ExtremeCloud™ Orchestrator v4.0.2 GUI Administration Guide

User Interface Management and Configuration

9039311-01 Rev AA
April 2026

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

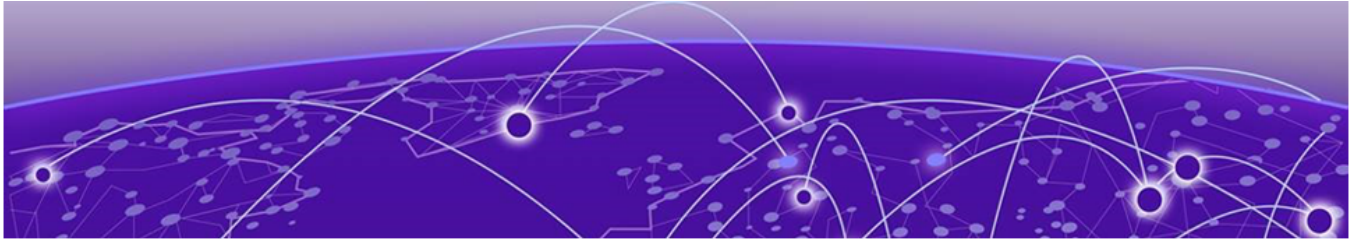
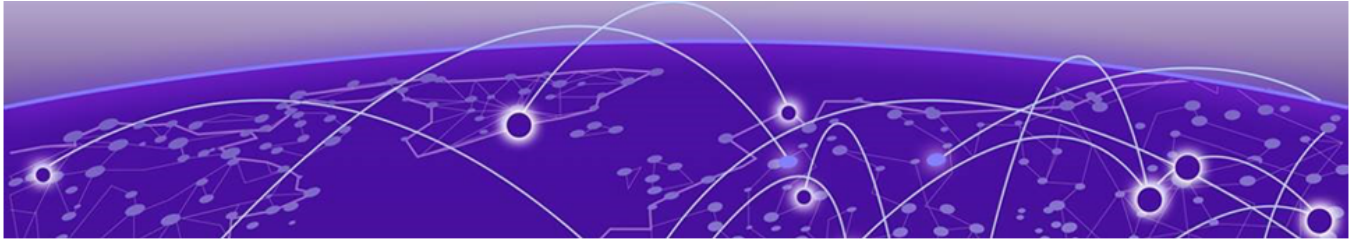


Table of Contents



Abstract

The ExtremeCloud™ Orchestrator v4.0.2 GUI Administration Guide provides comprehensive instructions for managing ExtremeCloud Orchestrator (XCO) through its graphical user interface (GUI) and APIs. This guide supports the orchestration of Extreme Networks solutions, including lifecycle management of SLX-OS and 8000 series devices, and introduces foundational support for Extreme OS ONE and the Extreme 8730 platform. Key topics include fabric creation and management for non-Clos, 3-stage Clos, and 5-stage Clos topologies, tenant provisioning, port channel (LAG) configuration, VRF and BGP setup, and firmware upgrades. The guide also details user interface navigation, dashboard widgets, device inventory operations, and user management with role-based access control (RBAC), LDAP, and TACACS+ authentication. Additional sections cover location-based device grouping, support save log collection, system and user logs, and troubleshooting FAQs. This guide is intended for system and fabric administrators seeking to deploy, monitor, and maintain scalable IP fabric networks using XCO's intuitive GUI.

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches, the product is referred to as *the switch*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and Software Compatibility for Extreme Networks products
Extreme Optics Compatibility
Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

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.

Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at Product-Documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.

What's New in this Document

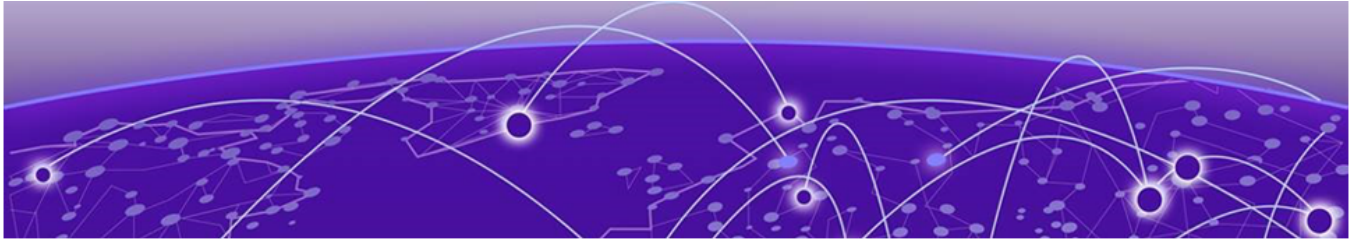
As of version 4.0.0, the ExtremeCloud Orchestrator (XCO) no longer includes support for the Visibility Skill. This deprecation follows the official End-of-Sale (EOS) announcement issued on February, 2025.

The following table describes changes to this guide for the ExtremeCloud Orchestrator 4.0.2 release.

Table 4: Summary of changes

Feature	Description
BGP Max-Path Fabric Setting	BGP Max-path fabric setting is supported on active fabric. Edit Fabric on page 45

For more information about this release, see the *ExtremeCloud Orchestrator Release Notes, 4.0.2*.



XCO OS ONE Integration and Platform Expansion

XCO 4.0.0 introduced foundational support for XCO OS ONE devices and added compatibility with the Extreme 8730 platform.

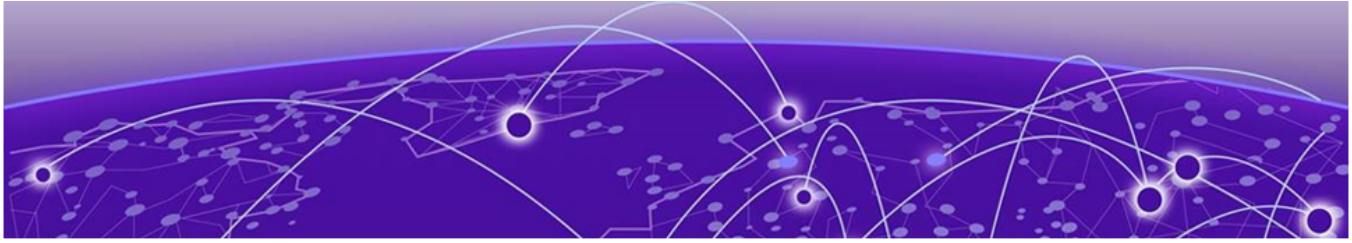
Extreme OS ONE Overview

Extreme OS ONE is a cloud-native, microservices-based network operating system designed for IP fabrics and data center environments.

For more information about XCO OS ONE Integration, see *ExtremeCloud™ Orchestrator v4.0.2 CLI Administration Guide*.

Note

- The features related to XCO OS ONE and Extreme 8730 support in XCO 4.0.0 are released as Control Released Features.
- For comprehensive feature descriptions, CLI command references, administrative procedures, and API documentation, contact Extreme Networks.



Welcome to ExtremeCloud Orchestrator

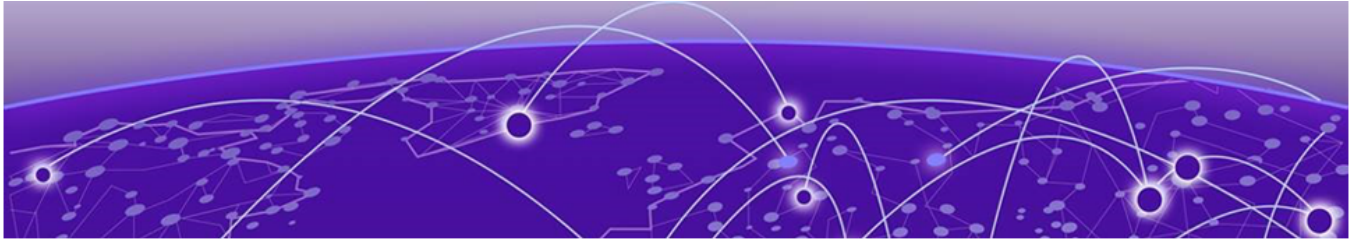
ExtremeCloud™ Orchestrator (XCO) is a single layer orchestration application that provides a unified and holistic GUI and APIs for fabric-wide life cycle management with highly scalable and flexible deployment model for Extreme solutions.

XCO provides common infrastructure and consistent installation and upgrade strategies for MLX, SLX-OS , and 8000 series devices with focus on scalability and performance.

XCO provides an industry leading user interface with a comprehensive, microservices-based solution to tailor the network to the changing user behavior. The user interface enables IP fabric life-cycle management of SLX-OS and Extreme 8000 series devices.

Note

- All procedures in this document are performed through GUI.
- As of version 4.0.0, the ExtremeCloud Orchestrator (XCO) no longer includes support for the Visibility Skill. This deprecation follows the official End-of-Sale (EOS) announcement issued on February, 2025.
- GUI support is not available for 8730 devices running Extreme OS ONE in XCO 4.0.0.

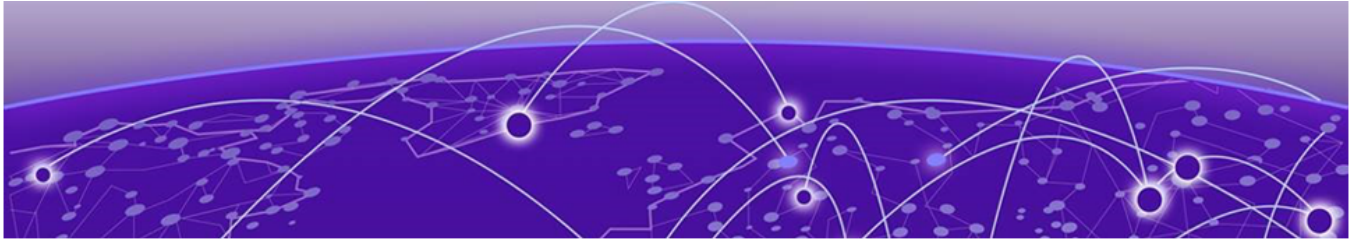


Fabric Automation and Orchestration

XCO automates and orchestrates SLX-OS IP fabric networks through CLI and UI.

For more information about fabric skill, see:

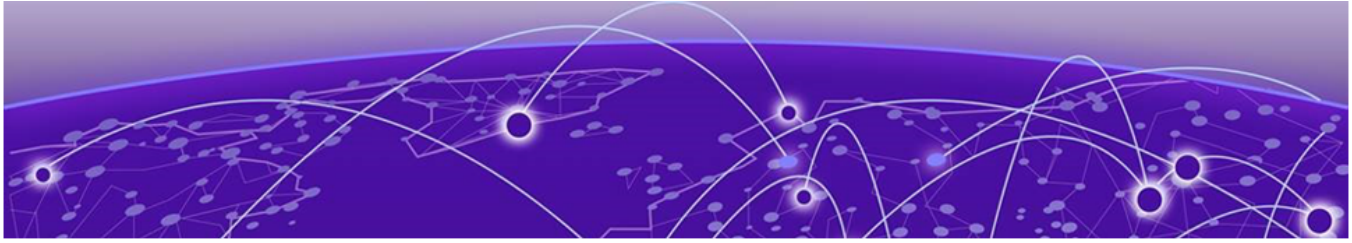
- ExtremeCloud Orchestrator CLI Administration Guide, 4.0.2.
- ExtremeCloud Orchestrator Command Reference, 4.0.2.
- ExtremeCloud Orchestrator Deployment Guide, 4.0.2.
- ExtremeCloud Orchestrator Security Configuration Guide, 4.0.2.
- ExtremeCloud Orchestrator Hyper-V Integration Guide, 4.0.2.
- ExtremeCloud Orchestrator VMware vCenter Integration Guide, 4.0.2.



XCO Limitations

XCO has the following limitations:

- Hostname or DNS name based device discovery is not supported.
- Device location cannot be modified after discovery.
- Only live statistics data streaming is supported.
- Secured Syslog configuration is not supported for MLX devices.
- Special characters such as %, {, }, \, and = are not supported in Name fields.
- If a device configured with both IPv4 and IPv6 addresses is discovered, only one entry is added to XCO. The first discovered IP address is used for communicating with that device.
- All configurations are reverted when a port channel deployment fails. However, a LAG is created and deleted immediately, and the events are captured in the device logs.
- Firmware upgrade requires an absolute path to the image location.



XCO Deployment

XCO supports the fabric skill deployment.

XCO user interface is not supported on TPVM deployments.

For information about deploying XCO, see the ExtremeCloud Orchestrator Deployment Guide, 4.0.2.

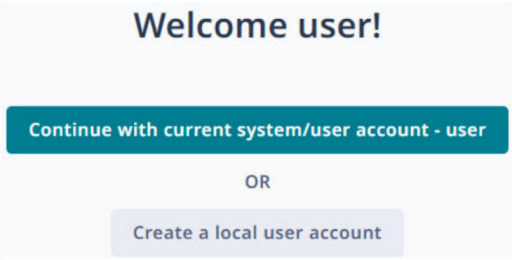
Navigate the User Interface

You can access XCO using the latest two versions of Google Chrome or Microsoft Edge web browsers.

Log in to XCO

Procedure

1. In a web browser, open `http://xx.xx.xx.xx/login`, where `xx.xx.xx.xx` is the IP address of the control plane node.
2. Complete the **Username** and **Password** fields.
3. Select **Login**.



If this is your first login as a host user, you are prompted to either continue with the current host user account or create a new local user account. Otherwise, the user interface opens to the **Dashboard** page.

Follow the instructions in Add User on page 96 to create new user accounts.

Local users are prompted to reset the password on first login.

Related Links

User Interface

The XCO interface provides access to all system functions. The interface pages vary depending on the logged-in user role. For more information about user roles, see User Roles on page 95.

Table 5 describes the numbered elements in this diagram.

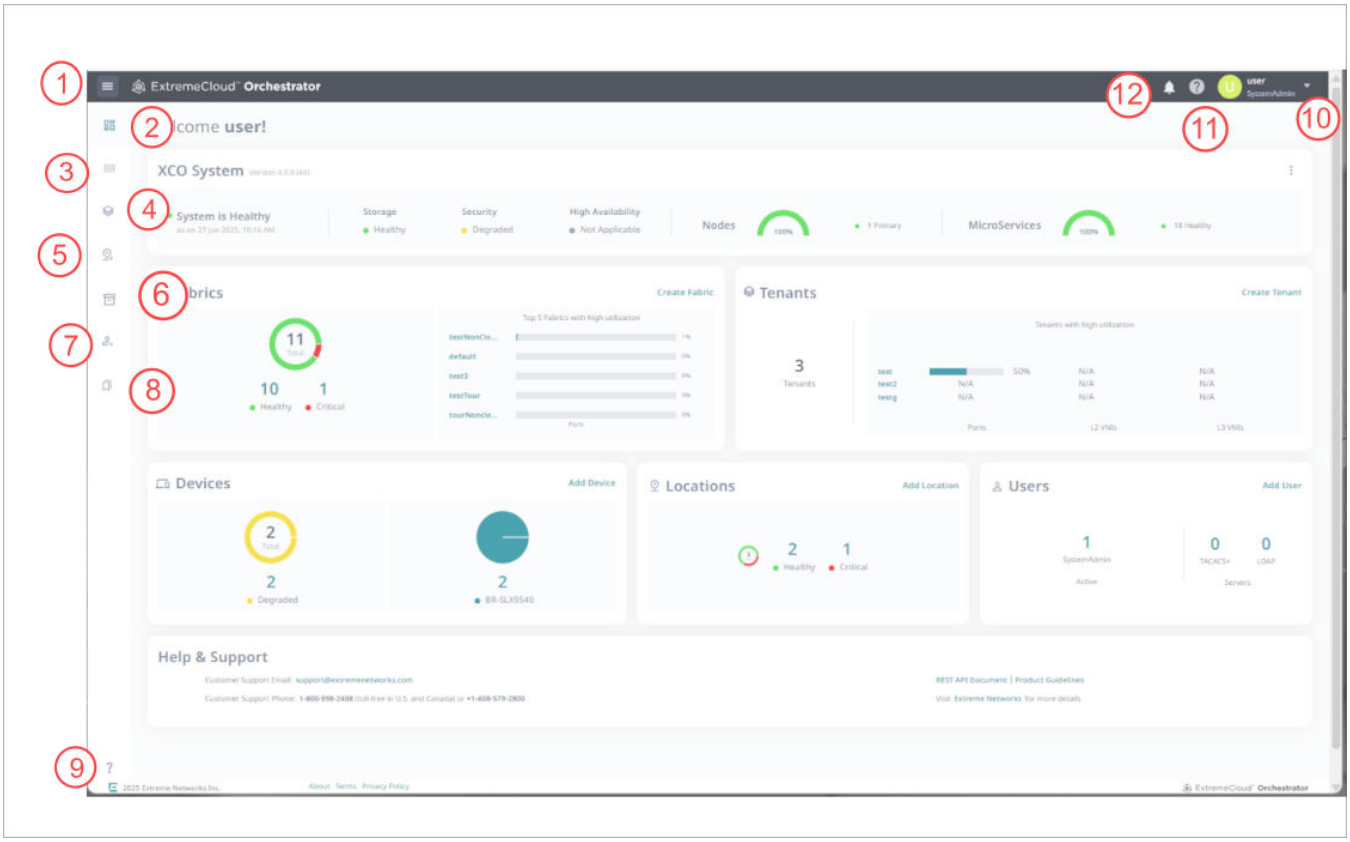


Figure 1: XCO user interface

Table 5: User interface descriptions

Legend	Interface Area	Description
1	Navigation menu	Provides access to all pages of the interface.
2	Dashboard	Provides an overview of system health and quick access to locations, devices, fabrics, and users configuration pages. See Dashboard on page 21.
3	Fabrics	Provides access to the fabrics management page. See Fabrics on page 29.
4	Tenants	Provides access to the tenant management page. See Tenants on page 59.
5	Locations	Provides access to the location management page. See Locations on page 79.

Table 5: User interface descriptions (continued)

Legend	Interface Area	Description
6	Device Inventory	Provides physical details and access to all configuration settings of the selected device. Details vary by device type. See Device Inventory on page 83.
7	Users	Provides access to settings for users, profile, and authentication. See Users on page 94.
8	Logs	Provides access to the logs page. See Logs on page 109.
9	Help & Support	Provides access to the help and support information.
10	User Profile	Displays the username and role of the logged-in user. From here, you can perform the following tasks: • Change own password • Log out
11	Online Help	Displays context-sensitive help for the active screen.
12	Notifications	Provides access to the notifications page. The notifications are user specific and do not persist. The  icon indicates new notifications.

Related Links

Refresh Page View on page 19
Pagination on page 19
Search, Group, and Filter on page 20

Refresh Page View

When you add a new entry or modify an existing entry in a table in the XCO user interface, you are prompted to refresh () the page to view the latest changes.

Pagination

About This Task

XCO supports pagination in all pages that show detailed data, such as locally configured users, devices, device configurations, policies, authentication servers, and locations.

Procedure

Select the required **Page Size** (**5**, **10**, **20**, **50**, **100**) to specify the number of entries in a table.

- The default page size is 10.
- Use the **Previous** (**<**) and **Next** (**>**) icons to scroll through the list.

Limitation:

The user interface displays incorrect data on the previous page when you scroll through list pages after applying filters.

Search, Group, and Filter

About This Task

You can search for an item and organize lists in the XCO user interface.

You can group records based on the pre-defined criteria that vary for different windows.

Use the **Previous** (**<**) and **Next** (**>**) icons to scroll through the lists.

Procedure

1. To search for a record in a page, enter a search attribute such as object name, IP address, location in the **Search** field and click **Search** ( ).

   To clear the search, click **X** in the **Search** field.
2. To group records in a page, select **Group By** and choose an attribute.

   To clear the grouping, select the **Clear** option.

   The list is organized by the grouping attribute you selected. The headings are collapsible.
3. To filter records in a page, select **Filter** ( ) and choose the filter attribute.

   To clear an individual filter, click **x** for the appropriate filter. To clear all the filters, click **Clear All Filters**.

   The list is organized by the filtering attribute you selected.

Dashboard

The XCO's **Welcome user!** dashboard screen or the landing page provides an overview of system health and provides quick access to various pages such as Fabrics, Locations, Devices, and Users. The critical errors in the system are marked in red.

The dashboard varies depending on the logged-in user role. For more information about user roles, see User Roles on page 95.

System Widget

The system widget on the dashboard displays information about nodes and microservices running in the system, health status of storage, security, and high availability. It also provides access to the **Support Save** menu.

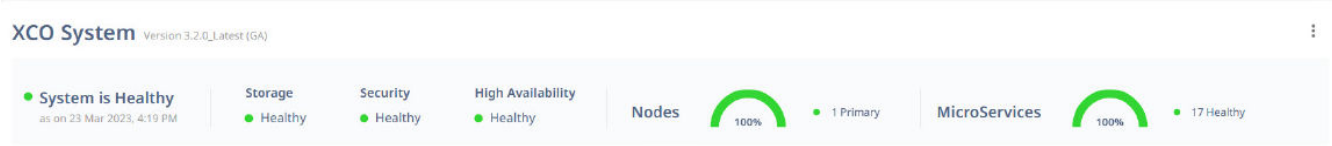


Table 6: System widget components

Component	Description
Storage	Indicates the storage status.
Security	Indicates the security status.
High Availability	Indicates the high availability status.

Table 6: System widget components (continued)

Component	Description
Nodes	Indicates the count of primary and standby nodes.
Microservices	Indicates the count of healthy, degraded, and critical state of microservices.

Related Links

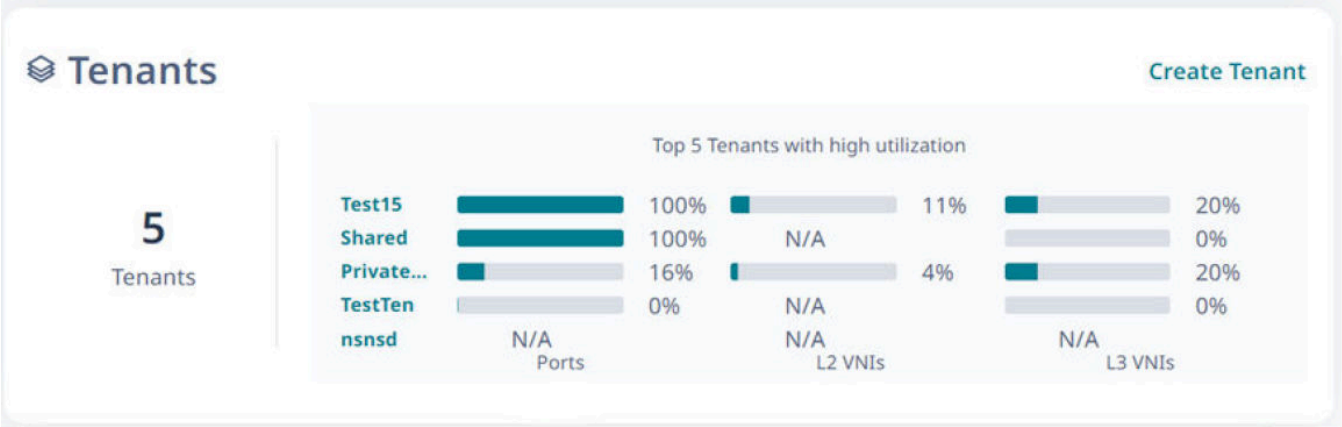
Support Save on page 24

Fabrics Widget

The **Fabrics** widget on the dashboard displays an overview of fabrics health and the five most heavily used fabrics with high utilization. Use the Fabrics widget to access the `Fabrics` management page.

Tenants Widget

The **Tenants** widget on the dashboard displays an overview of tenants health and the top five tenants in terms of utilization. Use the Tenants widget to access the `Tenants` management page.



Locations Widget

The **Locations** widget on the dashboard displays the total number of locations and their health status. Use the locations widget to access the `Locations` management page.

Devices Widget

The **Devices** widget on the dashboard displays the total number of discovered devices and their health status along with type specific device health status. Use the devices widget to access the `Devices` management page.

Users Widget

The **Users** widget on the dashboard displays the number of active users, active users by type, TACACS+ servers, and LDAP servers information. Use the users widget to access the `Users` management page.

Help & Support Widget

The **Help & Support** widget displays customer support contact information.

Support Save

XCO supports Support Save logs collection for troubleshooting.

You can generate and download Support Save logs as follows:

1. Generate system Support Save logs
2. Configure remote server for copying Support Save logs
3. Download Support Save logs

Related Links

Register Remote Server on page 24
Generate Support Save on page 27
Download Support Save on page 28

Register Remote Server

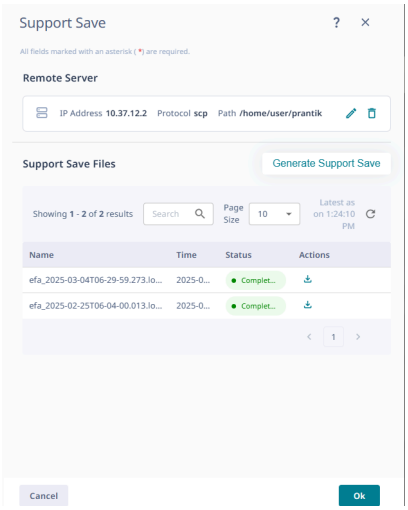
About This Task

You can configure a remote server to copy the generated Support Save logs.

Procedure

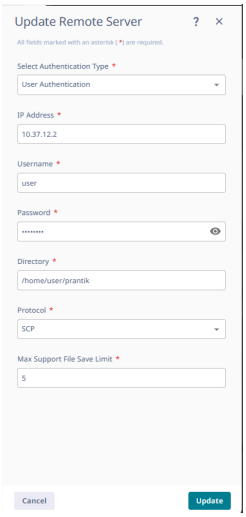
1. In the Navigation menu, select **Dashboard**.
2. Select ⋮ in the System Health widget.
3. Select **Support Save**.

