	Issue ID:	XCO-4146
Product:	XCO	Reported in Release:	EFA 2.7.2
Symptom:	The fabric devices continue to remain in cfg-refresh-err state after the tpvm fail over.		

Parent Defect ID:	XCO-4146	Issue ID:	XCO-4146
Condition:	1.Fabric devices are already in cfg-refresh-err state due to LLDP Link down(LD) event. 2. Bring up the LLDP links responsible for the fabric devices to be in cfg-refresh-err state. 3. Execute the TPVM failover by 'tpvm stop' and 'tpvm start' commands during the LLDP Link up (LA) event handling caused by 2.		
Recovery:	1The user triggers LD/LA event by flapping the interface links which are the devices are in the cfg-refreshed state even though DRC wouldn't help out to recover the device to the cfg-sync state and the pending reason is "LA/LD". 1.1. "shutdown" the interface link on the physical link on Devices follow by "efa inventory device update --ip <device-ip>", which generates LD events 21.. "no shutdown" the interface link on the physical link on Devices follow by "efa inventory device update --ip <device-ip>", which generates LA events 1.3. If the pending config contains "LA" : Execute "efa inventory drift-reconcile execute --ip <device-ip> --reconcile" on the devices which are in cfg-refresh-err /cfg-refreshed state [or] IF the pending config contains "LD,LA" : Execute "efa fabric configure --name <fabric-name>" to clean up the configuration on devices which are in cfg-refresh-err /cfg-refreshed state. [OR] 2. The user reboots the devices without maintenance mode which are the devices are in cfg-refreshed state even though DRC wouldn't help out to recover the device to the cfg-sync state. 2.1. "reload" the switches without out maintenance mode to enable 2.2. Execute "efa inventory drift-reconcile execute --ip <device-ip> --reconcile" on the devices which are in cfg-refresh-err /cfg-refreshed state.		

Parent Defect ID:	XCO-5263	Issue ID:	XCO-5263
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	Failed to report telemetry not streamed from device		
Condition:	When SLX device is discovered from XCO and statistics are getting streamed using telemetry service. Device is not sending statistics using telemetry service.		
Workaround:	Select the individual device and verify the statistics are streaming from device.		

Parent Defect ID:	XCO-6172	Issue ID:	XCO-6172
	XCO	Reported in Release:	XCO 3.2.0

Parent Defect ID:	XCO-6172	Issue ID:	XCO-6172
Product:			
Symptom:	SLX currently doesn't support configuring both IPv4 and IPv6 DNS together. When both IPv4 and IPv6 DNS are configured during tpvm deployment, only one trusted peer config takes effect.		
Workaround:	It is recommended to use IPV4 DNS for XCO deployment.		

Parent Defect ID:	XCO-6189	Issue ID:	XCO-6189
Product:	XCO	Reported in Release:	XCO 3.2.0
Symptom:	SLX currently doesn't support configuring both IPv4 and IPv6 trusted peers together. When both IPv4 and IPv6 trusted-peers are configured after tpvm deploy, only one trusted peer config takes effect.		
Workaround:	It is recommended to use IPV4 trusted peer for XCO deployment.		

Parent Defect ID:	XCO-6360	Issue ID:	XCO-6360
Product:	XCO	Reported in Release:	XCO 3.1.1
Symptom:	Few important system logs are not seen in the XCO UI.		
Condition:	Device is discovered from XCO and some of the cards are removed or inserted in the device.		

Parent Defect ID:	XCO-7100	Issue ID:	XCO-7100
Product:	XCO	Reported in Release:	XCO 3.2.0
Symptom:	"Target TPVM Version" Does not display until new TPVM is already installed.		
Condition:	During the TPVM upgrade, "Target TPVM Version" gets updated late in the workflow.		
Recovery:	The correct Target TPVM version gets updated after the new version is installed.		