4. Select **Register** if no remote server is configured, or  to update the Remote Server details.



5. In the **Select Authentication Type** select the authentication type. The options are:
   - **User Authentication**
   - **Digital Certificate Authentication**
   - **SSH Key Authentication**

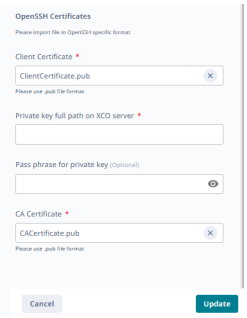
Note
If the authentication type is changed between Digital Certificate Authentication and SSH Key Authentication, the existing configuration will be overwritten. The user will be prompted to continue with the change.



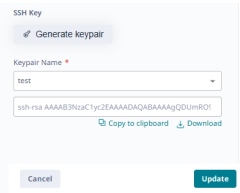
6. In the **IP Address** field, add the IP address of the remote server.
7. In the **Username** and **Password** fields, add the device credentials.
8. In the **Directory** field, provide the remote server path.

9. In the **Protocol** field, select the protocol.
   - **FTP**
   - **SCP**
10. In the **Max Support File Save Limit**, select a value to configure the number of support save files.

    When the configured support save file limit is reached, the oldest support save file is deleted when a new support save request is triggered.
    - The number of save files defaults to five and a maximum of 20 files are supported.
    - A minimum of two support files are required.
11. Complete the configuration steps specific to the authentication type selected:
12. If you selected User Authentication proceed to Step 15.
13. If you selected Digital Certificate Authentication:

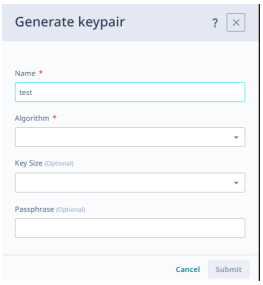


    a. In the **Client Certificate** field, select the Client Certificate file.
    b. In the **Private key full path on XCO server** field, select the file path.
    c. [Optional] In the **Pass phrase for private key** field, enter the pass phrase.
    d. In the **CA Certificate** field, select the CA certificate.
    e. Proceed to Step 15.
14. If you selected SSH Key Authentication:



    a. Select **Generate keypair**.
    b. In the **Keypair Name** field, enter a unique keypair name, or select an existing one to overwrite it.

       When generating a SSH Key Pair, there is a choice of algorithm:



rsa, with optional key sizes of 1024, 2048, 4096, or 8192;

ecdsa, with optional key sizes of 256, 384, or 521;

or **ed25519**, with key size 256;

and an optional **Passphrase**.

Select **Submit** to generate the keypair.

c. Select **Copy to clipboard** to copy the public key or **Download** to download the keypair file.

d. Proceed to Step 15.

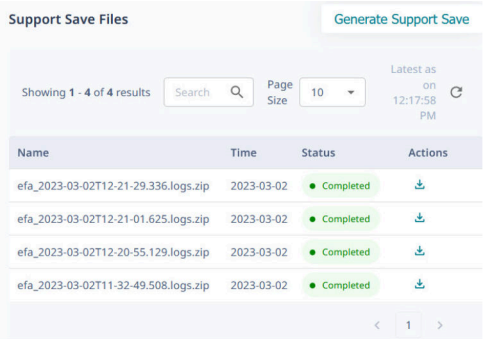
15. Select **Register** to add **Remote Server** details or **Update** to overwrite existing.

Generate Support Save

Procedure

1. In the Navigation menu, select **Dashboard**.
2. Select ⋮ in the System Health widget.
3. Select **Support Save**.
4. Select **Generate Support Save**.

   The new support save file is added to the list of support save files.



When the configured support save file limit is reached, the oldest support save file is deleted when a new support save request is triggered.

- The number of save files defaults to five and a maximum of 20 files are supported.
- A minimum of two support files are required.

For information on configuring the support save file limit, see Register Remote Server on page 24.

5. Select **OK**.

   A notification is displayed when the Support Save file is generated.

Download Support Save

Procedure

1. In the Navigation menu, select **Dashboard**.
2. Select in the System Health widget.
3. Select **Support Save**.
4. Select **Download** () for the required support save logs file.

   The selected support save file is downloaded to your device.

Fabrics

A fabric denotes a collection of interconnected devices in a topology on which underlay and overlay networks are configured.

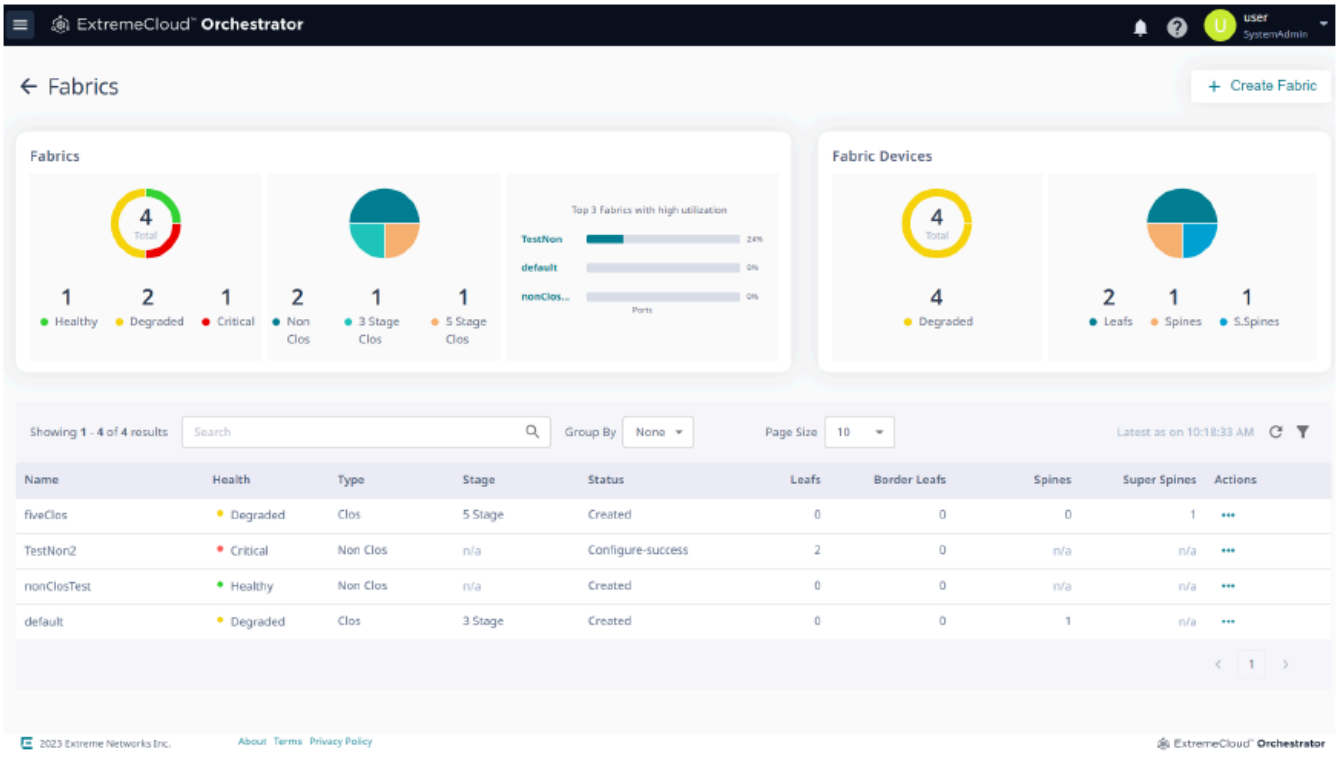
XCO 3.2.0 and later releases support building and managing small data center (non-Clos) fabrics and 3-Stage and 5-Stage IP Clos fabrics based on a BGP underlay with a BGP or EVPN overlay.

- Non-Clos topology involves one to four interconnected racks. Each rack consists of a pair of leaf nodes or border leaf nodes.
- 3-Stage Clos topology involves a spine layer and leaf or border leaf layer. The border leaf can be single-homed or dual-homed.
- 5-Stage Clos topology involves a super spine layer, spine layer, and leaf or border leaf layer. The leaf or border leaf can be single-homed or dual-homed.

For more information on IP fabric topologies, see *ExtremeCloud Orchestrator CLI Administration Guide, 4.0.2*.

Tenant Network onboarding services are supported on both 3-stage and 5-stage Clos topologies, allowing connectivity for devices connected to the fabric, such as compute (servers), storage, and external routers or gateways. For information on configuring and managing tenants, see Tenants on page 59.

You can use the **Fabrics** page to configure and manage IP fabrics.



For information on common operations such as refresh page view, pagination, search, group, and filter in the user interface, see:

- User Interface on page 17
- Refresh Page View on page 19
- Pagination on page 19
- Search, Group, and Filter on page 20

Create a Non-Clos Fabric

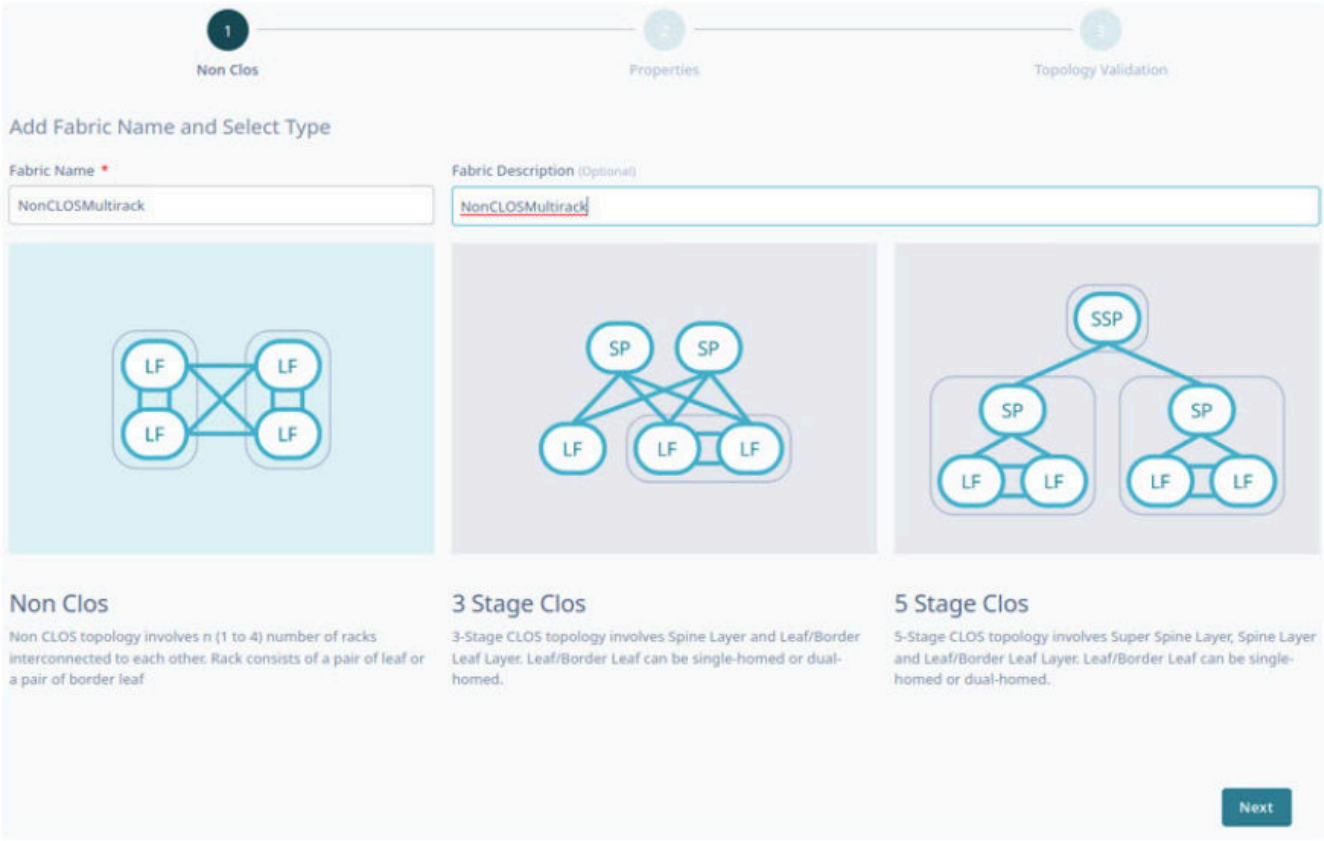
Before You Begin

- A non-clos topology supports a maximum of four racks with two devices each.
- The devices must be registered with the inventory before adding them to the fabric.

Procedure

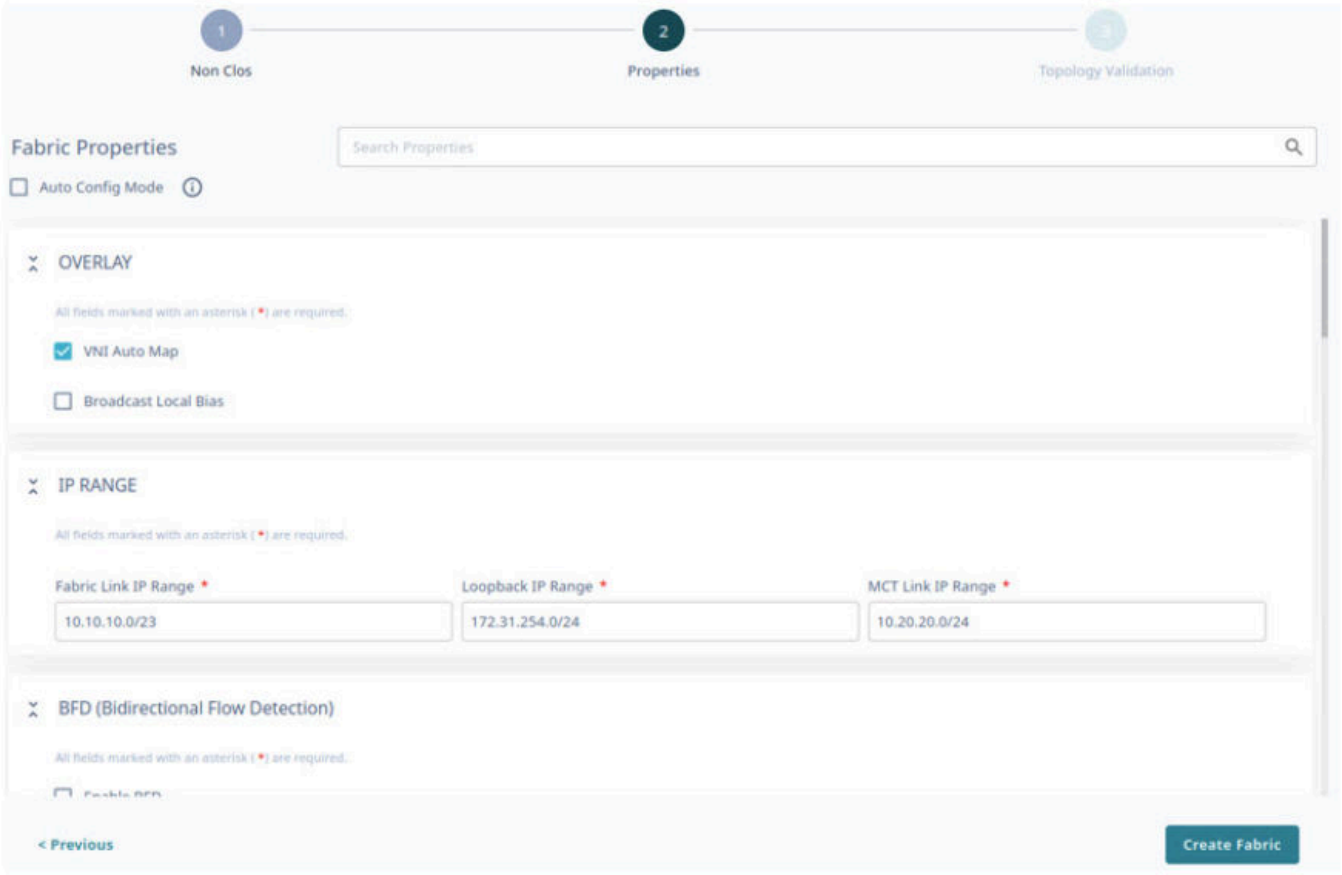
1. In the Navigation menu, select **Fabrics**.
2. In the Fabrics page, select **Create Fabric**.
3. In the **Fabric Name** field, enter a name for the fabric.
4. (Optional) In the **Fabric Description** field, enter a description for the fabric.

5. Select **Non Clos** topology.



6. Select **Next**.

7. In the **Fabric Properties** page, complete the fields as required or select the **Auto Config Mode** check box to use the default fabric settings.



8. To create a multi-rack Non-Clos fabric, clear the **Single Rack Deployment** check box.
9. Select **Create Fabric**.
10. In the **Physical Topology** page, add racks as required.

    Use **Topology View** ( ) and **List view** ( ) to switch the view between topology and list.

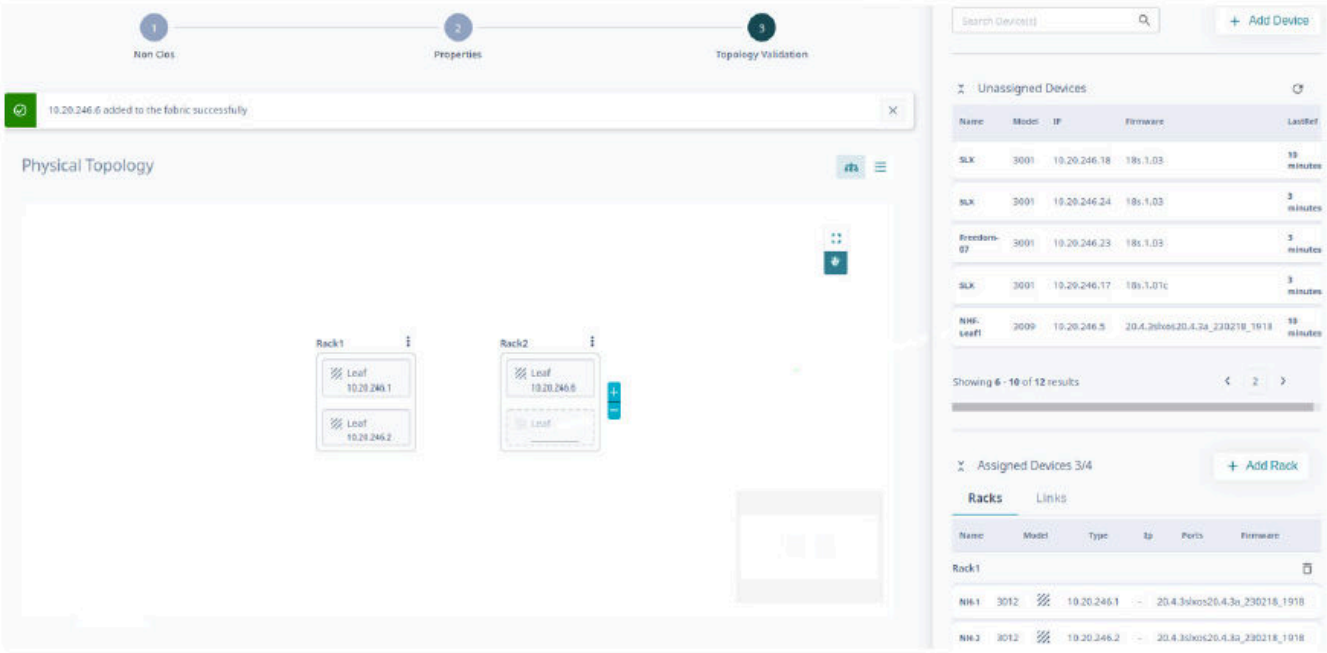
    a. Select **+** or **-** to add or remove a rack.

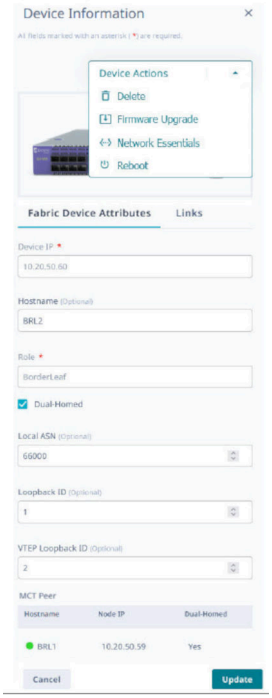
    Alternatively, you can do the following:

    - In the Devices panel, select **+ Add Rack** to add a new rack.
    - From the rack menu ( ), select **Remove** or select **Delete** ( ) in the devices panel to remove a rack.

    b. (Optional) From the rack menu ( ), select **Convert to Border Rack** or **Convert to Leaf Rack** to change the rack type.



11. Drag and drop the required devices from the Devices panel to the rack.
    - Select **Add Device** to add a device to the inventory. For more information, see Add Devices on page 84.
    - The devices available in the rack are displayed in the **Assigned Devices** list.
    - The inventory devices that are not part of the fabric are displayed in the **Unassigned Devices** list.
    - You can select devices in the rack to access and update device specific configurations such as ASN, VTEP Loopback ID, and Loopback ID. The attributes in the **Device Information** window vary by device role.
    - You can select and edit device and fabric configurations directly from the **Physical Topology** or **Devices** panel as required.
    - In the **Device Information** window, select **Device Actions** > **Network Essentials** to modify network essential configurations of the required device ports. For more information, see Network Essentials on page 51.

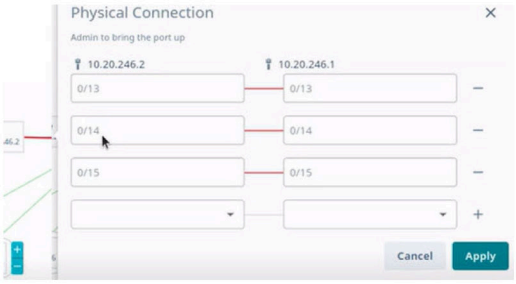


12. Select **Discover Topology** to validate the topology.

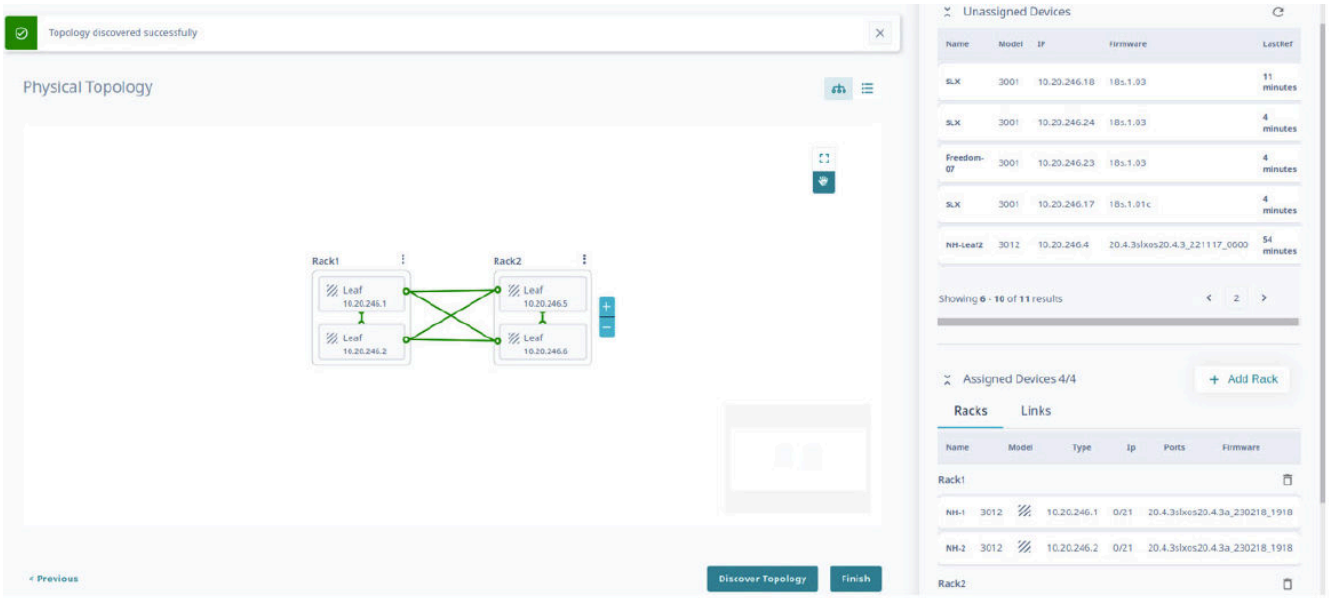
    The discovered topology is displayed.

    The ports or links that are down are marked in red in the topology. To turn a port or link up:

    a. Select the link that is down.
    b. In the **Physical Connection** dialog box, configure the ports.
    c. Select **+** or **-** to add or delete ports.
    d. Select **Apply**.



    e. Select **Discover Topology** to validate the topology.



13. To enlarge the topology to the width of the interface, select **Expand** ( ).
14. To zoom in and out on the topology screen, use the **Zoom** ( ) icons.
15. To scroll through the topology screen, use the **Scroll** ( ) icon.
16. Select **Finish** to configure the topology.

    The non-Clos fabric topology is configured.

What to Do Next

Select **View Fabric** or **Proceed to Dashboard** to return to the **Fabrics** page.

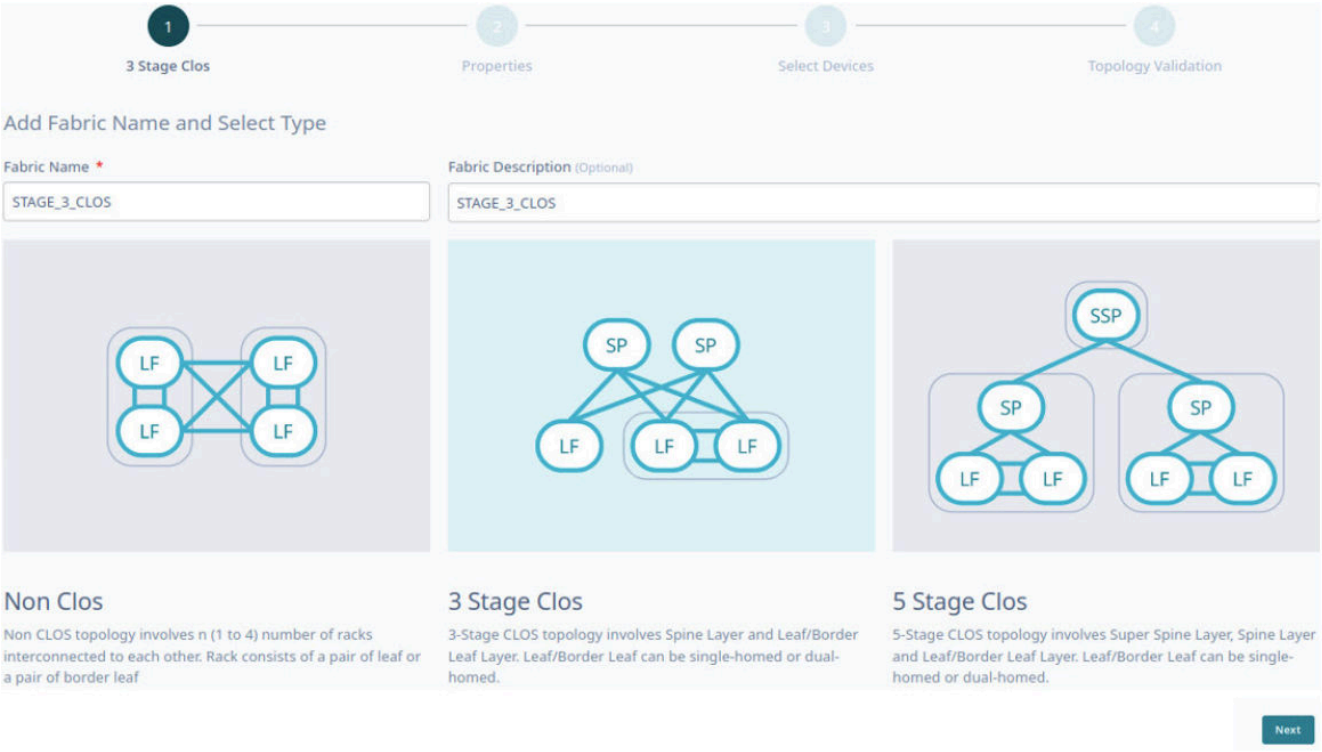
Related Links

Create a 3 Stage Clos Fabric on page 36
Create a 5 Stage Fabric on page 40
Edit Fabric on page 45
Download Fabric Inventory on page 47
Delete Fabric on page 47
Download Health Report on page 47
View Fabric Topology on page 47
Edit Fabric Topology on page 49
Configure Network Essentials on page 51
Firmware Upgrade on page 52
Clone a Fabric on page 57
Reboot a Device on page 57

Create a 3 Stage Clos Fabric

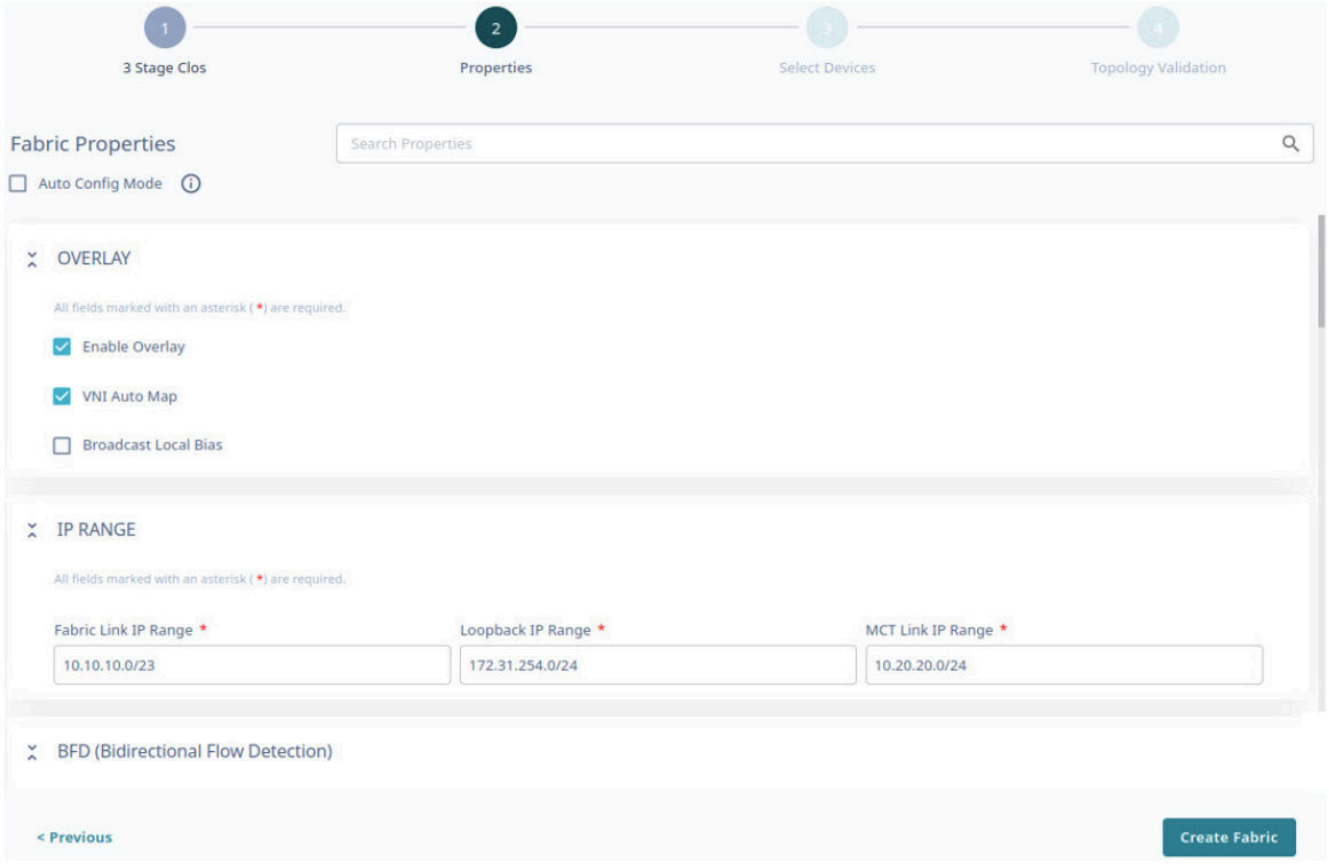
Procedure

1. In the Navigation menu, select **Fabrics**.
2. In the Fabrics page, select **Create Fabric**.
3. In the **Fabric Name** field, enter a name for the fabric.
4. (Optional) In the **Fabric Description** field, enter a description for the fabric.
5. Select **3 Stage Clos** topology.

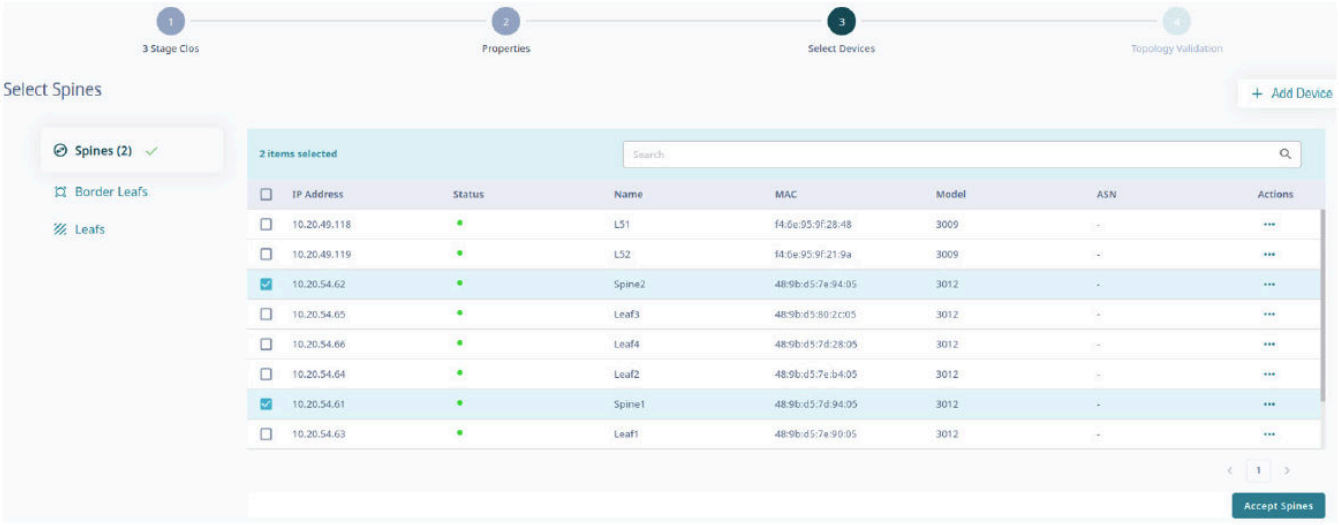


6. Select **Next**.

7. In the **Fabric Properties** page, complete the fields as required or select the **Auto Config Mode** check box to use the default fabric settings.



8. Select **Create Fabric**.
9. Select the check boxes of the required leaf devices from the following tabs:
   - **Spines**
   - **Border Leafs**
   - **Leafs**

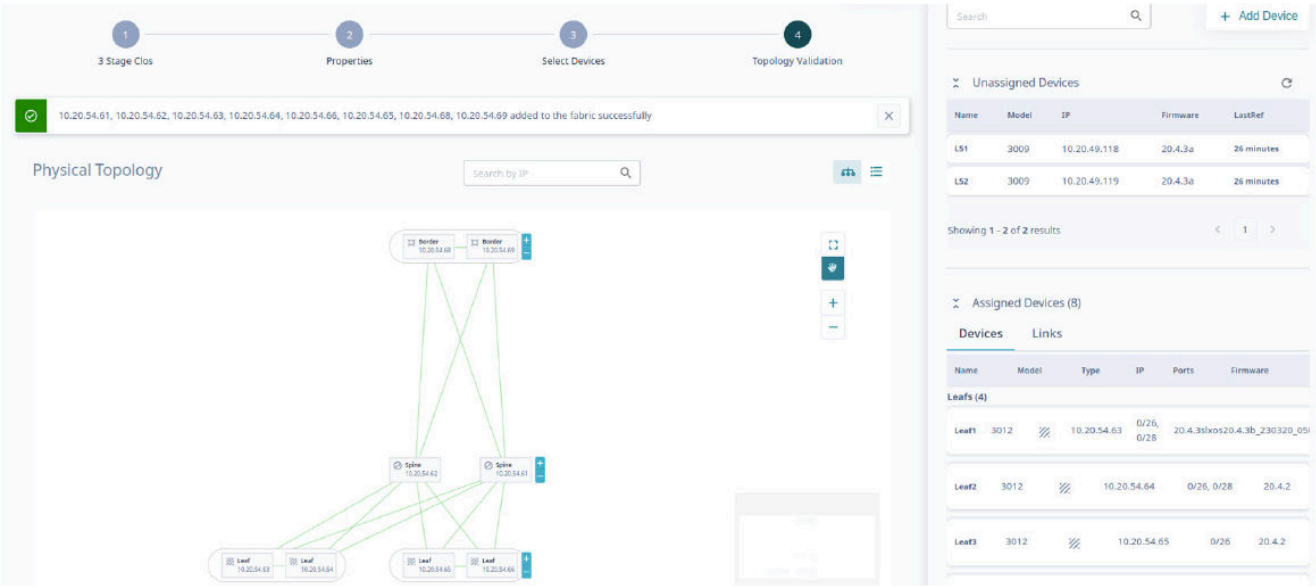


The border leaf devices are optional. Select **Skip Border Leafs** to skip border leaf devices.

Select **+ Add Device** to add new devices to the inventory. For more information, see Add Devices on page 84.

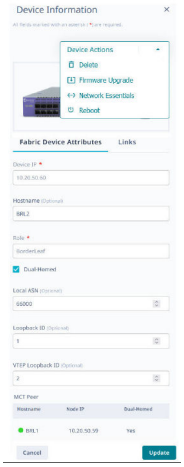
You can select any device row and update device specific configurations such as ASN, VTEP Loopback ID, and Loopback ID. The attributes in the **Device Information** window vary by device role.

10. Select **Accept Spine Leafs**, **Accept Border Leafs**, or **Accept Leafs** as applicable.
11. Select **Accept All** to add all devices to the topology.



- The discovered topology is displayed. You can select and edit device and fabric configurations directly from the **Physical Topology** or **View Devices** panel as required.

- In the **Device Information** window, select **Device Actions** > **Network Essentials** to modify network essential configurations of the required device ports. For more information, see Network Essentials on page 51.

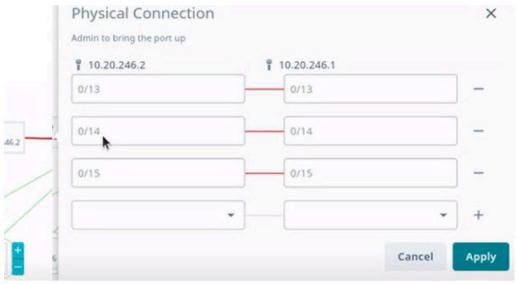


12. Select **Discover Topology** to validate the topology.

    The discovered topology is displayed.

    The ports or links that are down are marked in red in the topology. To turn a port or link up:

    a. Select the link that is down.
    b. In the **Physical Connection** dialog box, configure the ports.
    c. Select **+** or **-** to add or delete ports.
    d. Select **Apply**.



    e. Select **Discover Topology** to validate the topology.

    Select **Topology View** ( ) and **List view** ( ) to switch the view between topology and list.

13. To enlarge the topology to the width of the interface, select **Expand** ( ).
14. To zoom in and out on the topology screen, use the **Zoom** ( ) icons.
15. To scroll through the topology screen, use the **Scroll** ( ) icon.
16. Select **Finish** to configure the topology.

    The 3 stage Clos fabric topology is configured.

What to Do Next

Select **View Fabric** or **Proceed to Dashboard** to return to the **Fabrics** page.

Related Links

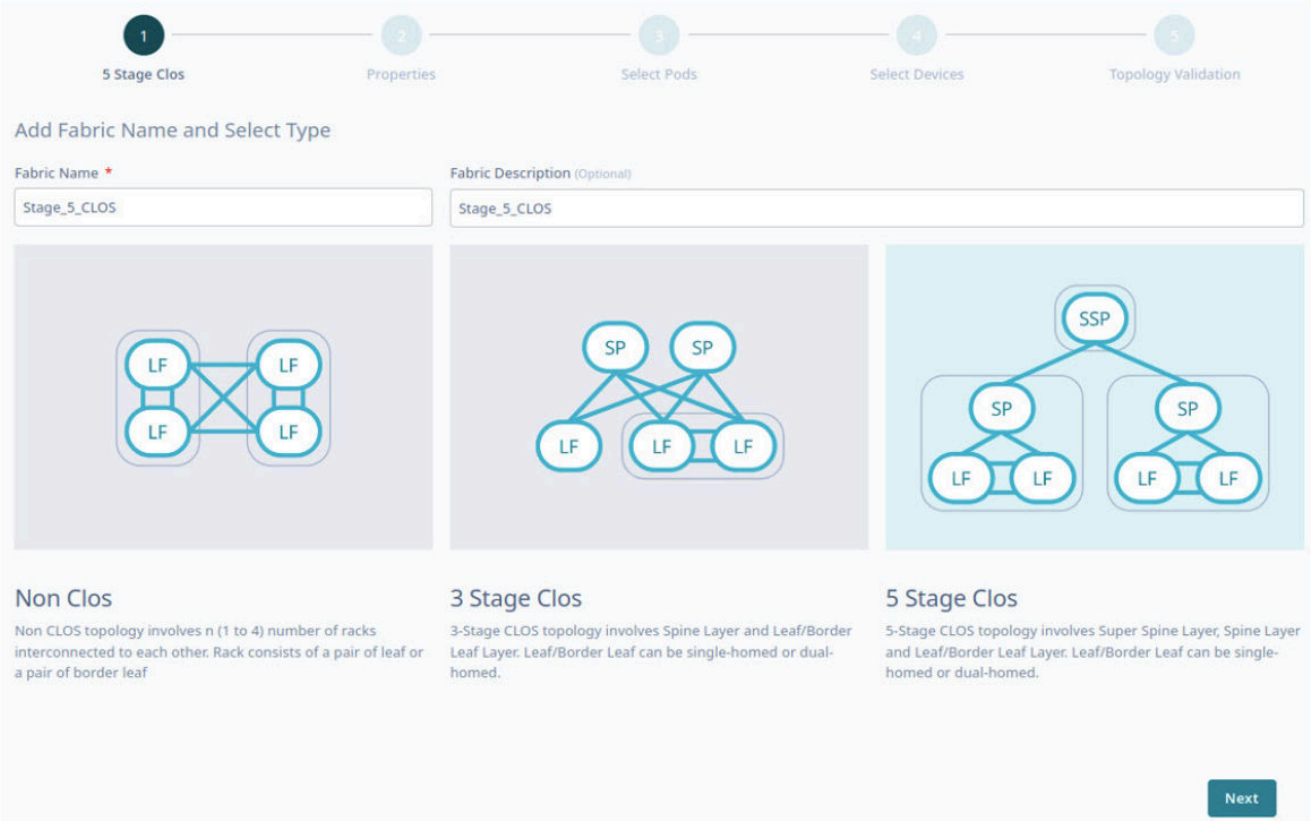
Create a Non-Clos Fabric on page 30
Create a 5 Stage Fabric on page 40
Edit Fabric on page 45
Download Fabric Inventory on page 47
Delete Fabric on page 47
Download Health Report on page 47
View Fabric Topology on page 47
Edit Fabric Topology on page 49
Configure Network Essentials on page 51
Firmware Upgrade on page 52
Clone a Fabric on page 57
Reboot a Device on page 57

Create a 5 Stage Fabric

Procedure

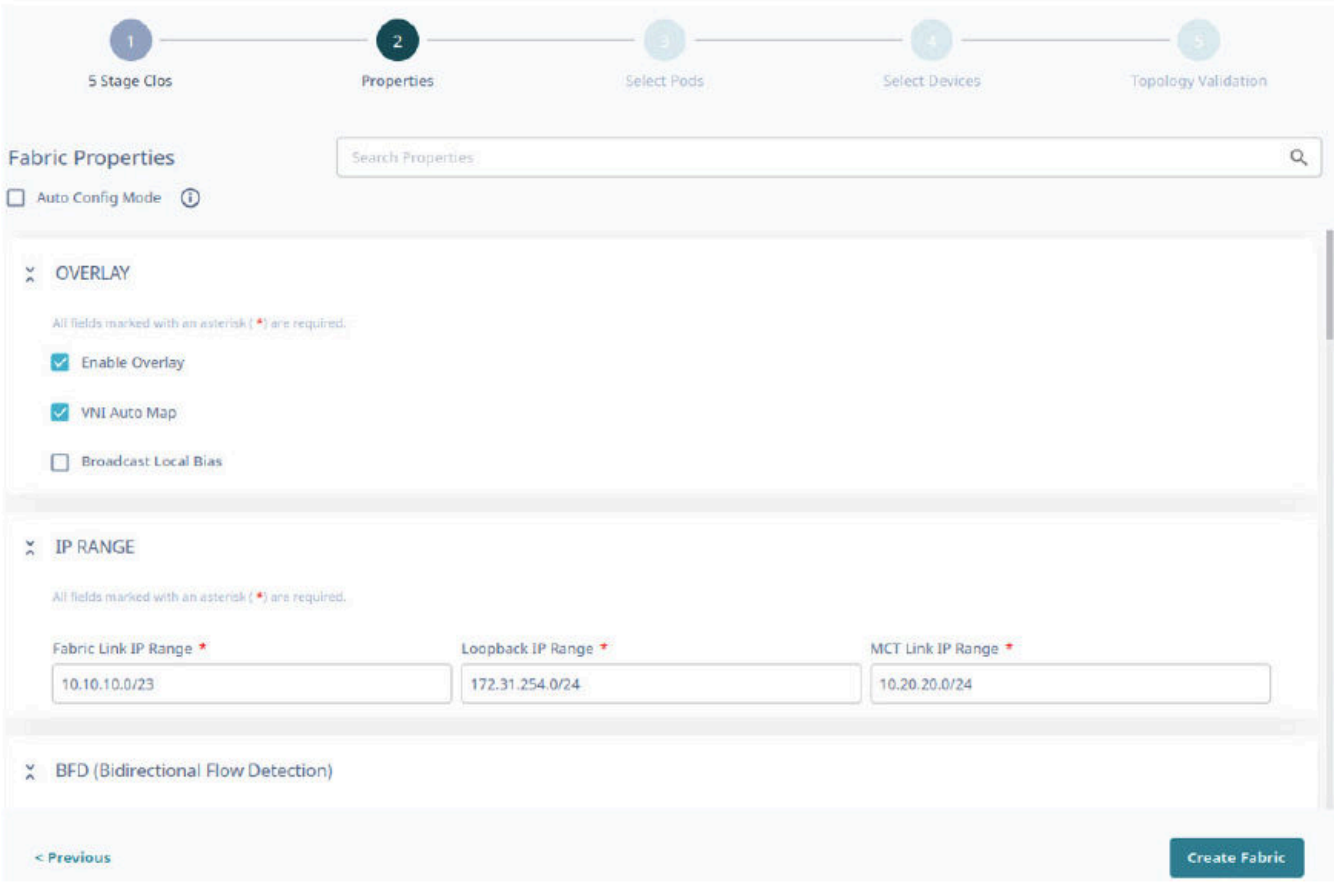
1. In the Navigation menu, select **Fabrics**.
2. In the Fabrics page, select **Create Fabric**.
3. In the **Fabric Name** field, enter a name for the fabric.
4. (Optional) In the **Fabric Description** field, enter the description for the fabric.

5. Select the **5 Stage Clos** topology.



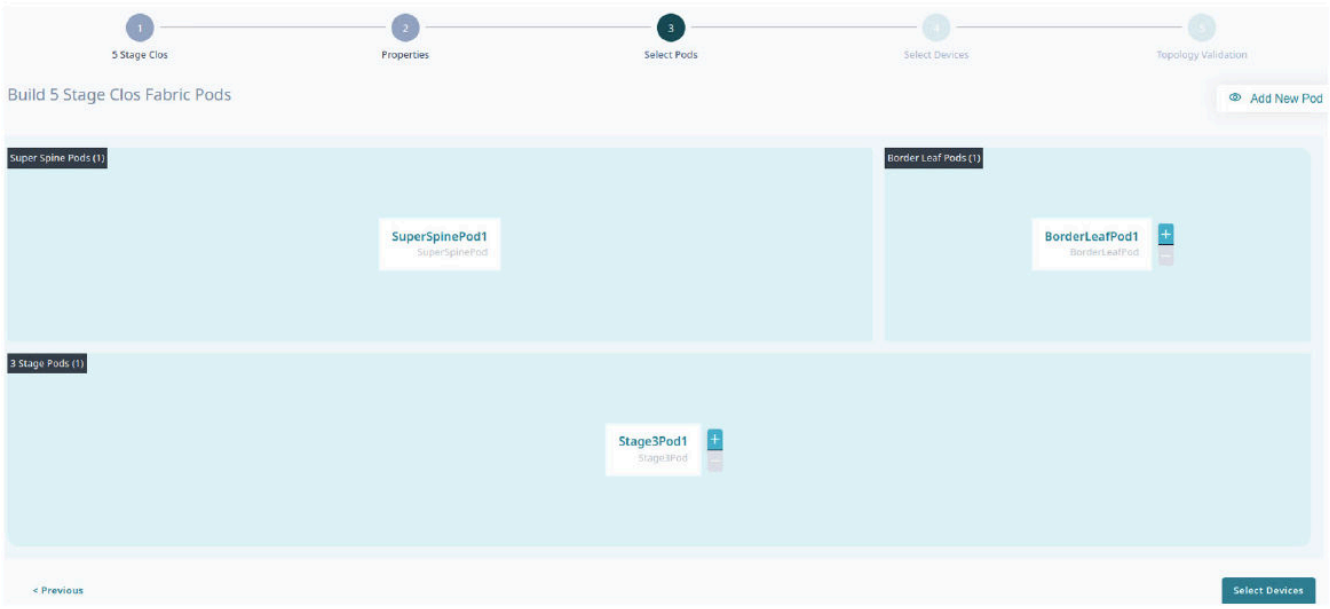
6. Select **Next**.

7. In the **Fabric Properties** page, complete the fields as required or select the **Auto Config Mode** check box to use the default fabric settings.



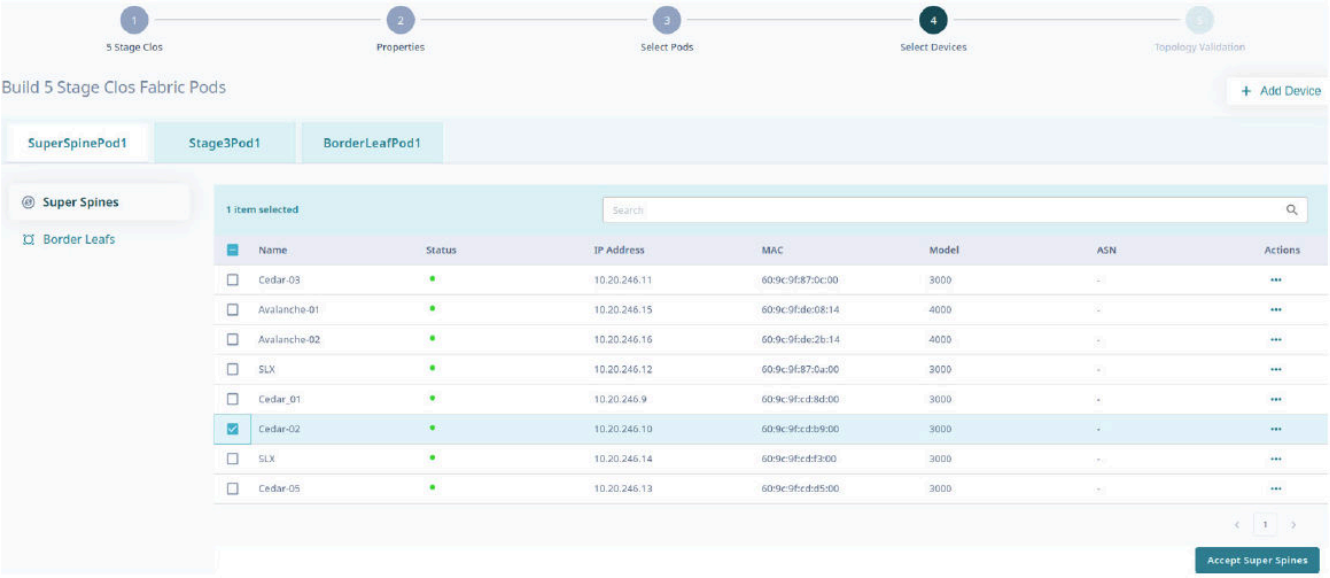
8. Select **Create Fabric**.