Parent Defect ID:	XCO-7183	Issue ID:	XCO-7183
Product:	XCO	Reported in Release:	EFA 3.0.0
Symptom:	After changing DNS nameservers in /etc/netplan and running the update-dns.sh --dns-action allow, the following error is seen: (efa:ubuntu)ubuntu@efa:/opt/efa$ sudo /opt/efa/update-dns.sh /opt/efa/update-dns.sh Usage: --help - Show this message		

Parent Defect ID:	XCO-7183	Issue ID:	XCO-7183
	--dns-action <'allow'|'disallow'> - Allow host DNS entries to be forwarded to the pods (efa:ubuntu)ubuntu@efa:/opt/efa$ sudo /opt/efa/update-dns.sh --dns-action allow Unexpected nameserver entry of 127.0.0.53 found in /etc/resolve.conf (efa:ubuntu)ubuntu@efa:/opt/efa$		

Parent Defect ID:	XCO-7183	Issue ID:	XCO-7183
Condition:	In 18.04.6 and 20.04, Ubuntu uses a stub-resolv.conf located in /run/systemd/resolve/stub-resolv.conf . This file is symlink to /etc/resolv.conf in /run/systemd/resolve/. There is another file, resolv.conf which contains the information for DNS from netplan. Additionally, systemd-resolved provides a local DNS stub listener on IP address **`127.0.0.53`** on the local loopback interface. Programs issuing DNS requests directly,bypassing any local API may be directed to this stub, in order to connect them to systemd-resolved. **Note:** The best practice is for local programs to use the glibc NSS or bus APIs instead (as described above), as various network resolution concepts (such as link-local addressing, or LLMNR Unicode domains) cannot be mapped to the unicast DNS protocol. We do not recognize the 127.0.0.53 address as valid.		

Workaround:	If updating DNS to allow host entries to be forwarded to the pods using the update-dns.sh script in XCO-3.3.0 on Ubuntu 20.0.4 or 18.0.4-6 or above, follow these steps.
	After netplan is applied and before running update_dns.sh
	1. Check if symlink exists, if not directly edit /etc/resolv.conf to netplan ip:
	
	$ ls -l /etc/resolv.conf
	
	lrwxrwxrwx 1 root root 39 Feb 20 2021 /etc/resolv.conf -> ../run/systemd/resolve/stub-resolv.conf <<<symlink exists
	2. Check if it has 127.0.0.53 ip in the following files:
	
	$ cat /etc/resolv.conf | grep nameserver
	
	nameserver 127.0.0.53
	
	$ cat /run/systemd/resolve/stub-resolv.conf | grep nameserver
	
	nameserver 127.0.0.53
	3. Edit the following file to add netplan DNS ip for the nameserver and remove 127.0.0.53
	
	sudo vi /run/systemd/resolve/stub-resolv.conf
	4. Check if both files are updated
	
	$ cat /run/systemd/resolve/stub-resolv.conf | grep nameserver
	
	nameserver 10.10.10.0
	
	$ cat /etc/resolv.conf | grep nameserver
	
	nameserver 10.10.10.0		

Parent Defect ID:	XCO-7183	Issue ID:	XCO-7183
	5. Run as root ./update_dns.sh --dns-action allow 6. Run sudo netplan apply to restore /etc/resolv.conf and /run/systemd/resolve/stub-resolv.conf to its default value of 127.0.0.53		

Parent Defect ID:	XCO-7426	Issue ID:	XCO-7426
Product:	XCO	Reported in Release:	EFA 2.7.0
Symptom:	While performing `efa show-running-config` , application was not able to process inventory data from Device table.		
Condition:	Old entry present in DB, with invalid IP_address. Causing the issue.		
Workaround:	The only workaround here would be to remove this entry from dcapp_asset.device table.		
Recovery:	Make sure old devices are properly removed from inventory. No old devices entry exists in Inventory. No invalid device entry exists in device DB.		

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:	Execute the peer delete command again and it gets deleted on the second attempt.		

Parent Defect ID:	XCO-7955	Issue ID:	XCO-7955
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	When triggering the "Firmware Activate" process, it can lead to either parallel or serial execution, irrespective of the behavior of grouping devices for traffic loss. In cases where auto-commit is enabled, the activation can result in a "Firmware Commit Failed" status on the EFA end, even though the firmware commit has been successfully completed on the device end.		