9. In the **Build 5 Stage Clos Fabric Pods** page, select **+** or **-** to add new 3 stage or border leaf pods.



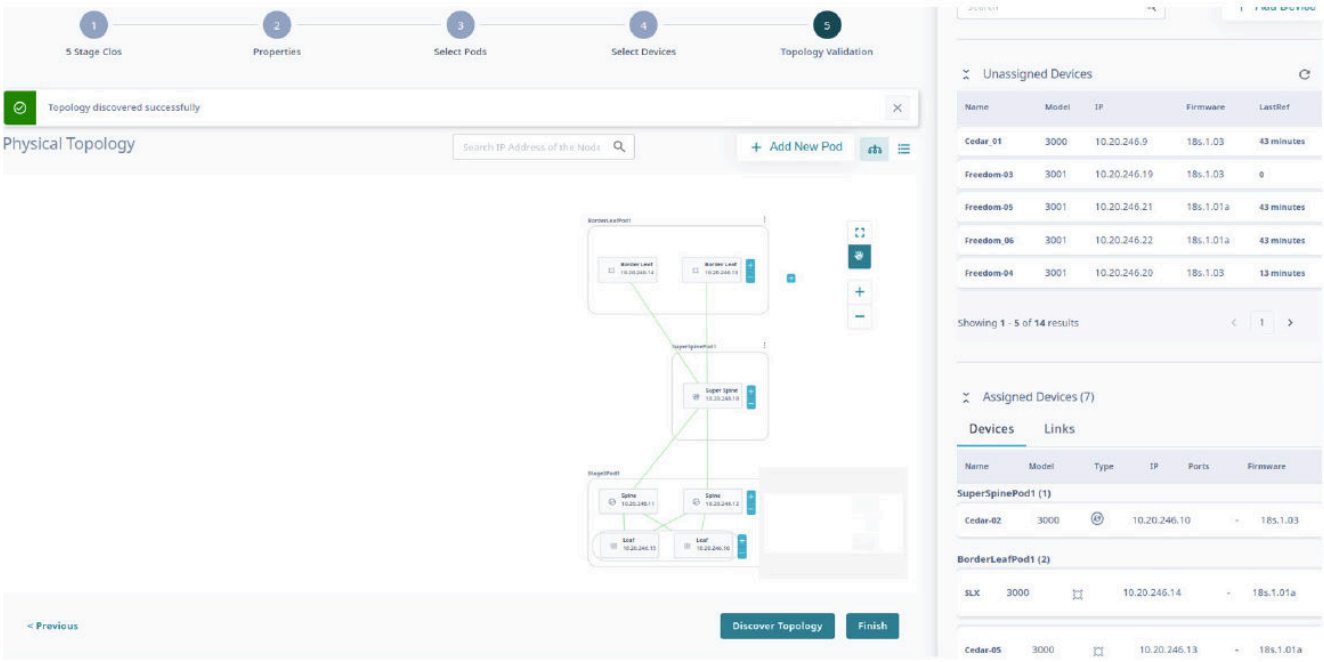
- Alternatively, you can select **Add New Pod**.
- One pod of each type is available in the UI by default and the pod names are auto-generated. For example: SuperSpinePod1, Stage3Pod1, and BorderLeafPod1.

10. Select **Select Devices** to add new devices.
11. Select the check boxes of the required devices from the following tabs:
    - **SuperSpinePod1**
    - **Stage3Pod1**
    - **BorderLeafPod1**

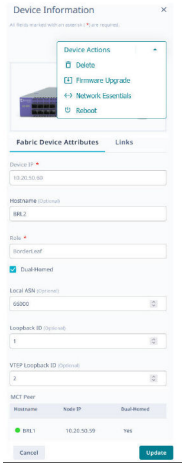


12. Select **Accept Super Spine Pods**, **Accept Spines**, or **Accept Border Leaf Pods** as applicable.

13. Select **Accept All the Pods** to add all devices to the topology.



- The discovered topology is displayed. You can select and edit the device configuration directly from the **Physical Topology** or **View Devices** panel as required.
- You can select devices in the rack to access and update device specific configurations such as ASN, VTEP Loopback ID, and Loopback ID. The attributes in the **Device Information** window vary by device role.
- In the **Device Information** window, select **Device Actions** > **Network Essentials** to modify network essential configurations of the required device ports. For more information, see Network Essentials on page 51.



Select **Topology View** ( ) and **List view** ( ) to switch the view between topology and list.

14. To enlarge the topology to the width of the interface, select **Expand** ( ).
15. To zoom in and out on the topology screen, use the **Zoom** ( ) icons.
16. To scroll through the topology screen, use the **Scroll** ( ) icon.
17. Select **Finish** to configure the topology.

    The 5 stage Clos fabric topology is configured.

What to Do Next

Select **View Fabric** or **Proceed to Dashboard** to return to the Fabrics page.

Related Links

Create a Non-Clos Fabric on page 30
Create a 3 Stage Clos Fabric on page 36
Edit Fabric on page 45
Download Fabric Inventory on page 47
Delete Fabric on page 47
Download Health Report on page 47
View Fabric Topology on page 47
Edit Fabric Topology on page 49
Configure Network Essentials on page 51
Firmware Upgrade on page 52
Clone a Fabric on page 57
Reboot a Device on page 57

Edit Fabric

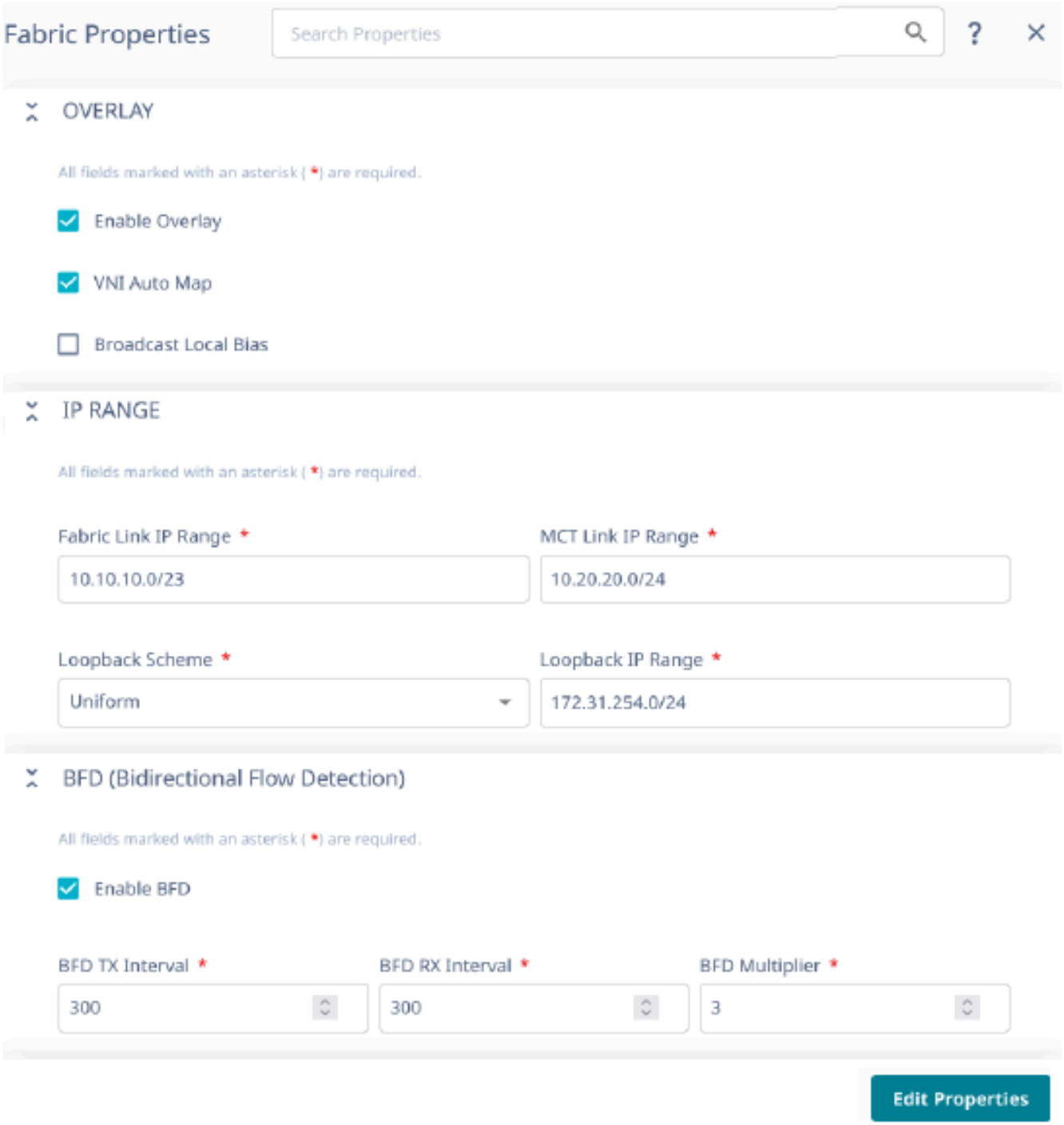
Procedure

1. In the Navigation menu, select **Fabrics**.
2. In the Fabrics page, click anywhere in the required fabric row except the Actions column ( ) to proceed to the device Topology page.
3. Select **Settings**.

   Alternatively, you can select **Edit Settings** from the Actions column for the required fabric.

4. In the **Fabric Properties** page, modify the fields as required.

Note
XCO 4.0.2 introduces BGP maximum-paths support in the SLX-OS fabric, enabling ECMP multipathing for BGP routes across all fabric devices (Leaf, Spine, Super-Spine) based on a fabric-wide setting. All SLX-OS devices in the fabric automatically inherit and enforce the fabric-wide max-paths setting for BGP ECMP with built-in drift detection and consistent multi-rack support.



5. Select **Edit Properties**.

Download Fabric Inventory

Procedure

1. In the Navigation menu, select **Fabrics**.
2. Select **Download**.

   A file in .csv format is downloaded to your device.

Delete Fabric

Procedure

1. In the Navigation menu, select **Fabrics**.
2. In the **Fabrics** page, select **Delete** ( ) from the Actions column (•••) for the fabric you want to delete.
3. Select **Confirm** when prompted.

Download Health Report

Procedure

1. In the Navigation menu, select **Fabrics**.
2. In the **Fabrics** page, select **Download Health Report** from the Actions column (•••) for the required fabric.

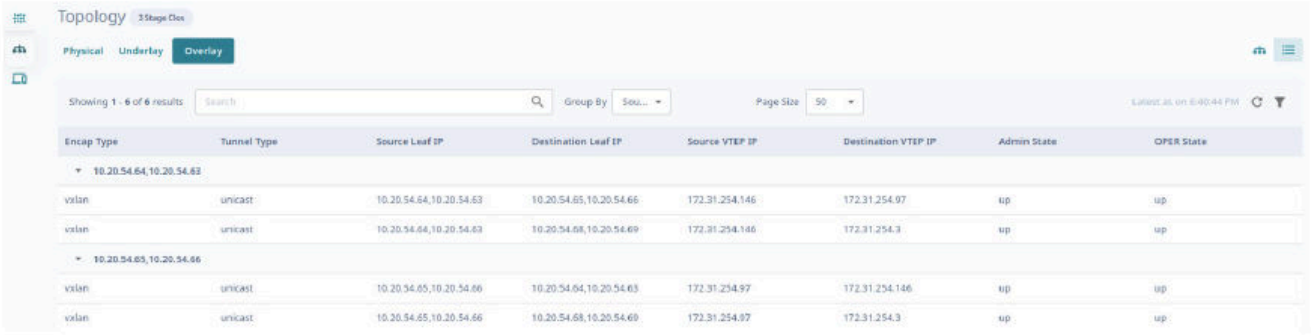
   The fabric health report is downloaded to your device.

View Fabric Topology

Procedure

1. In the Navigation menu, select **Fabrics**.
2. In the Fabrics page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the device Topology page.
3. Select the required topology tab.
   - **Physical**: Represents physical connections of the fabric devices
   - **Underlay**: Represents BGP sessions between the fabric devices
   - **Overlay**: Represents the overlay (VXLAN) tunnel state between leaf or border-leaf devices

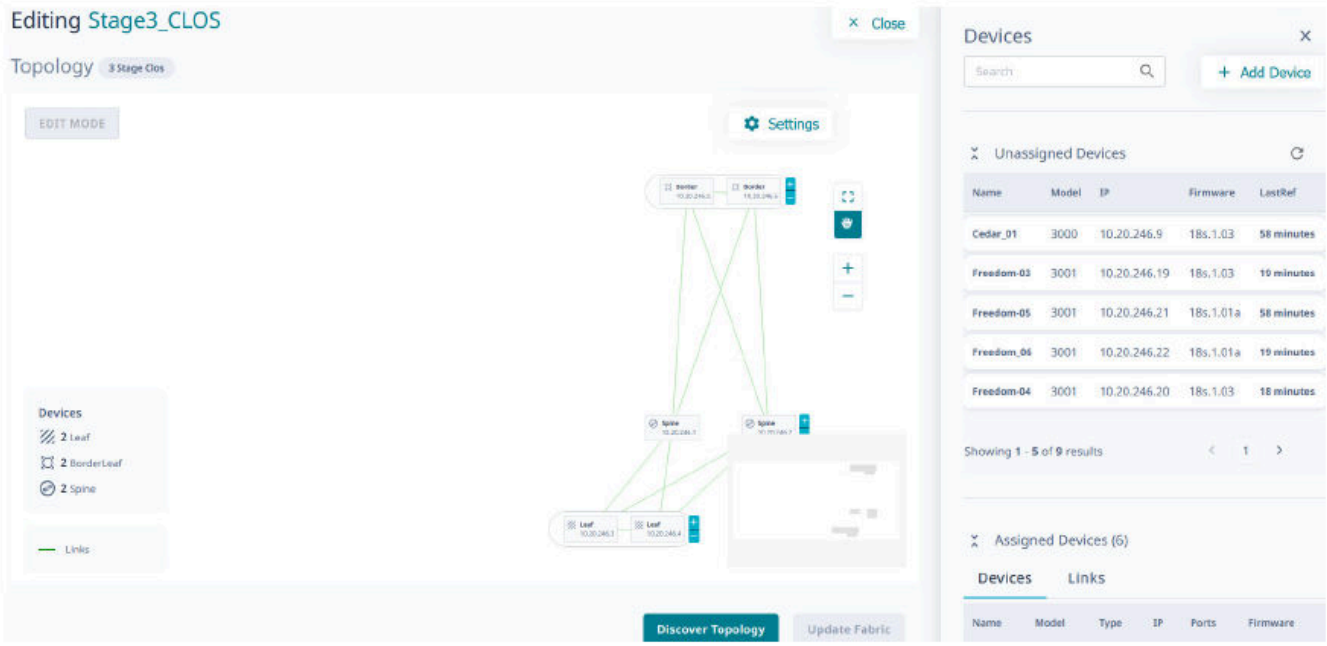
Select **Topology View** ( ) and **List view** ( ) to switch the view between topology and list.



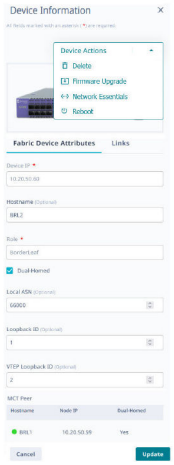
Edit Fabric Topology

Procedure

1. In the Navigation menu, select **Fabrics**.
2. In the Fabrics page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the device Topology page.
   - The fabric topology is displayed.
   - Alternatively, you can select **Edit** from the Actions column for the required fabric.
3. In the **Topology** page, select **Edit**.
   - Select **Devices** to add or remove devices in the topology.



   - Alternatively, you can select a device directly from the topology to access **Device Information** and edit **Fabric Device Attributes** as required.



- In the **Device Information** window, select **Device Actions** > **Network Essentials** to modify network essential configurations of the required device ports. For more information, see Network Essentials on page 51.

4. Select **Discover Topology** to verify the links in the topology.
5. Select **Update Fabric** to update the fabric.

   Refresh the page to view the updated list.

View Firmware History

About This Task

You can access **Firmware History** from both **Device Inventory** and **Fabrics** pages.

Procedure

1. In the Navigation menu, select **Fabrics**.
2. In the Fabrics page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the device Topology page.

   The fabric topology is displayed.
3. In the upper right corner of the **Topology** page, select ⋮ to access the **More** menu.
4. Select **Firmware History**.

   Alternatively, you can do one of the following:

   a. Select **Device Management** ( ) to view the devices in the fabric.
   b. Select **Firmware History** from the Actions column for the required device.

   In the **Device Inventory** page, select **Firmware History** from the Actions column for the required device.

   The firmware history is displayed.
5. To view firmware history of multiple devices, select the check boxes of the required devices and select **Firmware History** from the Devices table menu ⋮.

   Alternatively, in the **Device Inventory** page, select the check boxes of the required devices and select **Firmware History** from the Devices table menu ⋮.

The firmware history is displayed.

Related Links

View Operational History on page 51

View Operational History

Procedure

1. In the **Firmware History** page, select to view Operational History of the required firmware.
2. To view operational history of multiple firmware updates, select the check boxes of the required firmware history and select **Operational History** from the Firmware History table menu .

   The operational history is displayed.

Related Links

View Firmware History on page 50

Network Essentials

XCO 3.2.0 and later releases support the following network essential configurations that are required for creating and configuring fabric networks:

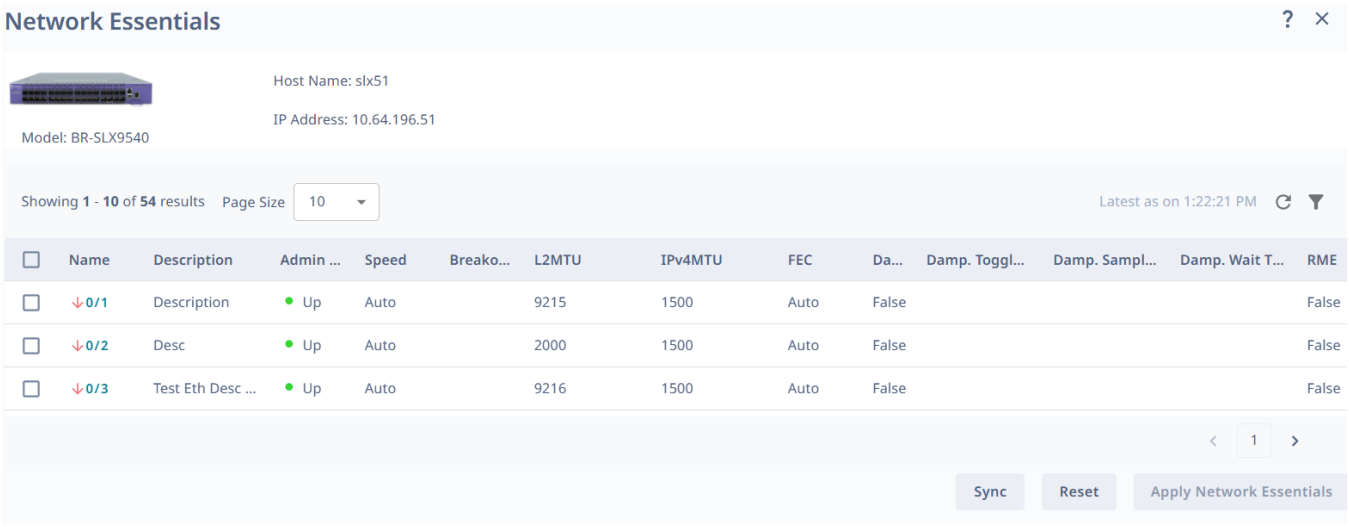
- Description
- Admin State (up/down)
- MTU (L2/Ipv4/Ipv6)
- Speed
- Breakout
- FEC (Forward Error Correction)
- Link Error
- RME (Redundant Management Ethernet)

Configure Network Essentials

Procedure

1. In the Navigation menu, select **Fabrics**.
2. In the Fabrics page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the device Topology page.
3. Select **Device Management** ( ).
4. Select **Network Essentials** from the Actions column (•••) for the required device.
   - Network essential configuration of all ports in the selected device is displayed.
   - You can access **Network Essentials** configurations from both **Device Inventory** and **Fabrics** pages.

5. Edit the required ports.



6. Select **Apply Network Essentials**.

Firmware Upgrade

Before You Begin

- Register firmware host. For more information, see Register Firmware Host on page 89.
- You can use the **Device Inventory** or **Fabrics** page in the user interface to perform firmware upgrade. You can check the firmware download status on both the pages.
- The **Fabrics** page initializes firmware download process with default strategy to determine the grouping of devices for firmware download to achieve least traffic disruption when upgrading a fabric with active traffic.
- You can select single or multiple devices in the fabric for firmware upgrade.
- The **Device Inventory** page supports parallel firmware download requests for any set of devices. However, the parallel firmware download processes on the **Device Inventory** page might lead to traffic loss. Use caution when you select devices on the **Device Inventory** page for firmware download.

About This Task

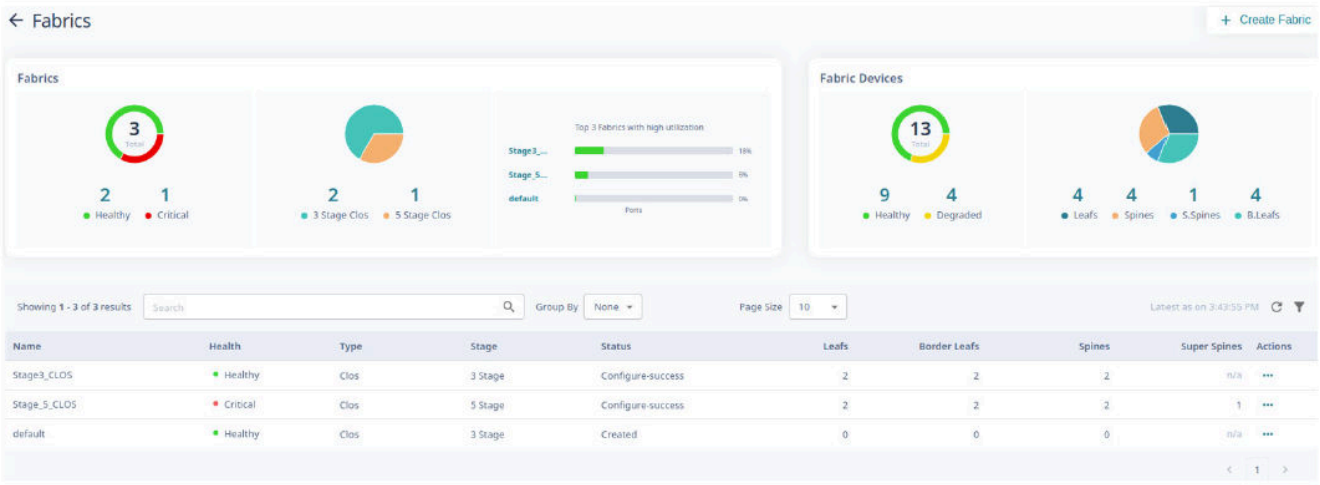
XCO supports firmware download and upgrade across all devices of the fabric.

Note

- As a best practice, do not change the target firmware version file name and the directory name.
- After downloading the firmware on a set of devices, attempt **Activation** and **Commit** from the same page. Switching between the **Device Inventory** page and **Fabrics** page is not supported for an ongoing upgrade cycle.
- If a set of devices that are part of a fabric is undergoing firmware upgrade process from the **Device Inventory** page, you cannot initiate a new firmware upgrade process for another set of devices from the same fabric from the **Fabrics** page.
- If you are upgrading firmware of selected devices from the **Fabrics** page, complete the **Download** and **Activation** process before initiating a new firmware download request on a new set of devices.

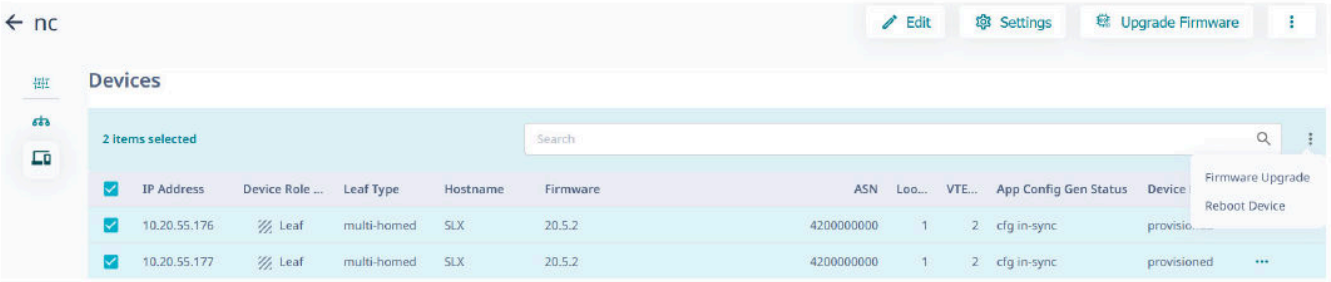
Procedure

1. In the Navigation menu, select **Fabrics**.
2. In the Fabrics page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the device Topology page.



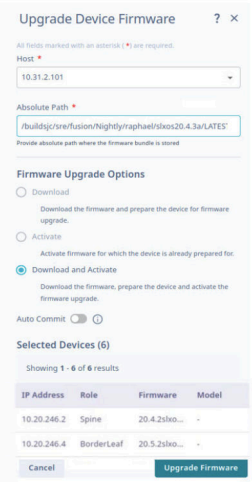
3. (Optional) To upgrade firmware of the selected devices in the fabric, do the following:
   a. In the **Topology** page, go to **Device Management** ( ) to select the check boxes of the required devices.
   b. Select **Firmware Upgrade** from the Actions column (•••) for the device you want to upgrade.

      To upgrade firmware of multiple devices in the fabric, select **Firmware Upgrade** from the Devices table menu ( ).



Skip this step to upgrade all devices in the fabric.

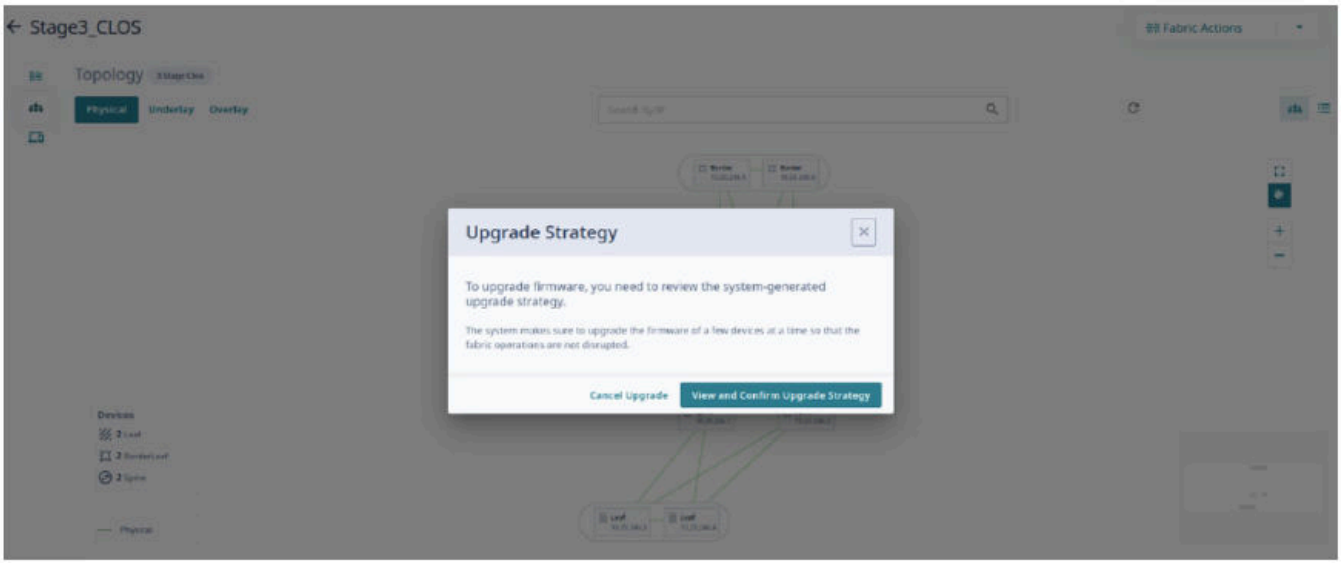
4. Select **Upgrade Firmware** to upgrade all devices in the fabric.

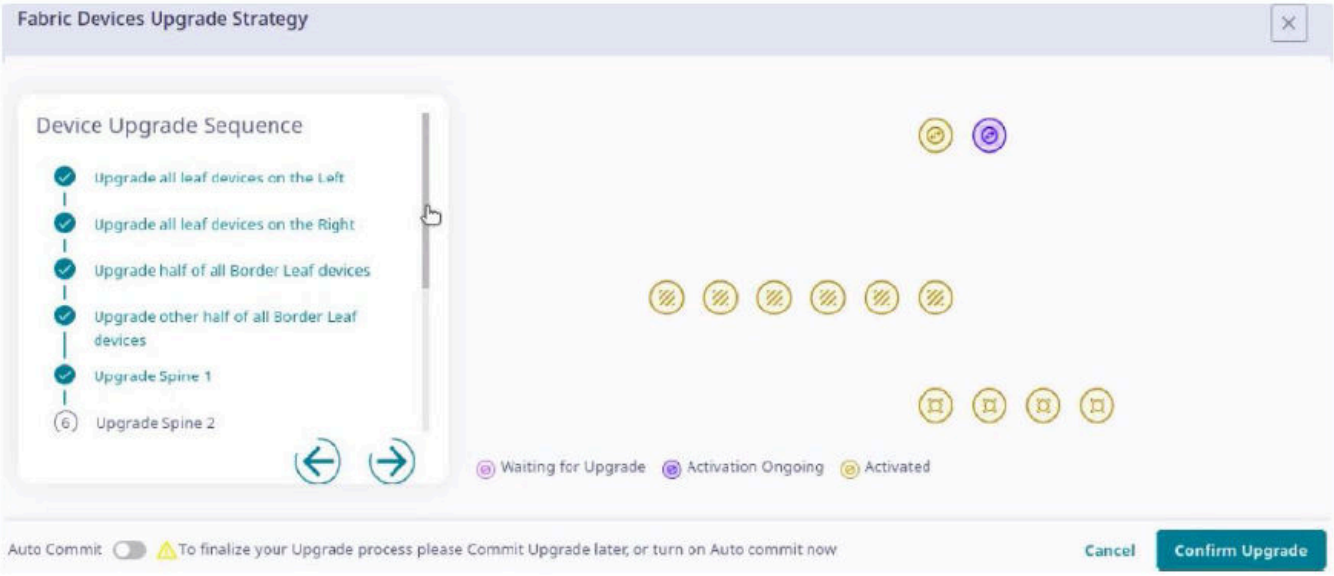


5. In the **Host** field, provide the IPv4 or IPv6 address of the firmware host server.
6. In the **Absolute Path** field, provide the firmware file path.
7. Select **Download and Activate**.
8. (Optional) Activate or deactivate **Auto Commit** as required.

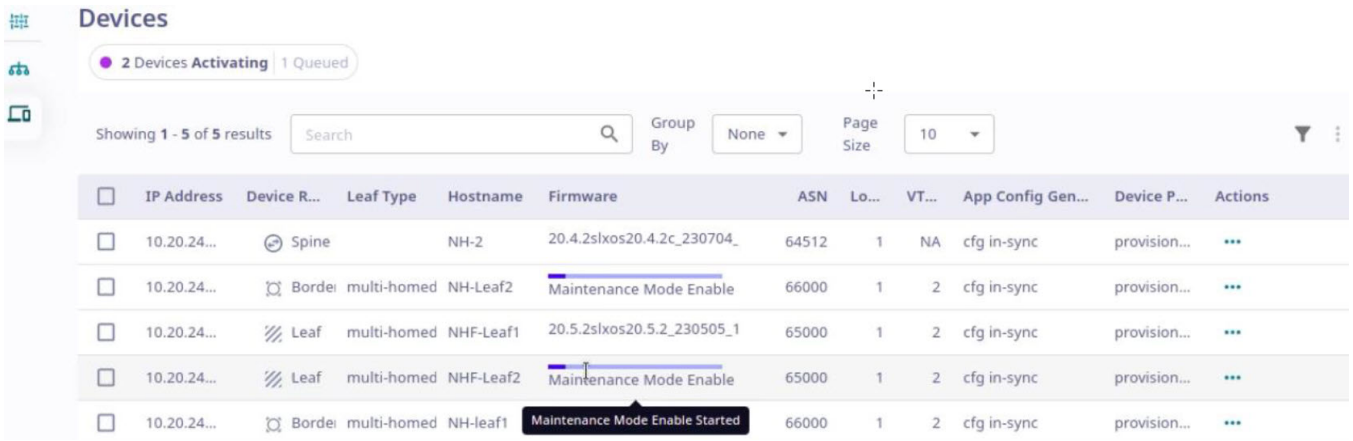
   If Auto Commit is disabled, select **Commit Upgrade** or **Restore Upgrade** from the top of the fabric page to commit the pending devices.
9. Select **Upgrade Firmware**.
   - The list of devices in the fabric is displayed.
   - The LLDP links of the devices in the fabric might go down during firmware download as devices reload and will be in the maintenance mode. This is reflected in the fabric topology view as "No physical links discovered".
   - You are prompted to review the system generated upgrade strategy to minimize traffic disruption to the active fabric.

10. Select **View and Confirm Upgrade Strategy** to review and approve the device upgrade sequence.

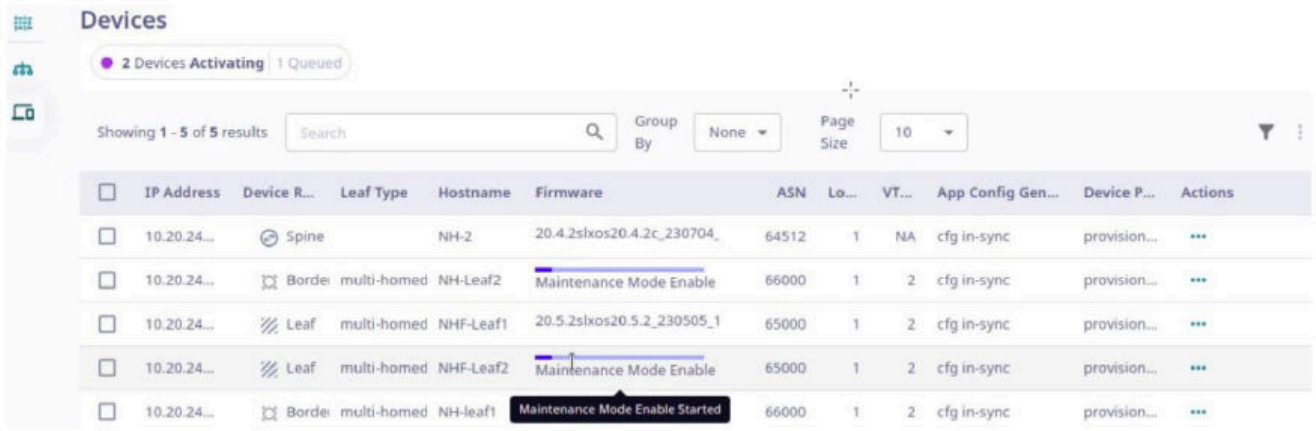




11. Select **Confirm Upgrade**.
    - The list of devices in the fabric along with upgrade status is displayed.



- The device upgrade status indicates various stages such as download, active, and commit. The user interface also provides updates such as the number of devices undergoing upgrade, waiting for upgrade, activation and commit pending, commit upgrade, restore upgrade, and upgrade success.
- To change maintenance mode settings of a device, see Device Settings on page 88.



12. Select **Commit Upgrade** to commit pending devices.

The devices are upgraded to the downloaded firmware version. Refresh the page to view the updated list.

Related Links

Register Firmware Host on page 89
Upgrade Firmware (Device Level) on page 90
View Registered Firmware Hosts on page 90
Edit a Firmware Host on page 90
Delete a Firmware Host on page 90
View Firmware History on page 50
View Operational History on page 51

Clone a Fabric

About This Task

You can clone (copy) a fabric to create a new fabric with the same or similar topology.

Procedure

1. In the Navigation menu, select **Fabrics**.
2. In the Fabrics page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the device Topology page.
3. Select **Clone** ( ) from the fabric menu ( ).
4. Enter a name for the new fabric.
5. Select **Clone**.

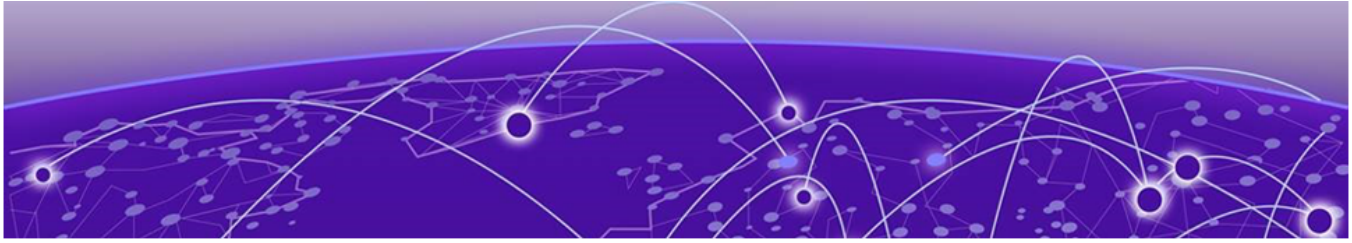
Reboot a Device

About This Task

You can reboot devices from both **Device Inventory** and **Fabrics** pages.

Procedure

1. In the Navigation menu, select **Fabrics**.
2. In the Fabrics page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the device Topology page.
3. Select **Device Management** ().
4. Select **Reboot Device** from the Actions column (•••) for the device you want to reboot.
   - The device is rebooted.
   - To reboot multiple devices, select the check boxes of the required devices and select **Reboot Device** from the Devices table menu ( ).
5. Select **Confirm** when prompted to reboot the device.

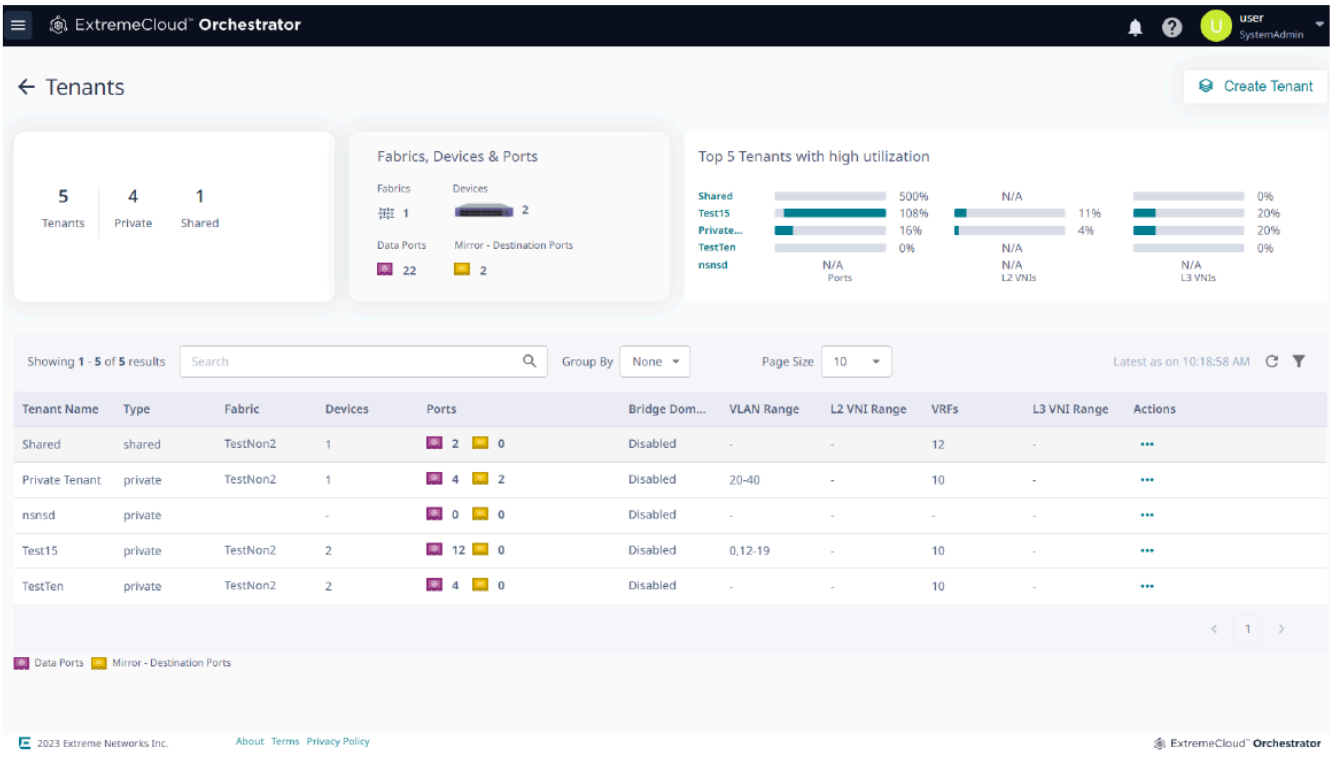


Tenants

XCO 3.4.0 and later releases support tenant management. The XCO user interface allows provisioning of tenants, tenant port-channels, tenant VRFs, tenant BGP peer-groups, and tenant BGP peers. The Tenants overview page varies depending on the logged-in user role.

The **Tenants** page displays the list of tenants the logged-in FabricAdmin or TenantAdmin is authorized to view. For more information about user roles, see User Roles on page 95.

Tenant network configuration includes VLAN, Bridge Domain (BD), Virtual Ethernet (VE), Ethernet VPN (EVPN), VXLAN Tunnel Endpoint (VTEP), Virtual Routing and Forwarding (VRF), and router BGP configuration on fabric devices to provide Layer 2 extension, Layer 3 extension across the fabric.



Create Tenant

Before You Begin

Users with SystemAdmin and FabricAdmin roles can create, edit, and delete tenants.

About This Task

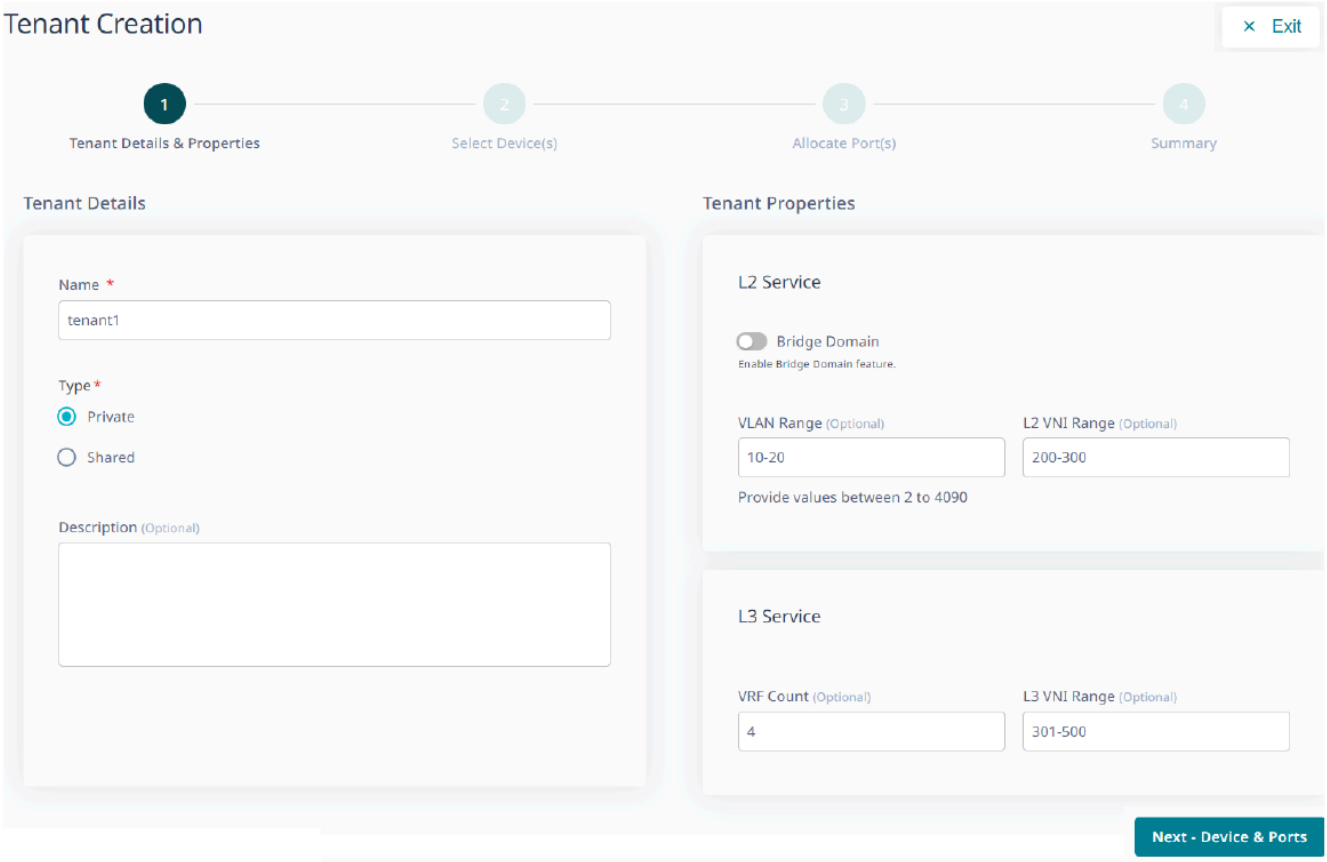
You can create both Shared and Private tenants.

Procedure

1. In the Navigation menu, select **Tenants**.
2. In the Tenants page, select **Create Tenant**.
3. Enter the **Tenant Details**:
   - In the **Name** field, enter a name for the tenant.
   - In the **Type** field, select the tenant type, **Shared** or **Tenant**.
   - Configure **L2 Service** properties:
     - Activate or deactivate **Bridge Domain**.
     - Enter the **VLAN Range**.
     - Enter the **L2 VNI Range**.
   - Configure **L3 Service** properties:
     - Enter the **VRF Count**.

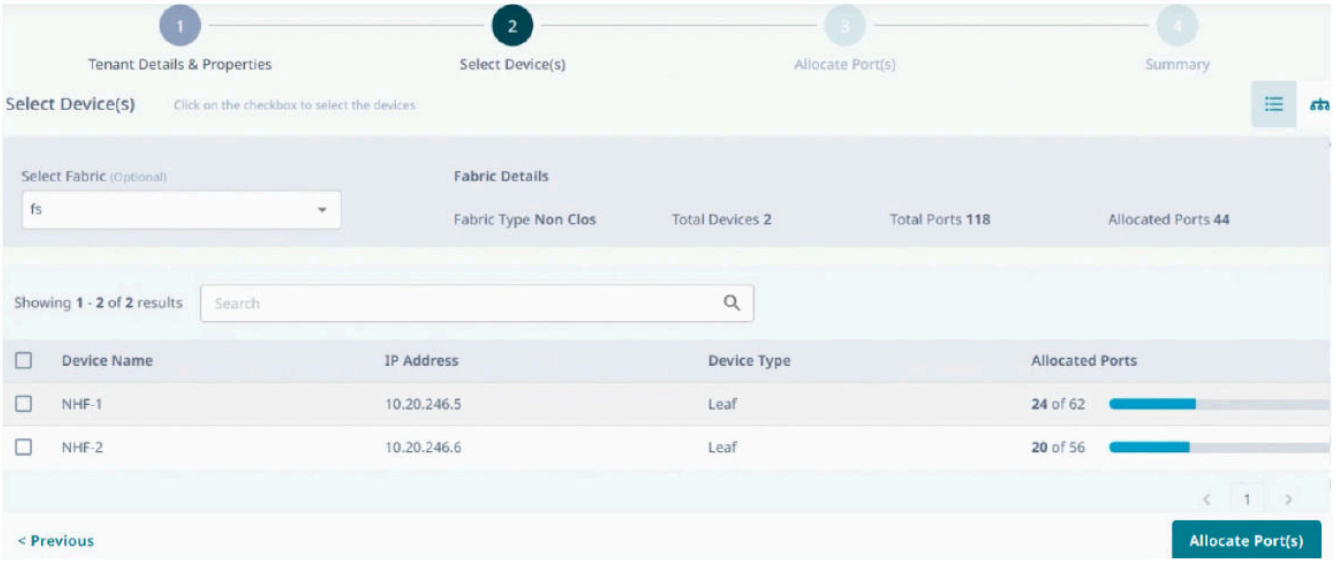
- Enter the **L3 VNI Range**

Note
L2 VNI Range and **L3 VNI Range** are required only for **Map VNI Auto** disabled fabrics.



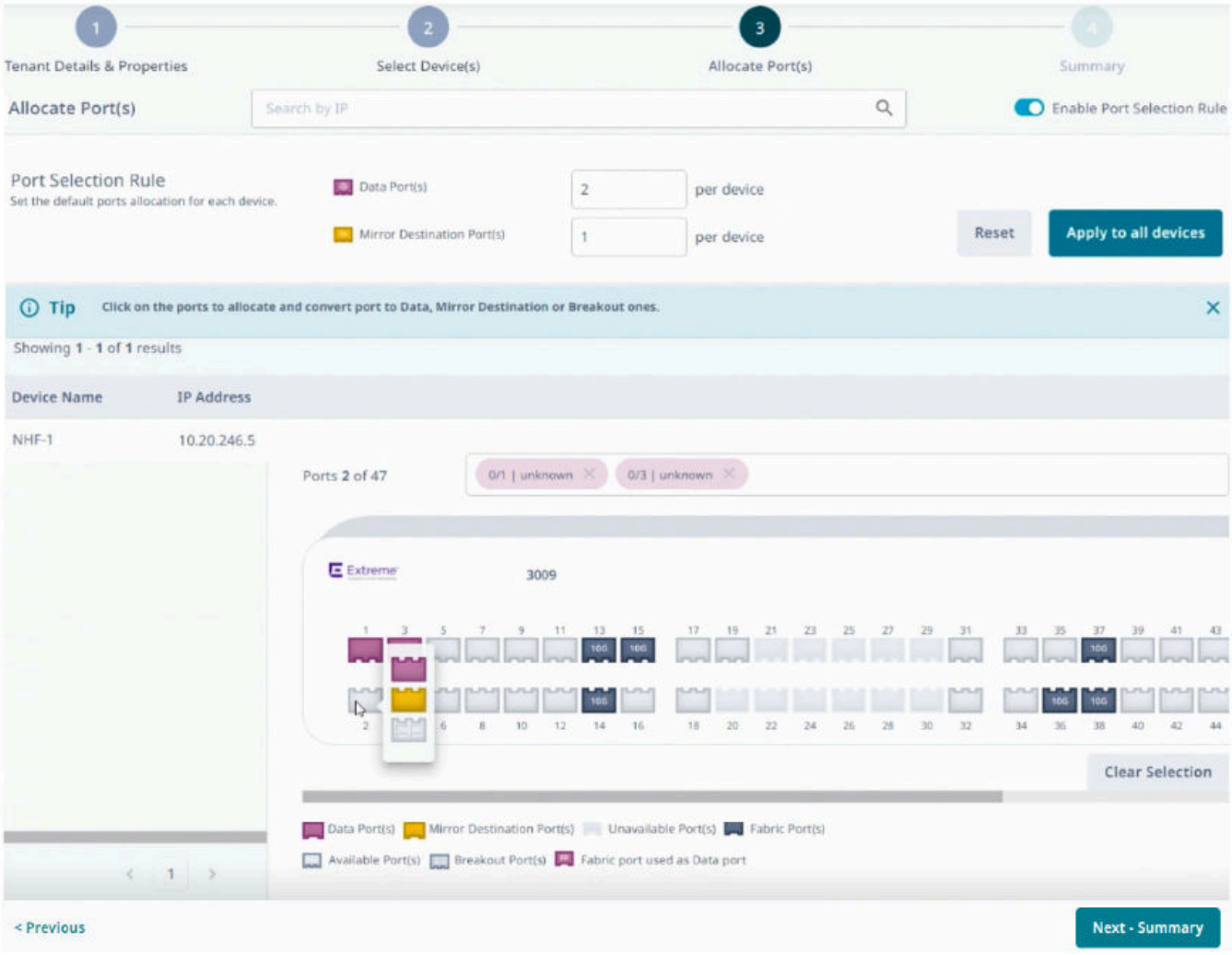
4. Select **Next - Device & Ports**.