Parent Defect ID:	XCO-7955	Issue ID:	XCO-7955
Condition:	The "Firmware Activate" process is initiated from the user interface, either through the Inventory Page or the Fabric-wide Page, even in the midst of an incomplete operation on a subset of devices. For instance: Device 1 and Device 2 trigger a download with auto-commit enabled from either the Inventory or Fabric-wide Page. Device 3 triggers a download from the Fabric or Inventory Page. Subsequently, Device 1 and Device 2 attempt to continue with the "Activate Download" operation from the inventory or fabric page, resulting in a "Firmware Commit Failed" failure.		
Workaround:	Do not initiate firmware upgrades on other devices until the device completes both the Activate operation and the commit operation.		
Recovery:	Based on the error in the flow sequences, use the following set of commands: "efa inventory debug unblock-from-fwdl" , "efa inventory device firmware-download" to continue with download operation		

Parent Defect ID:	XCO-8072	Issue ID:	XCO-8072
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	When configuring an OOB QoS map of traffic-class-cos type without DP value provided on SLX, after device update, the entry showed up on EFA with DP value of 4.		
Condition:	When configuring an OOB QoS map of traffic-class-cos type without DP value provided on SLX, after device update, the entry showed up on EFA with DP value of 4.		
Workaround:	No workaround for this OOB entry.		
Recovery:	Delete this OOB entry from SLX device side.		

Parent Defect ID:	XCO-8170	Issue ID:	XCO-8170
Product:	XCO	Reported in Release:	XCO 3.2.1
Symptom:	User is unable to login to XCO using LDAP authentication.		

Parent Defect ID:	XCO-8170	Issue ID:	XCO-8170
Condition:	The XCO login fails after configuring LDAP on TPVM and XCO.		
Workaround:	To authenticate using LDAP, set auth preference for LDAP to a higher value. For example: Set the preference to 1. Below commands can be used efa auth authentication preference show efa auth authentication preference add --authType=LDAP --identifier ldap1 --preference 1		

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 can 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-8200	Issue ID:	XCO-8200
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	SLX Devices are not allowed to execute the same firmware download execution flow, which could result in traffic loss. For example, it is not allowed to choose two Leaf devices from the same MCT pair.		
Condition:	From User Interface, Go to the fabric page & select a few devices Go to table action & select Firmware Upgrade Option		
Workaround:	The user selects the left-side leaf of the MCT pair and triggers firmware download and activation. Similarly, the user selects the right-side leaf of the MCT pair and triggers firmware download and activation.		
Recovery:	Choose another set of devices that will not result in traffic loss and proceed with the firmware download operation.		

Parent Defect ID:	XCO-8230	Issue ID:	XCO-8230
	XCO	Reported in Release:	EFA 3.0.1

Parent Defect ID:	XCO-8230	Issue ID:	XCO-8230
Product:			
Symptom:	When the user tries to import docker images after disk cleanup, the image import fails.		
Condition:	The k3s image import fails after disk cleanup.		
Recovery:	Run the image import on Active TPVM. Follow the below steps to recover from the above state 1. Clean up the disk space and restart all the services to run only with new instances. Free up the disk space # efactl clean Reimport the images using: # k3s ctr image import /opt/efa/docker_images/docker_k3s_images.tar Restart EFA/k3s # efactl restart # systemctl restart k3s		

Parent Defect ID:	XCO-8232	Issue ID:	XCO-8232
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	Error is observed while updating EFA system CLI setting Error : error creating directory on remote: Could not chdir to home directory /users/home21/<username>: No such file or directory		
Condition:	While using CLI "efa system settings update --remote-server-ip <ip> --remote-transfer-protocol scp --remote-server-username <username> --remote-server-password <password> --remote-server-directory <remote-server-directory>"		
Workaround:	Use Remote Server which has bash support installed.		
Recovery:	Add bash support and retry the CLI command.		

Parent Defect ID:	XCO-8234	Issue ID:	XCO-8234
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	The fabric alarm and the alarm status update notifications can briefly reflect a small time window where the fabric alarm is cleared when it is actually unhealthy.		
Condition:	This can occur during fabric formation or during any operation where fabric health is degraded due to multiple reasons (example:- spine to leaf link going down, BGP neighborship going down between spine and leaf, etc...). When a specific device and links are repaired and deemed healthy, the overall fabric alarm can temporarily be cleared although other devices remain unhealthy. Then subsequently the fabric alarm will be corrected and put into an unhealthy state due to the remaining unhealthy devices.		

Workaround:	N/A
Recovery:	The fabric alarm automatically recovers to the proper state. The fabric alarm can temporarily be cleared when it is actually not cleared yet.

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.