5. In the **Select Devices** page, do the following:



- (Optional) Select the required fabric from the **Select Fabric** drop-down menu.
- Select the check boxes of the required devices in the fabric to span the tenant.
- Use **Topology View** ( ) and **List view** ( ) to switch the view between topology and list.
- To enlarge the topology to the width of the interface, select **Expand** ( ).
- To zoom in and out on the topology screen, use the **Zoom** ( ) icons.
- To scroll through the topology screen, use the **Scroll** ( ) icon.

6. Select **Allocate Port(s)**.



7. (Optional) Activate **Enable Port Selection Rule** to auto select the available ports based on the port selection rule.

   You can create port selection rule to select uniform number of ports across all devices. Proceed to the next step to create a port selection rule. Else, go to step 9.

8. (Optional) In the **Port Selection Rule** section, configure the ports allocation for each device.

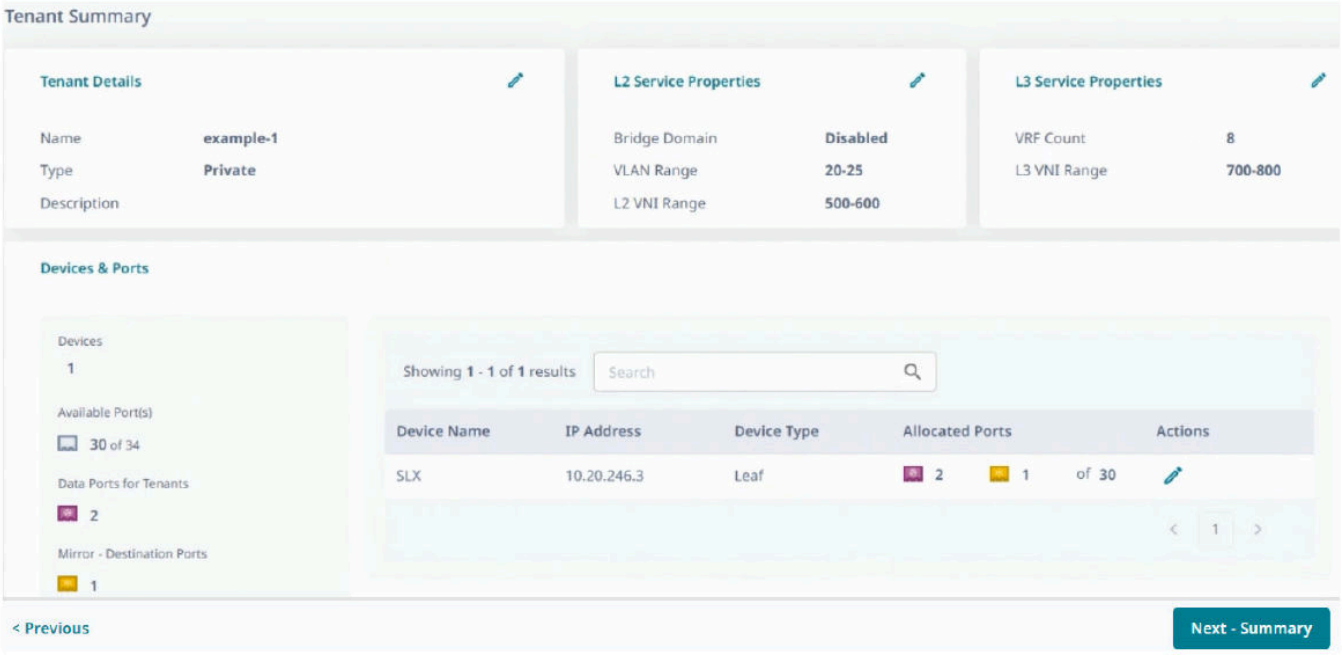
   a. Select the required number of **Data Port(s)** for auto allocation.

   b. Select the required number of **Mirror Destination Port(s)**.

   c. Select **Apply to all Devices**.

   If the available ports do not meet the requirement input in the **Port Selection Rule**, an error message is displayed. Correct the port selection rule to proceed to the next step.

9. Select the required port in the rack to allocate and change the port type: **Data Port**, **Mirror Destination Port**, or **Breakout Port**.
   - You can manually update the ports allocated using the **Port Selection Rule**, if required.
   - XCO supports breakout ports. The breakout ports are indicated as four sub-ports within a single port. The breakout ports are suffixed with `:1-4`.
   - The ports that are allocated to other tenants or fabrics are marked as **Unavailable Ports**.
10. Select **Next - Summary** to verify tenant details.
11. In the **Tenant Summary** page, select  to modify tenant details as required.



12. Select **Create Tenant**.

    The tenant is created.

Related Links

Edit Tenant on page 64
Delete Tenant on page 65

Edit Tenant

Before You Begin

Users with SystemAdmin and FabricAdmin roles can create, edit, and delete tenants.

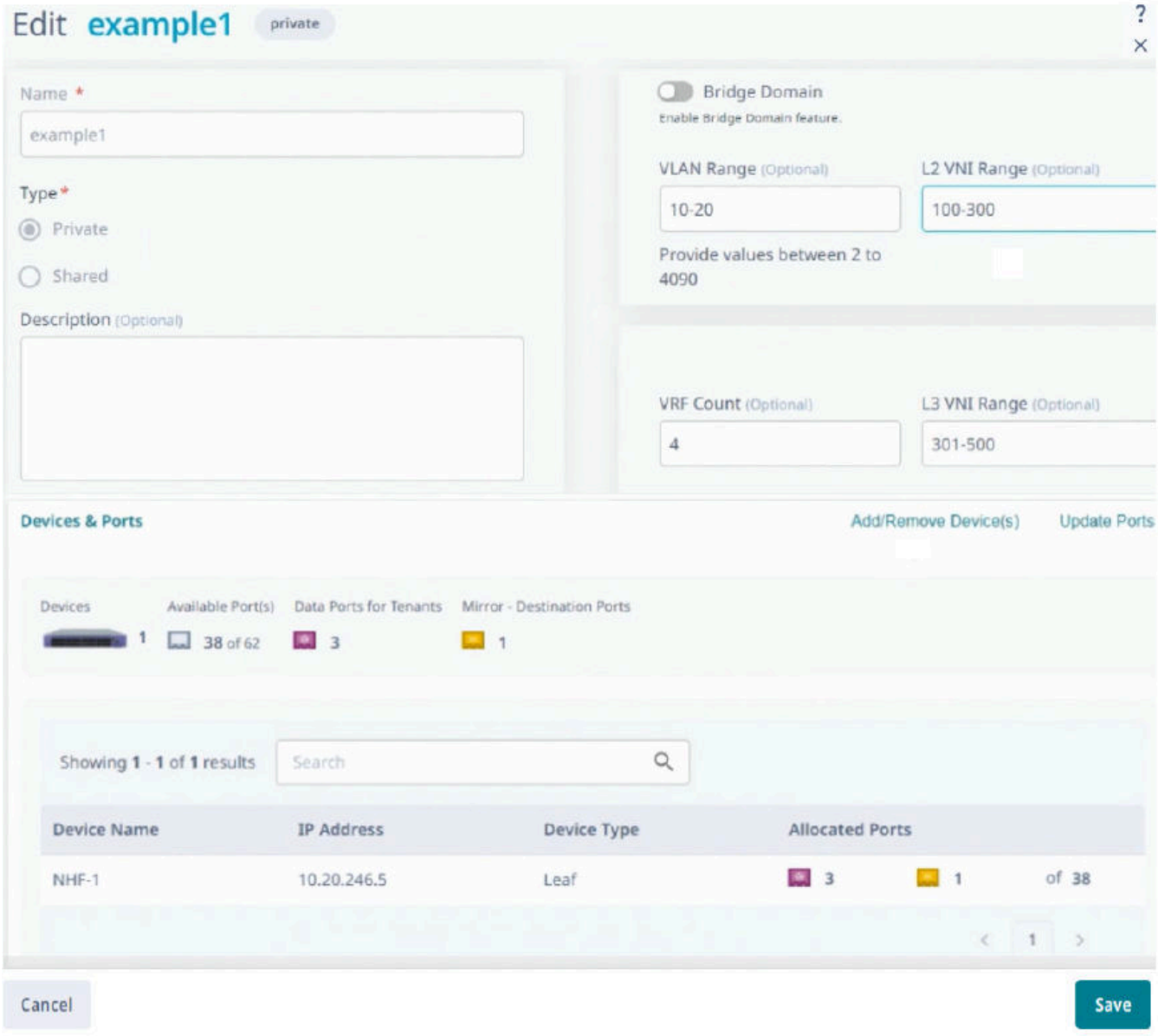
Procedure

1. In the Navigation menu, select **Tenants**.
2. In the Tenants page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the tenant Overview page.

3. Select **Edit**.

   Alternatively, In the **Tenants** page, you can select **Edit** ( ) from the Actions column (•••) for the tenant you want to edit.
4. Update the tenant settings as required.

   You can add or remove devices and update ports.



5. Select **Save**.

Delete Tenant

Before You Begin

Users with SystemAdmin and FabricAdmin roles can create, edit, and delete tenants.

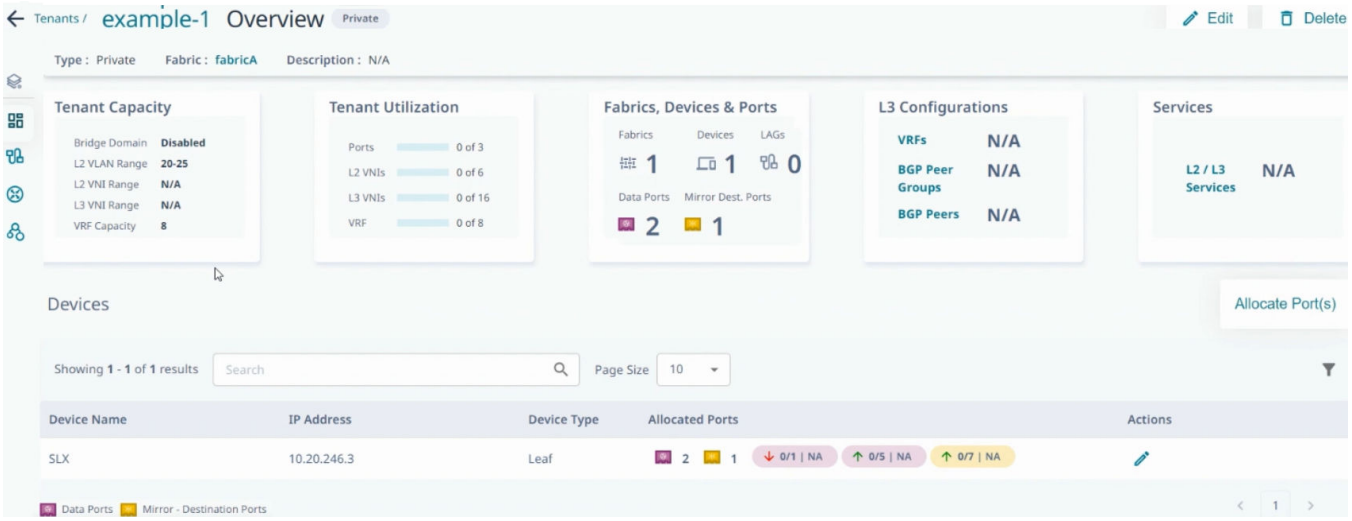
Procedure

1. In the Navigation menu, select **Tenants**.
2. In the Tenants page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the tenant Overview page.
3. Select **Delete**.

   Alternatively, in the **Tenants** page, select **Delete** ( ) from the Actions column (•••) for the tenant you want to delete.
4. Select **Confirm** when prompted.

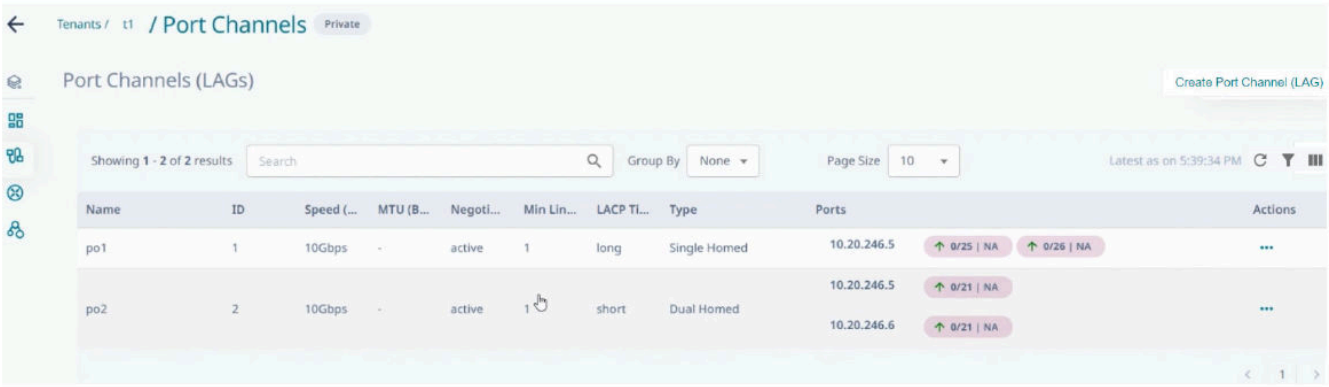
Overview

The **Tenant Overview** ( ) page shows resources and entities associated with the tenant. Use **Tenant Options** ( ) to expand or collapse the tenant navigation menu.



Port Channels (LAGs)

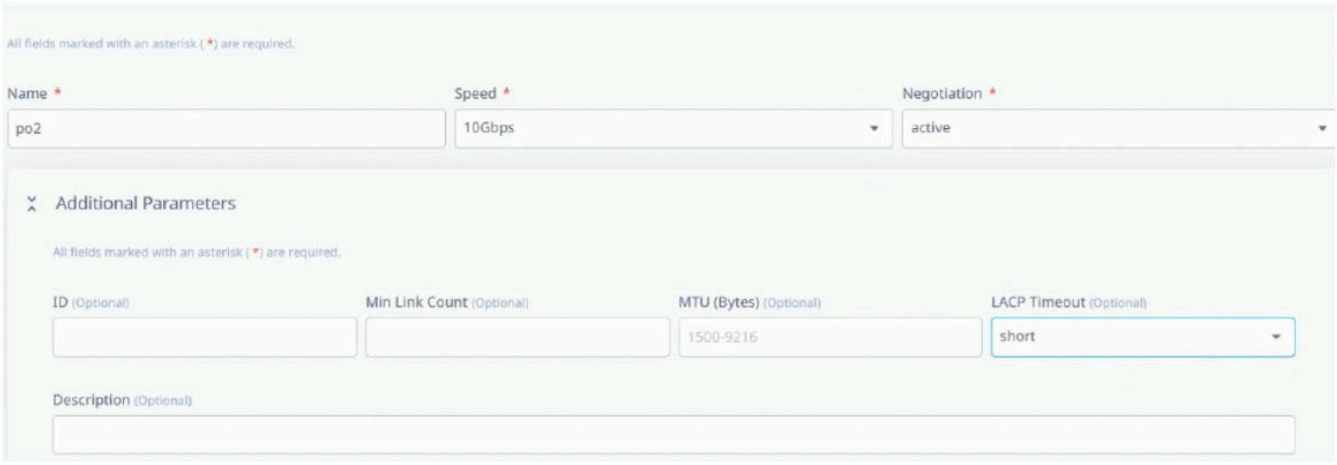
A port channel, also known as a Link Aggregation Group (LAG), allows you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as a single link, which increases fault tolerance and provides load sharing.



Create Port Channel or LAG

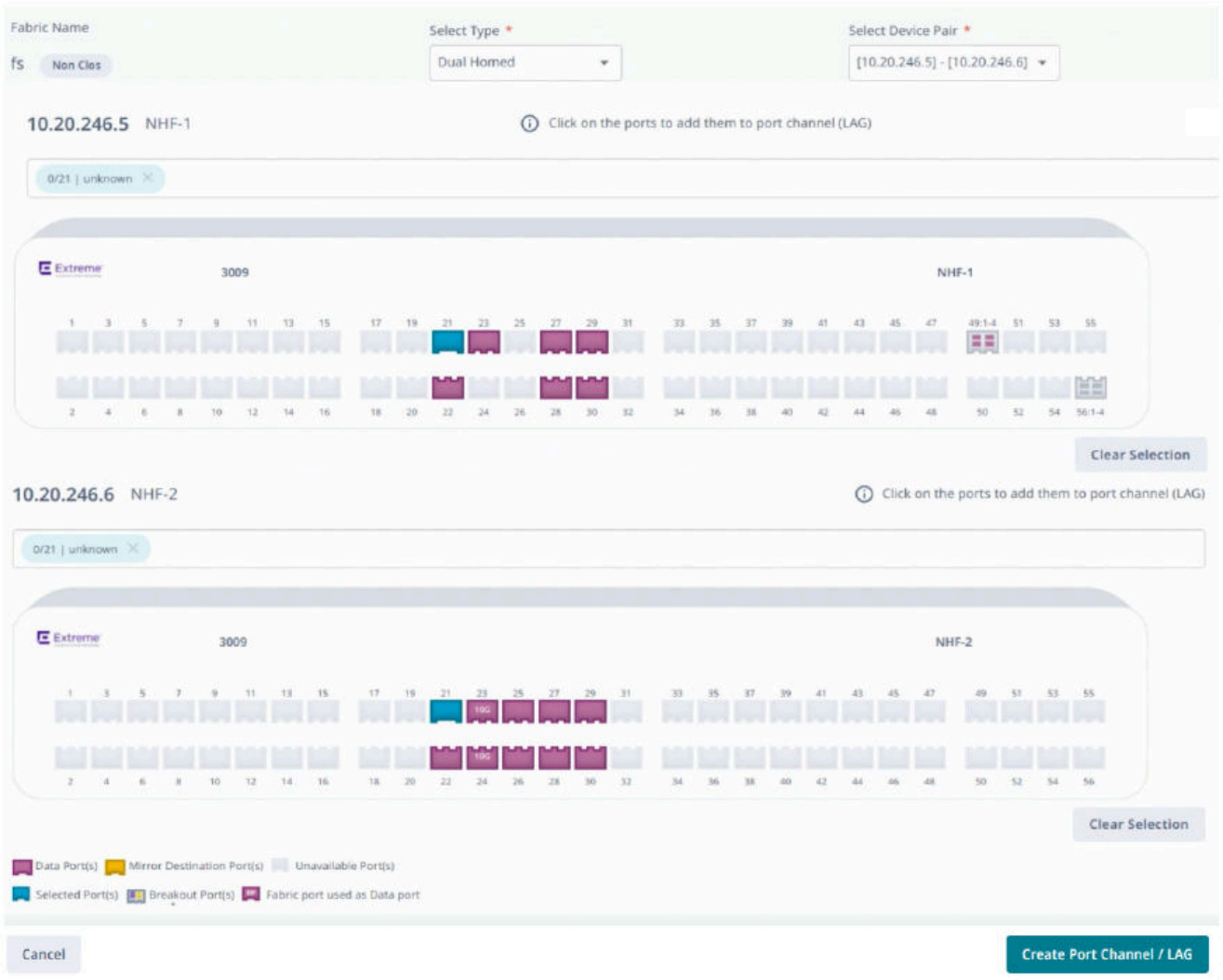
Procedure

1. In the Navigation menu, select **Tenants**.
2. In the Tenants page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the tenant Overview page.
3. In the Tenant Navigation menu, select **Port Channels (LAG)** ( ).
4. Select **Create Port Channel (LAG)**.



5. In the **Name** field, enter a unique name for the port channel.
6. In the **Speed** field, select the required speed for the ports.
   - **100Mbps**
   - **1Gbps**
   - **10Gbps**
   - **25Gbps**
   - **40Gbps**
   - **50Gbps**
   - **100 Gbps**

7. In the **Negotiation** field, select the negotiation value.
   - **active**
   - **passive**
   - **static**
8. (Optional) Enter the **Additional Parameters** as required.
   - **ID**: Unique numeric ID for the port channel
   - **Min Link Count**: Minimum number of interfaces that the port channel requires to be active
   - **MTU (Bytes)**: Maximum transmission unit for packets that pass through the ports in the channel
   - **LACP Timeout**: Timeout value in seconds
   - **Description**: Port channel description
9. (Optional) In the **Description** field, provide a description for the port channel.
10. In the Fabric section, select the port channel **Type**:
    - **Single Homed**: Port channel members are from to a single homed device or a single device of the dual homed MCT pair.
    - **Dual Homed**: Port channel members are from both the devices of the dual homed MCT pair.



11. Select the **Device** (Single homed) or **Device Pair** (Dual homed) for the port channel.

    The port layout of the selected device is displayed.
12. Select member ports for the port channel.

    All ports owned by the tenant (including shared tenants) and the ports that are not associated with any of the port channels or services (EPGs) will be available for member port selection.
13. Select **Create Port Channel (LAG)**.

Related Links

Edit Port Channel on page 69
Delete Port Channel on page 70

Edit Port Channel

Procedure

1. In the Navigation menu, select **Tenants**.

2. In the Tenants page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the tenant Overview page.
3. In the Tenant Navigation menu, select **Port Channels (LAG)** ( ).
4. In the **Port Channels (LAGs)** page, select **Edit** ( ) from the Actions column (•••) for the port channel you want to edit.
5. Follow the instructions in Create Port Channel or LAG on page 67 to update port channel properties and port channel member ports.
6. Select **Update Port Channel**.

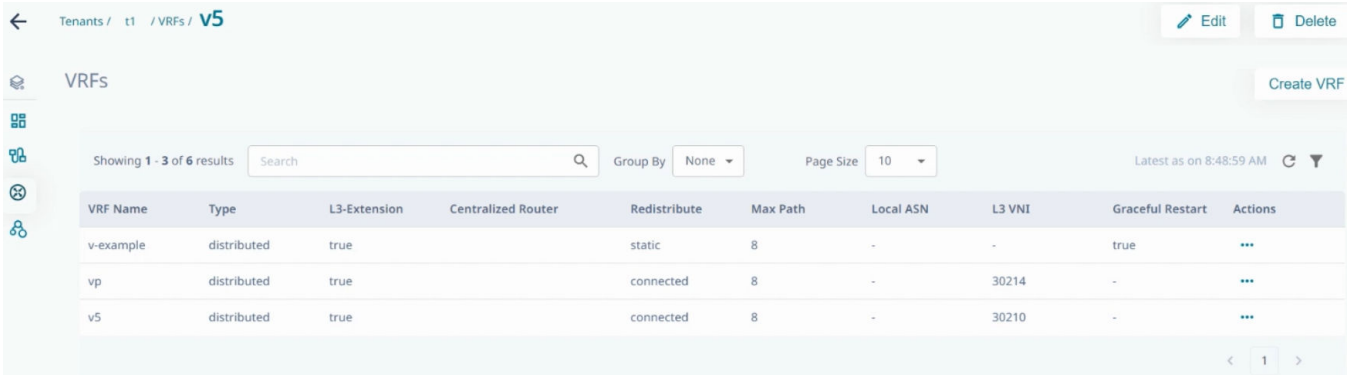
Delete Port Channel

Procedure

1. In the Navigation menu, select **Tenants**.
2. In the Tenants page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the tenant Overview page.
3. In the Tenant Navigation menu, select **Port Channels (LAG)** ( ).
4. In the **Port Channels (LAGs)** page, select **Delete** ( ) from the Actions column (•••) for the port channel you want to delete.
5. Select **Confirm** when prompted.

Virtual Routing and Forwarding (VRF)

Virtual Routing and Forwarding (VRF) is a technology that controls information flow within a network, isolating the traffic by partitioning the network into different logical VRF domains.

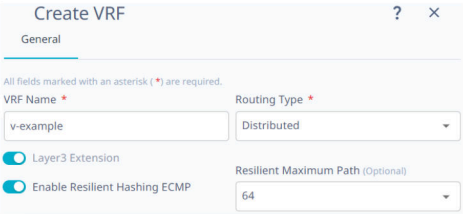


Create VRF

Procedure

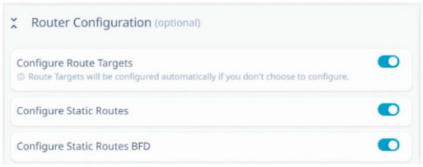
1. In the Navigation menu, select **Tenants**.
2. In the Tenants page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the tenant Overview page.

3. In the Tenant Navigation menu, select **VRF** ( ).
4. Select **Create VRF**.



5. In the **VRF Name** field, enter a unique name for the VRF.
6. In the **Routing Type** field, select the type: **Distributed** or **Centralized**.

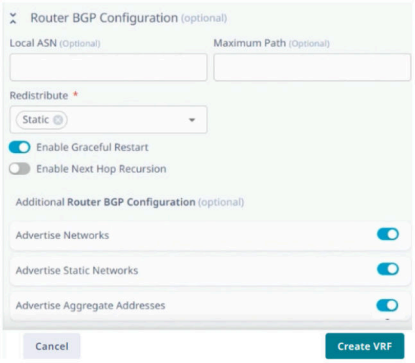
   If you selected centralized routing type, proceed to the next step to select a centralized router. Else skip the next step.
7. In the **Centralized Routers** field, select the required router.
8. Activate or deactivate **Layer3 Extension**.
9. Activate **Enable Resilient Hashing ECMP**.
   a. Select the required value from the **Resilient Maximum Path** drop-down menu.
10. (Optional) In the **Router Configuration** section, activate the route configurations as required:
    - **Configure Route Targets**
    - **Configure Static Routes**
    - **Configure Static Routes BFD**



   The selected router configuration tabs are added to the **Create VRF** window. To configure the route settings, perform step 12 through 14.
11. (Optional) In the **Router BGP Configuration** page, configure the following as required:
    a. (Optional) In the **Local ASN** field, enter the required value.
    b. (Optional) In the **Maximum Path** field, enter the route load-sharing max path.
    c. Select the required **Redistribute** option: **Static** or **Connected**.

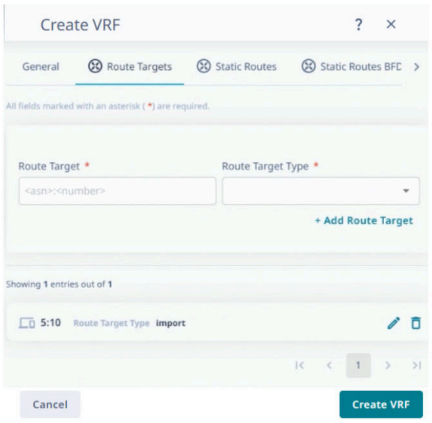
       The default value is **Connected**.
    d. Activate **Enable Graceful Restart**.
    e. Activate **Enable Next Hop Recursion**
    f. (Optional) Activate the **Additional Router BGP Configuration** options:

    - **Advertise Networks**
    - **Advertise Static Networks**
    - **Advertise Aggregate Addresses**



The selected router BGP configuration tabs are added to the **Create VRF** window. To configure the additional BGP settings, perform step 15 through 17.

12. Select the **Route Targets** tab to configure the parameters.
    a. Configure the **Route Targets** parameters.
    b. Select **+ Add Route Target**.



The route target is created.

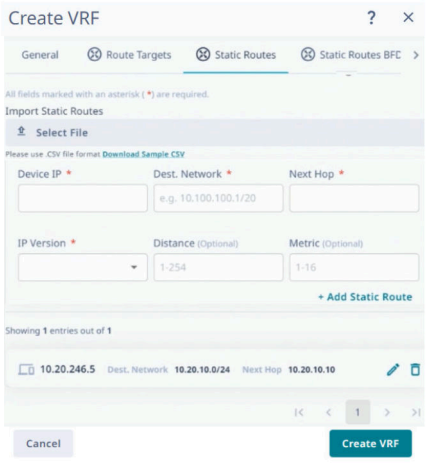
Use the **Edit** ( ) and **Delete** ( ) options to edit and delete the configured route targets.

13. Select the **Static Routes** tab to configure the parameters.
    a. Configure the **Static Route** parameters.
    b. Select **+ Add Static Route**.

The static route is created.

c. To add multiple static routes, use **Select File** and import the static routes.csv file.

Download the sample CSV file to create the static routes.csv file.

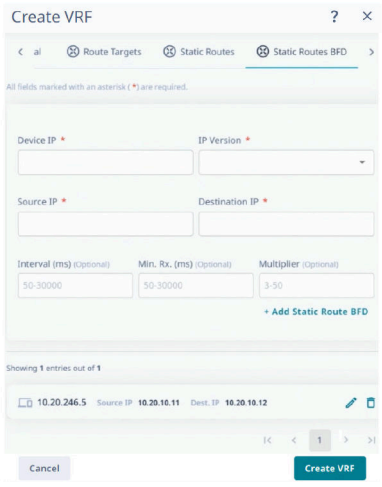


Use the **Edit** ( ) and **Delete** ( ) options to edit and delete the configured static routes.

14. Select the **Static Routes BFD** tab to configure the parameters.
    a. Configure the **Static Routes BFD** parameters.
    b. Select **+ Add Static Route BFD**.

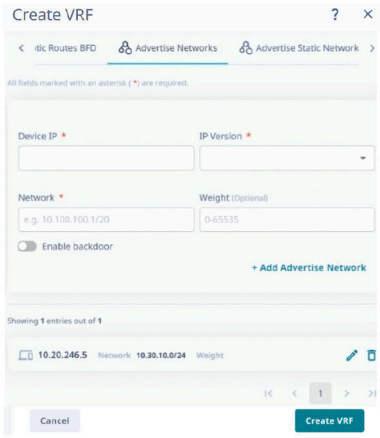
    The static route BFD is created.
    c. To add multiple static routes, use **Select File** and import the static routes.csv file.

    Use the **Edit** ( ) and **Delete** ( ) options to edit and delete the configured static routes.



15. Select the **Advertise Networks** tab to configure the parameters.
    a. Configure the **Advertise Networks** parameters.

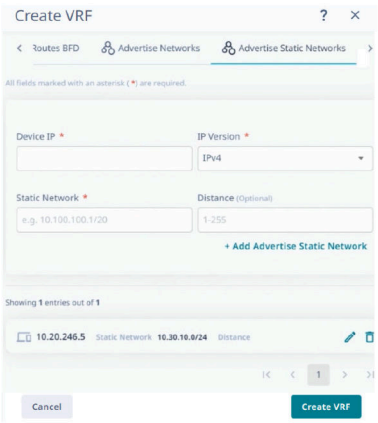
b. Select **+ Add Advertise Network**.



The advertise network is created.

Use the **Edit** ( ) and **Delete** ( ) options to edit and delete the configured static routes.

16. Select the **Advertise Static Networks** tab to configure the parameters.
    a. Configure the **Advertise Static Networks** parameters.
    b. Select **+ Add Advertise Static Network**.

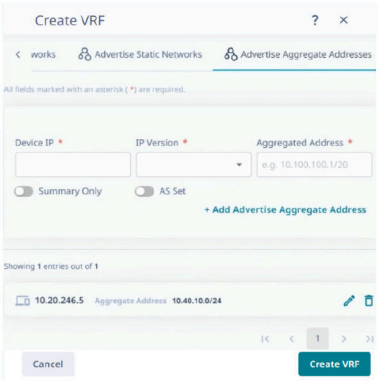


The advertise static network is created.

Use the **Edit** ( ) and **Delete** ( ) options to edit and delete the configured static routes.

17. Select the **Advertise Aggregate Addresses** tab to configure the parameters.
    a. Configure the **Advertise Aggregate Addresses** parameters.
    b. Select **+ Add Advertise Aggregate Address**.

    The advertise aggregate address is created.



Use the **Edit** ( ) and **Delete** ( ) options to edit and delete the configured static routes.

18. Select **Create VRF**.

    The VRF is created.

Related Links

Edit VRF on page 75
Delete VRF on page 75

Edit VRF

Procedure

1. In the Navigation menu, select **Tenants**.
2. In the Tenants page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the tenant Overview page.
3. In the Tenant Navigation menu, select **VRF** ( ).
4. Select **Edit** ( ).

   Alternatively, you can select **Edit** ( ) from the Actions column (•••) for the VRF you want to edit.
5. Follow the instructions in Create VRF on page 70 to update the VRF.
6. Select **Update VRF**.

Delete VRF

Procedure

1. In the Navigation menu, select **Tenants**.
2. In the Tenants page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the tenant Overview page.
3. In the Tenant Navigation menu, select **VRF** ( ).
4. Select **Delete**.

   Alternatively, you can select **Delete** ( ) from the Actions column (•••) for the VRF you want to delete.

5. Select **Confirm** when prompted.

Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) is a routing protocol, which establishes routing between ISPs. ISPs use BGP to exchange routing information between Autonomous Systems (ASs) on the Internet.

BGP peers (also referred to as neighbors) are BGP enabled devices that are directly connected through an established TCP connection. The BGP dynamic neighbors allow peering to a group of remote neighbors defined by a listen range. BGP neighbors can be created without statically configuring them.

A BGP peer group groups the BGP neighbors sharing the same outbound policies together. A peer group allows you to group the policies which can be applied to individual peers thus making efficient update calculation along with simplified configuration.

Create BGP Peer Group

Procedure

1. In the Navigation menu, select **Tenants**.
2. In the Tenants page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the tenant Overview page.
3. In the Tenant Navigation menu, select **BGP** ( ).
4. Select the **BGP Peer Groups** tab.
5. In the **BGP Peer Groups** tab, select **Create BGP Peer Group**.
6. In the **Group Name**, enter a name for the BGP peer group.
7. In the **Device(s)** drop-down menu, select the required devices.
8. Enter a value for **Remote As**.
9. Enable **BFD** and configure the BFD parameters as required.
10. Complete the fields as required.
11. Enable **Remote Private AS**.
12. (Optional) Select a value from the **Send Community** drop-down menu.
13. Select **Create BGP Peer Group**

Related Links

Edit BGP Peer Group on page 76
Delete BGP Peer Group on page 77

Edit BGP Peer Group

Procedure

1. In the Navigation menu, select **Tenants**.
2. In the Tenants page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the tenant Overview page.

3. In the Tenant Navigation menu, select **BGP** ( ).
4. Select the **BGP Peer Groups** tab.
5. In the **BGP Peer Groups** page, select **Edit** ( ) from the Actions column ( ) for the group you want to edit.
6. Follow the instructions in Create BGP Peer Group on page 76 to update the VRF.
7. Select **Save BGP Peer Group**.

Delete BGP Peer Group

Procedure

1. In the Navigation menu, select **Tenants**.
2. In the Tenants page, click anywhere in the required fabric row except the Actions column ( ) to proceed to the tenant Overview page.
3. In the Tenant Navigation menu, select **BGP** ( ).
4. Select the **BGP Peer Groups** tab.
5. In the **BGP Peer Groups** page, select **Delete** ( ) from the Actions column ( ) for the group you want to delete.
6. Select **Confirm** when prompted.

Create BGP Peer

Procedure

1. In the Navigation menu, select **Tenants**.
2. In the Tenants page, click anywhere in the required fabric row except the Actions column ( ) to proceed to the tenant Overview page.
3. In the Tenant Navigation menu, select **BGP** ( ).
4. Select the **BGP Peers** tab.
5. Select **Create BGP Peer**.
6. In the **Name** field, enter a name for the BGP peer.
7. In the **Device(s)** drop-down menu, select the required devices.
8. Select the required **VRF**.
9. Select the BGP peer **Type**:
   - **Static**: Go to step 10 to create a Static BGP Peer.
   - **Dynamic**: Go to step 11 to create a Dynamic BGP Peer.

   The options vary by the BGP peer type.
10. Configure the required **Static** BGP peer parameters.
    a. Enter the **Neighbor IP** address.

       XCO 3.4.0 and later releases support only one **Neighbor IP** configuration.
    b. Select the required **Remote As** value.
    c. Configure the required **Detailed Configuration** parameters.

d. Configure the required **Additional Path** parameters.
e. Configure the required **Multi Protocol Capability** parameters.
f. Select **Create BGP Peer**.

11. Configure the required **Dynamic** BGP peer parameters.
    a. Enter the **Listen IP Address Range**.
    b. Select the required peer group from the **Peer Group Name** drop-down menu.
    c. Select **Create BGP Peer**.

Related Links

Edit BGP Peer on page 78
Delete BGP Peer on page 78

Edit BGP Peer

Procedure

1. In the Navigation menu, select **Tenants**.
2. In the Tenants page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the tenant Overview page.
3. In the Tenant Navigation menu, select **BGP** ( ).
4. Select the **BGP Peers** tab.
5. In the **BGP Peers** page, select **Edit** ( ) from the Actions column (•••) for the BGP peer you want to edit.
6. Follow the instructions in Create BGP Peer on page 77 to update the BGP peer.
7. Select **Save BGP Peer**.

Delete BGP Peer

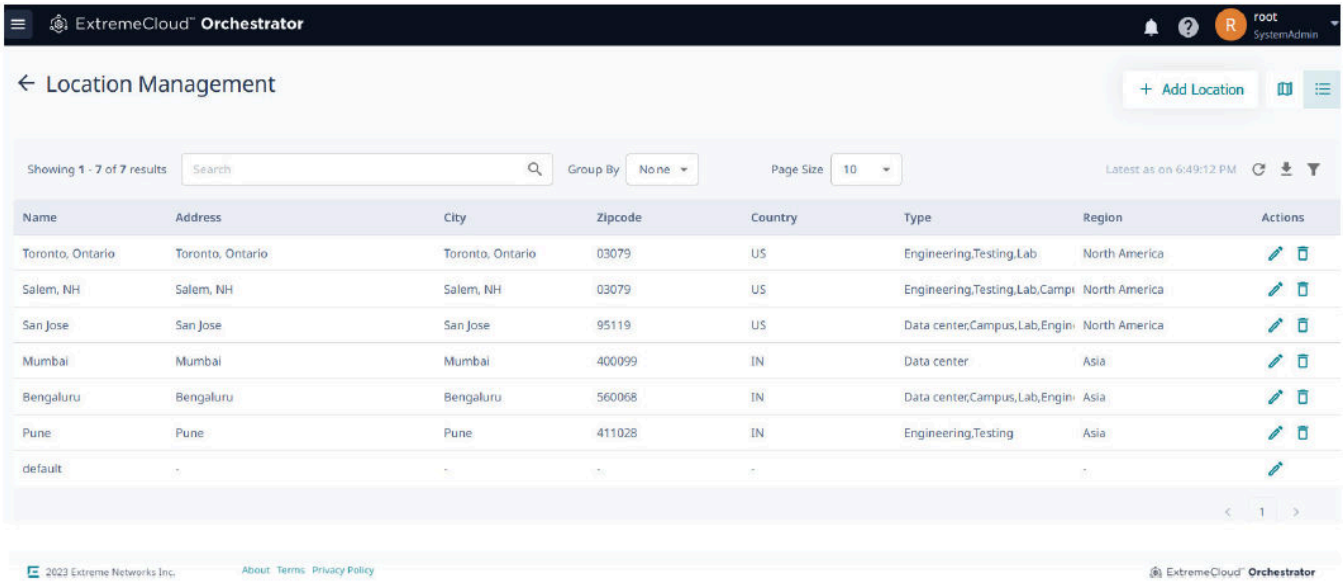
Procedure

1. In the Navigation menu, select **Tenants**.
2. In the Tenants page, click anywhere in the required fabric row except the Actions column (•••) to proceed to the tenant Overview page.
3. In the Tenant Navigation menu, select **BGP** ( ).
4. Select the **BGP Peers** tab.
5. In the **BGP Peer** page, select **Delete** ( ) from the Actions column (•••) for the BGP peer you want to delete.
6. Select **Confirm** when prompted.

Locations

The **Location Management** page allows you to view and manage devices from different geographical locations. A default location is created during the XCO boot up which can be used for small deployments.

XCO manages the region, site, or location information for categorizing the devices by their physical location.



Note

- The default location cannot be modified or deleted.
- When an existing location is deleted, all its devices are moved to the default location.
- The device location cannot be modified after discovery.

Add Location

About This Task

The Location Definition file (in CSV format) identifies geographical locations.

After XCO is installed, you can upload the CSV file to the interface. For information about deploying XCO, see the *ExtremeCloud Orchestrator Deployment Guide, 4.0.2*.

Procedure

1. In the Navigation menu, select **Locations**.

   The **Location Management** window opens.
2. Select **Add Location**.

   The **Add New Location** window opens.
3. To add new locations manually, take the following steps:
   a. Select **Add Address** and type the following information:
      - Name
      - Type
      - Region
      - Street Address
      - Country
      - State
      - City
      - Zipcode
      - Latitude
      - Longitude

      Note
      All the above mentioned fields are mandatory to add a new location.

   b. Select **Add**.
4. To import the `locations.csv` file, do the following:
   a. Select **Import Location**.
   b. Click **Select File**.

      Use the sample .CSV file provided to create a .CSV file with all the location details.
   c. Upload the .CSV file.
   d. Select **Add**.

Related Links

Edit Location on page 81
Download Location Definition File on page 81
Delete Location on page 81
Display Location-Specific Device List on page 81
Display Locations Map View on page 82

Edit Location

About This Task

When an existing location is deleted, all associated devices are updated and moved to the default location.

Procedure

1. In the Navigation menu, select **Locations**.
2. In the **Location Management** page, select **Edit** ( ) from the Actions column (•••) for the location you want to modify.
3. Follow the instructions in Add Location on page 80 to change the location details.
4. Select **Add**.

Download Location Definition File

About This Task

The Location Definition file (in CSV format) identifies regions and their associated zones and managed locations.

Procedure

1. In the Navigation menu, select **Locations**.
2. Select **Download**.
   A file in .csv format is downloaded to your device.

Delete Location

About This Task

When an existing location is deleted, all associated devices are updated and moved to the default location.

Procedure

1. In the Navigation menu, select **Locations**.
2. In the **Location Management** page, select **Delete** ( ) from the Actions column (•••) for the location you want to delete.

Display Location-Specific Device List

Procedure

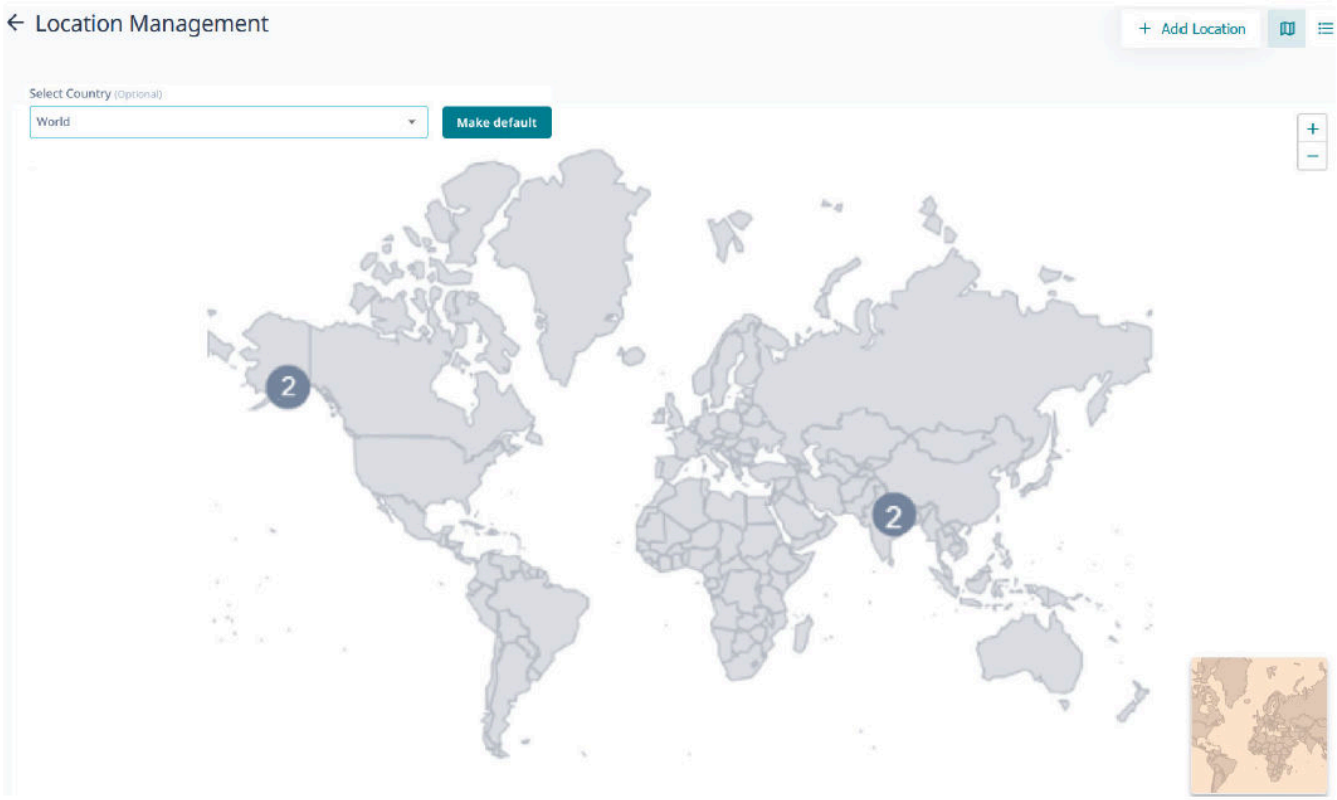
1. In the Navigation menu, select **Locations**.
2. In the **Location Management** page, click anywhere in the location row except the Actions column (•••) to display the list of devices associated with the location.
   To configure and manage devices, see Device Inventory on page 83.

Display Locations Map View

Procedure

1. In the Navigation menu, select **Locations**.
2. In the upper right corner of the **Location Management** page, select  to display the map view.

   The default map view is the list view.

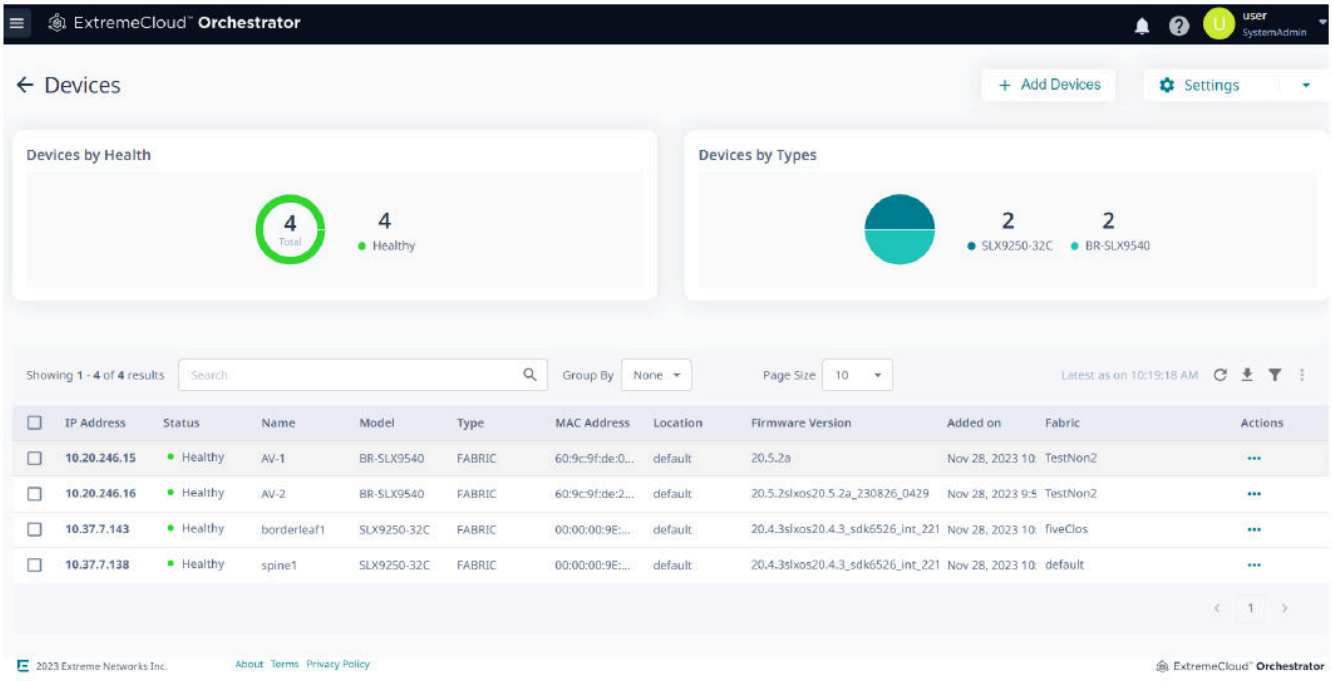


3. Select a country from the drop-down menu to view the country specific location information.
4. (Optional) Select **Make Default** to make the selected country view as the default map view.

Device Inventory

ExtremeCloud Orchestrator supports device discovery based on IP address, user credentials, and location information.

The **Devices** page allows you to view and manage devices.



Device discovery limitations are as follows:

- Hostname or DNS name based device discovery is not supported.
- Device location cannot be modified after discovery.

- If a device configured with both IPv4 and IPv6 addresses is discovered, only one entry is added to ExtremeCloud Orchestrator. The first discovered IP address is used for communicating with that device.

Device Credentials

The device credentials are stored in the Inventory Service database. All other microservices retrieve device credentials from the Inventory Service.

Add Devices

Before You Begin

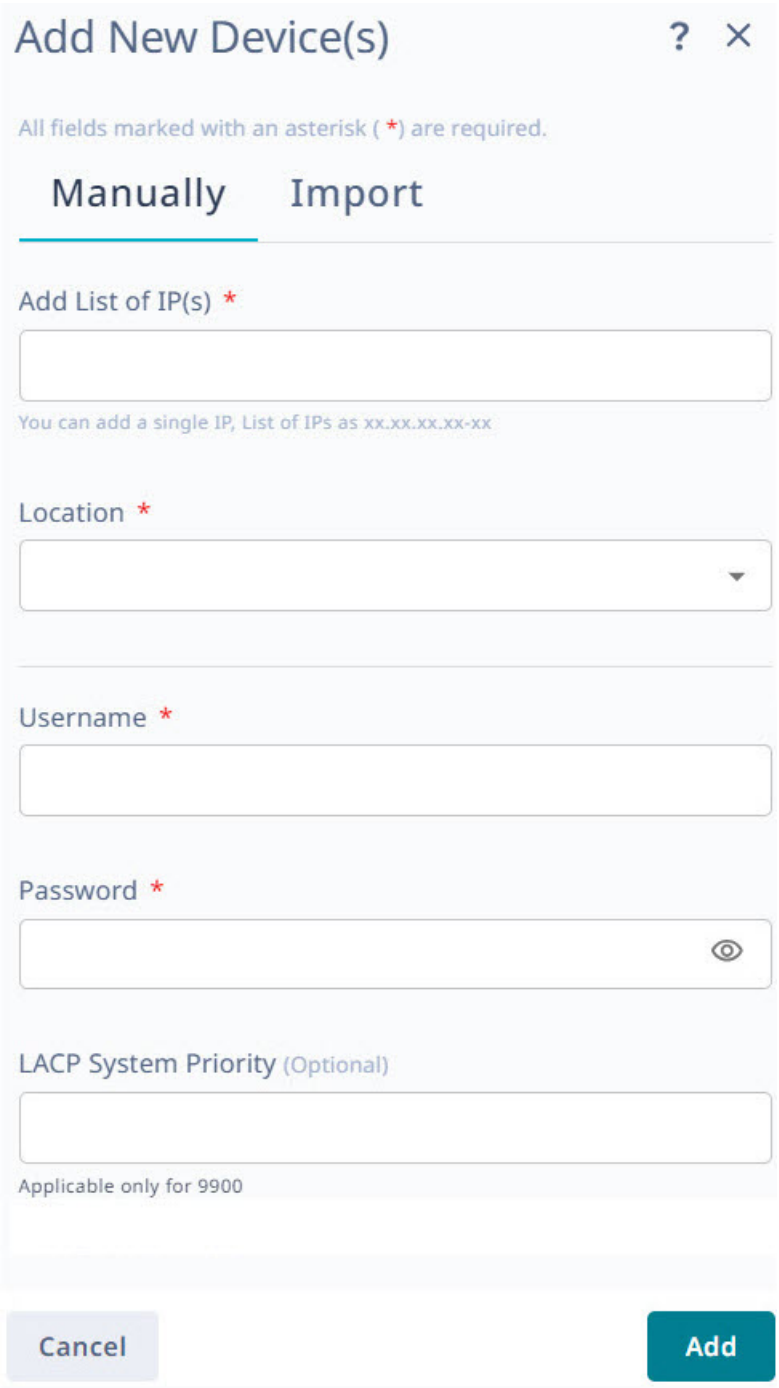
- To be able to add multiple devices in bulk, create a Device Definition File, a CSV file that specifies the devices that you want to add. For more information, see Create a Device Definition File on page 87.
- The MLX devices must be configured for SSH as they are not AAA enabled and do not have the default user name and password.

About This Task

When a device is discovered, the device state is updated as `In Progress`. If the device connection is not successful, the appropriate error message is added to the notifications page.

Procedure

1. In the Navigation menu, select **Device Inventory** > **Add Devices**.



2. Proceed to step 3 to add devices manually. Else, go to step 4 on page 86 to add multiple devices in bulk.

3. Select **Manually** and complete the following fields to add devices manually:
   a. In the **Add List of IP(s)** field, enter the IPv4 or IPv6 address of the devices.

      You can add a single IP address or a list of IP addresses enclosed in double quotes as shown in the following examples:

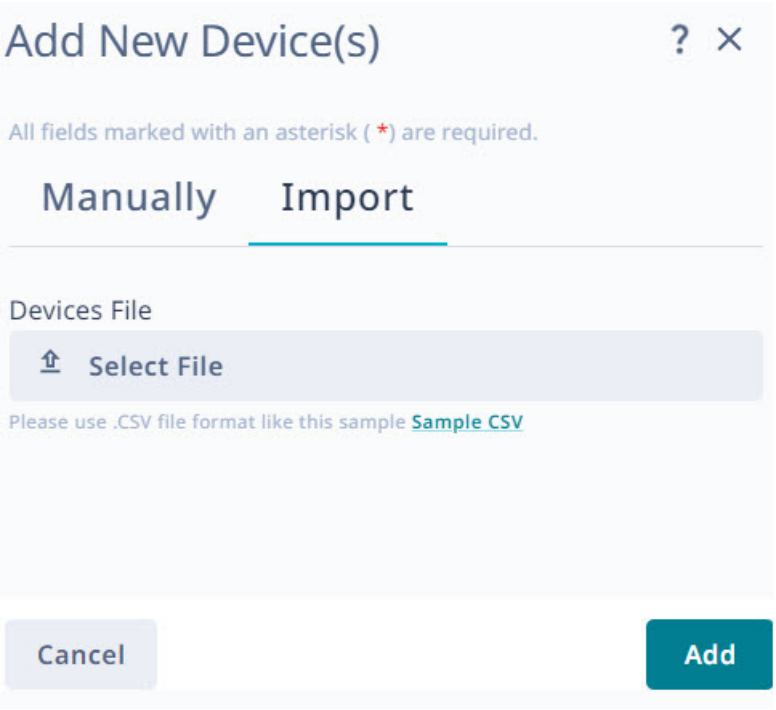
      ```
      1.1.1.1

      "1.1.1.1, 2.2.2.2"
      ```

   b. In the **Location** field, select the location where the device resides.

      - ExtremeCloud Orchestrator 3.2.0 deployed in IP fabric mode supports only the **default** location.
      - XCO creates periodic system backup at scheduled intervals and all services are locked during system backup. For more information, see the *ExtremeCloud Orchestrator CLI Administration Guide, 4.0.2*.

        The location drop-down list will not be available during system backup. This is reflected in the user interface as “Service is Locked with reason backup”.

   c. Enter the **Username** and **Password** information.
4. Select **Import** > **Select File** to browse to the CSV file.



   A sample CSV file template is available for download to create device definition files.
5. Select **Add**.

Create a Device Definition File

A Device Definition file (in CSV format) identifies devices by data such as IP address, location, and credentials.

About This Task

You use a Device Definition file to add multiple devices in bulk. Each row in the CSV file has a variation of the following format.

```
IP_ADDRESS, USER_NAME, PASSWORD, LOCATION, LACP_SYSTEM_PRIORITY
```

Table 7: Field descriptions

Field Number	Field	Description
1	IP_ADDRESS	One or more IPv4 or IPv6 addresses, separated by commas.
2	USER_NAME	Credentials for accessing the device, and not necessarily the credentials of the default user.
3	PASSWORD	Credentials for accessing the device, and not necessarily the credentials of the default user.
4	LOCATION	Specifies the name of a location.

Procedure

1. Create a CSV file with a file name of your choosing.

   Use the **Sample CSV** file available at **Device Inventory** > **+ Add Devices** > **Import** to create the .CSV file.
2. Add content to the .CSV file.
3. Save the CSV file to a location that is accessible from the XCO user interface.

Example

```
IP_ADDRESS,USER_NAME,PASSWORD,LOCATION,LACP_SYSTEM_PRIORITY
2620:100:c:fe08::110,admin,password,Site1,
2620:100:c:fe08::111,admin,password,Site1,
10.37.128.70,admin,password,Site1,
```

Download Bulk Device Inventory

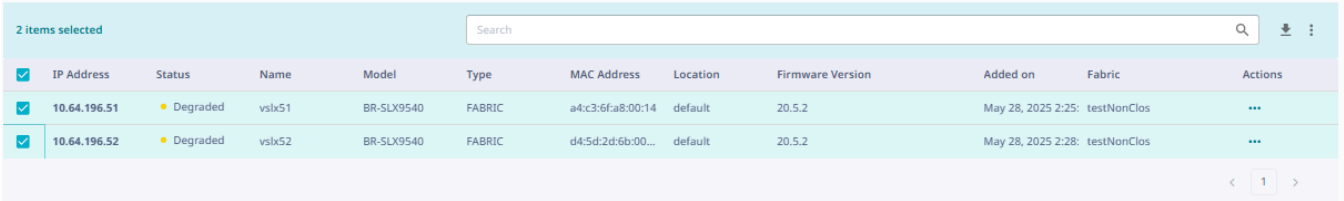
You can download multiple or bulk device inventory information.

Procedure

1. In the Navigation menu, select **Device Inventory**.
2. In the **Devices** page, select **Download** ( )

   A zip file containing individual CSV files for each device type is downloaded.

3. To download the inventory of selected devices, do the following:
   a. Select the check boxes for the devices you want to download.
   b. Select **Download** ( ).



- Alternatively, you can select **Download Inventory** from the Actions column ( ) for the required device.
- A zip file containing individual CSV files for each device type is downloaded.

Device Settings

About This Task

You can use the **Device Settings** option in the XCO user interface to activate maintenance mode on the SLX-OS devices.

XCO supports drift and reconcile (DRC) of a configuration at device level. A single device configuration is compared with XCO and if there is a drift in the configuration, it is reconciled.

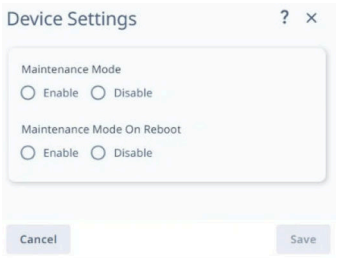
By default, XCO performs drift and reconcile actions on the SLX-OS devices that enter into maintenance mode after reboot, taking those devices out of maintenance mode after successfully reconciling the configuration on them.

Drift and reconcile operations are run in parallel across all devices in a fabric. It ensures that the multiple DRC operations that take place during fabric-wide firmware download or reboot of multiple devices together, run in parallel, and hence, reduce the overall maintenance window.

Perform this procedure to change maintenance mode settings of a device.

Procedure

1. In the Navigation menu, select **Device Inventory**.
2. In the Devices page, select **Device Settings** from the Actions column ( ) for the device you want to update.



3. Configure **Device Settings**:
   - Activate or deactivate **Maintenance Mode**
   - Activate or deactivate **Maintenance Mode on Reboot**.
4. Select **Save**.

Delete Device

Procedure

1. In the Navigation menu, select **Device Inventory**.
2. In the Devices page, select **Delete Device** from the Actions column (•••) for the device you want to delete.
3. Select **Confirm** when prompted.

Upgrade Firmware

You can download and upgrade the firmware on multiple devices.

For information about deploying XCO, see the *ExtremeCloud Orchestrator Deployment Guide, 4.0.2*.

Register Firmware Host

Procedure

1. In the Navigation menu, select **Device Inventory**.

   The **Devices** window opens.
2. Select **Settings** > **Firmware Hosts** > **Register Host**.

   The **Register Host** window opens.
3. In the **Host IP address** field, provide the IPv4 or IPv6 address of the firmware host sever.

   If a firmware host server has both IPv4 and IPv6 addresses, each IP address is treated as an independent entry.
4. In the **Protocol** field, select one or more options from the available protocols.
   - FTP
   - SFTP
   - SCP
5. In the **Username** field, provide a name.
6. In the **Password** field, provide the password.
7. Select **Register Host**.

View Registered Firmware Hosts

Procedure

1. On the Navigation menu, select **Device Inventory**.
   The **Devices** window opens.
2. Select **Settings** > **Firmware Hosts**.
   The list of registered hosts opens.

Edit a Firmware Host

Procedure

1. In the Navigation menu, select **Device Inventory** > **Settings** > **Firmware Hosts**.
   The list of registered firmware hosts opens.
2. Select **Edit** ( ) from the **Actions** column ( ) for the firmware host IP address you want to edit.
3. Complete the fields as described in Register Firmware Host on page 89.

Delete a Firmware Host

Procedure

1. In the Navigation menu, select **Device Inventory** > **Settings** > **Firmware Hosts**.
   The list of registered firmware hosts is displayed.
2. Select **Delete** ( ) from the Actions column ( ) for the host IP address you want to delete.

Upgrade Firmware (Device Level)

Before You Begin

- Register firmware host. For more information, see Register Firmware Host on page 89.
- When you upgrade to a new firmware image on SLX-OS products, the previous image is moved to the secondary location, and the previous secondary image is moved to the temporary location until the new image is committed.
- The Device Inventory page supports parallel firmware download requests for any set of devices. However, the parallel firmware download processes on the Device Inventory page might lead to traffic loss. Use caution when you select devices on the Device Inventory page for firmware download.

About This Task

For SLX-OS devices, XCO extracts the target firmware version file name from the directory name.

Example:

```
/root/slxos18s.1.03/slxos18s.1.03a
Target firmware version: 18s.1.03a
```

For MLX devices, the target firmware version file name is extracted from the manifest file name.

Example:

```
XMR-MLX/MLX06300bc_Manifest.txt
Target firmware version 6.3.00bc
```

Note

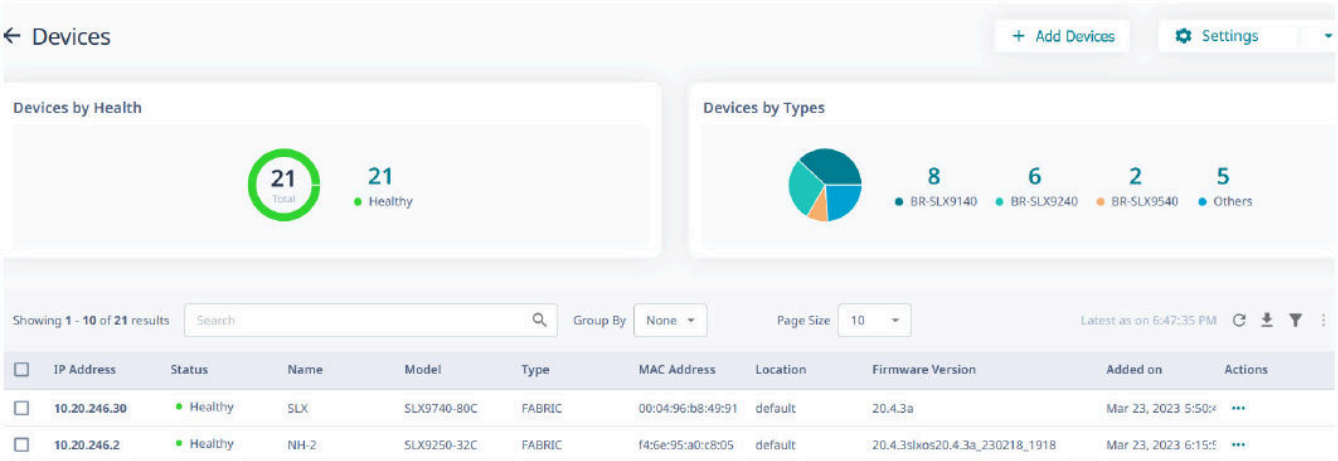
- As a best practice, do not change the target firmware version file name and the directory name.

Table 8: Supported protocol

Device Type	Protocol
SLX-OS fabric	SCP, SFTP, FTP
MLX	TFTP

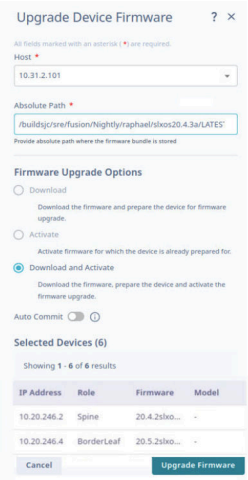
Procedure

1. In the Navigation menu, select **Device Inventory**.

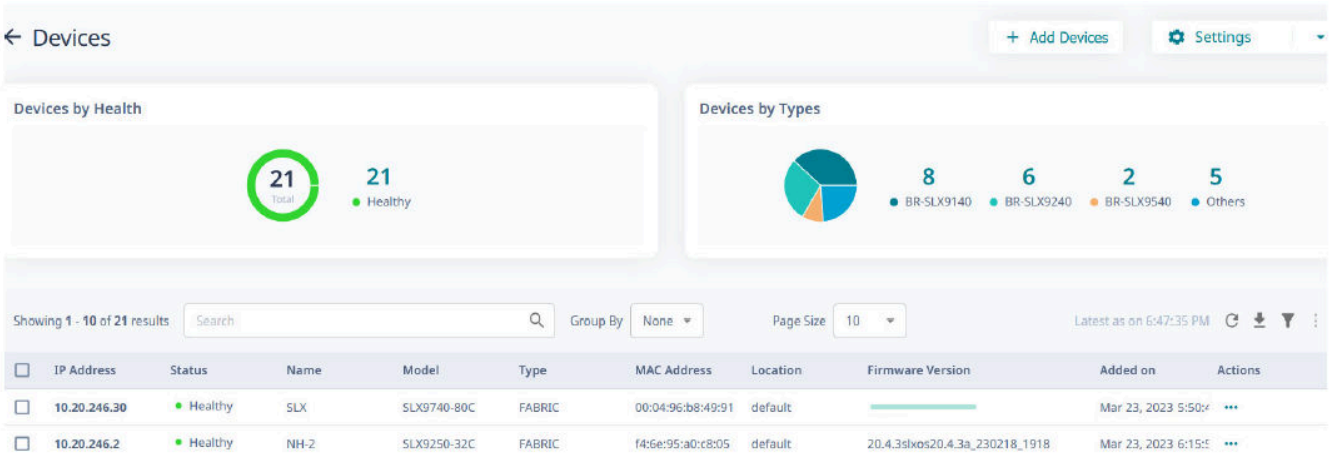


2. In the Devices page, select **Upgrade Firmware** from the Actions column (•••) for the device you want to upgrade.

   Alternatively, click anywhere in the device row except the Actions column to proceed to the Device Overview page and select **Upgrade Firmware** from the Device Actions menu.



3. In the **Host** field, provide the IPv4 or IPv6 address of the firmware host server.
4. In the **Absolute Path** field, provide the firmware file path.
5. Select **Download and Activate**.
6. Select **Upgrade Firmware**.
7. Select **Confirm** when prompted to confirm firmware upgrade of the selected devices.



To change maintenance mode settings of a device, see Device Settings on page 88.

The devices are upgraded to the downloaded firmware version. Refresh the page to view the updated list.

Related Links

Register Firmware Host on page 89
View Registered Firmware Hosts on page 90
Edit a Firmware Host on page 90
Delete a Firmware Host on page 90

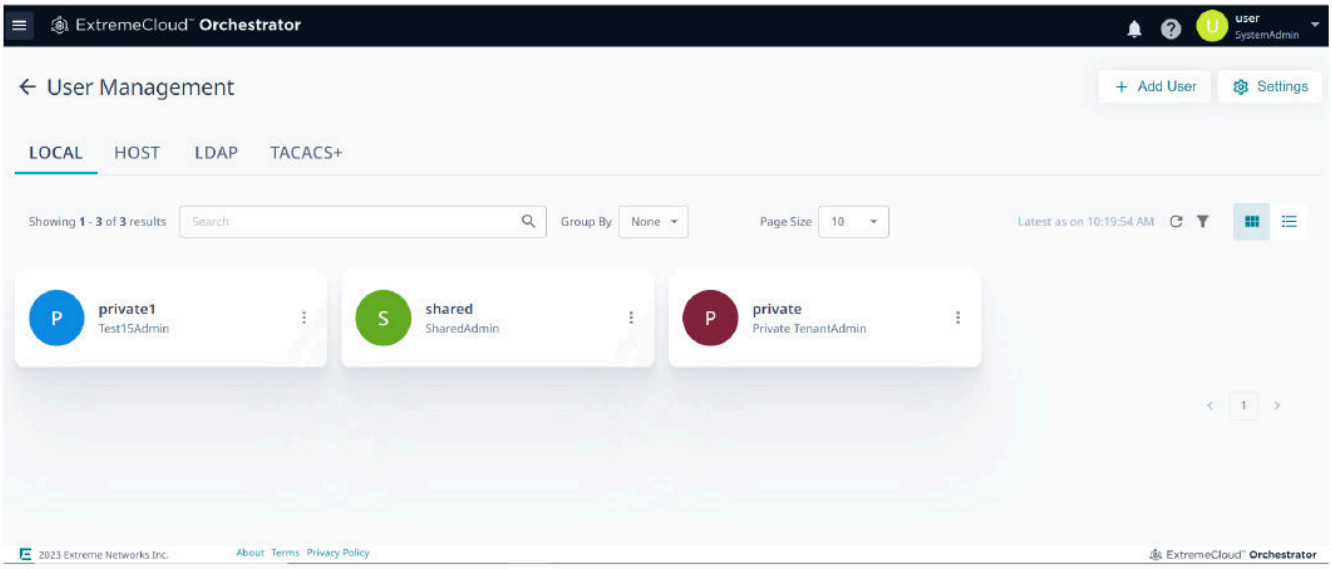
Sync Firmware Version

Procedure

1. In the Navigation menu, select **Device Inventory**.
2. In the Devices page, select **Sync** from the **Actions** column (•••) for the device you want to sync the firmware version.
3. Select **Confirm** when prompted to sync the firmware version of the selected device.

Users

The **Users** page allows you to configure the preferred authentication method for validating users.



XCO supports the following methods to manage and authenticate users:

- External LDAP server
- External TACACS+ server
- Local DB user
- Unix authentication on the host where XCO is installed

XCO supports predefined role management for LDAP and TACACS+. You can map the LDAP and TACACS+ specific roles with the predefined XCO roles.

For more information, see:

- LDAP Settings on page 101
- TACACS+ Settings on page 105

Role Based Access Control

XCO supports Role Based Access Control (RBAC). RBAC defines the capabilities that a user account has based on the assigned role. A role defines the access privileges of the user accounts.

XCO validates user privileges based on the assigned role:

- Custom roles are not supported. For information on supported roles, see User Roles on page 95.
- User-defined role management is supported for LDAP and TACACS+. For more information, see LDAP Settings on page 101 and TACACS+ Settings on page 105.

User Roles

A user is associated with one role. The user name and role of the logged-in user are displayed in the title bar.

Table 9: User role definitions

Role	Functions
SystemAdmin	Users with this role have complete privileges to perform all operations in the system. **Note:** The default host user who installs the XCO application has this role. You cannot edit or delete the host user.
NetworkOperator	Local users with this role have read-only privileges to all operations in the system. These users can change their own account password.
Fabric Mode Only:	
FabricAdmin	Users with this role have privileges to perform fabric management, device management, and location management operations.
TenantAdmin	Users with this role have read-only privileges to all operations in the system.
SecurityAdmin	Users with this role have privileges to perform user management operations.
SystemDebugger	Users with this role have privileges to perform system debug operations.

Authentication Tokens

Authentication tokens that are generated when a user logs in to XCO are stored in memory and validated for token authentication and authorization.

The token is cleared under the following conditions:

- User role modification
- User deletion
- User blocking
- User logout
- Session expiration
- Token expiration

If a user token is cleared during an active user session, the user is prompted to log in again.

Local

You can use the **Local** page to create and manage local users.

Add User

Only a user with the SystemAdmin role can add a local user.

About This Task

When the first local user is added, XCO automatically adds the **LOCAL Auth** type to the authentication preference settings in the following situations:

- **LOCAL auth** preference does not exist
- Authentication preference settings limit of five entries is not exceeded

Procedure

1. In the Navigation menu, select **Users**.
2. Select **+ Add User**.
3. In the **User Name** field, enter the user's user name.
4. In the **User Role** field, select the required user roles.
   - **NetworkOperator**
   - **SystemAdmin**
   - Fabric mode only:
     - **FabricAdmin**
     - **SecurityAdmin**
     - **SystemDebugger**
     - **TenantAdmin** (created dynamically per tenant)

XCO supports multiple role mapping for all users. For more information, see User Roles on page 95.

5. In the **New Password** and **Confirm New Password** fields, enter the new password for the user.
6. In the **Email-id** field, enter the user's email address.

   Special characters specified by RFC-5322 are supported in the email field.
7. (Optional) Complete the other fields as required.
8. Select **Add**.

   The new user is added to the **LOCAL** users page. Refresh the page to view the updated list.

Related Links

Edit User on page 97
Block User on page 97
Unblock User on page 98
Request Reset Password on page 98
Change Password on First Login on page 98
Delete User on page 99

Edit User

Before You Begin

Only a user with the role of SystemAdmin can change the role of another local user.

About This Task

To change the role of an LDAP or TACACS+ user, change the role on the remote server using the appropriate method.

Procedure

1. In the Navigation menu, select **Users** > **LOCAL**.
2. Select for the relevant user.
3. Select **Edit User**.
4. In the **User Type** field, select **NetworkOperator** or **SystemAdmin**.

   For more information, see User Roles on page 95.
5. Save your changes.

Block User

Before You Begin

Only a user with the SystemAdmin role can block or unblock a local user.

Procedure

1. In the Navigation menu, select **Users**.
2. Select the **Local** tab.

3. Select for the relevant user.
4. Select **Block User** to block the user.

Unblock User

Before You Begin

Only a user with the SystemAdmin role can block or unblock a local user.

Procedure

1. In the Navigation menu, select **Users**.
2. Select the **Local** tab.
3. Select for the blocked user.
4. Select **Unblock User** to unblock the user.

Request Reset Password

Before You Begin

- Only a user with the SystemAdmin role can reset the password of local users.
- Automated mail service for sharing the user password is not available.
- Password complexity check is not available.
- Local user passwords do not expire.

Procedure

1. In the Navigation menu, select **Users**.
2. Select for the relevant user.
3. Select **Reset Password**.

   The **Password Reset** window opens.
4. Enter the new password for the user.
5. Confirm the password.
6. Select **Save**.

   The user is prompted to change the password on first login after password reset.

Change Password on First Login

About This Task

You are prompted to change the password on first login.

Procedure

1. In the **New Password** field, enter the password.
2. In the **Confirm Password** field, enter the password again.
3. Select **Change Password**.

   The password is changed and you are logged out of the user interface.

What to Do Next

Log in to the user interface using the new password.

Delete User

About This Task

Only a user with the role of SystemAdmin can delete a local user.

Procedure

1. In the Navigation menu, select **Users** > **LOCAL**.
2. Select for the relevant user.
3. Select **Delete User**.

Host

When XCO is deployed, the user who installs the application is configured as SystemAdmin with complete access and permissions.

Host user authentication is configured as the default authentication method.

Change Host User Role

The default host user who installs ExtremeCloud Orchestrator is automatically added to the host users role mapping page. You cannot edit or delete the default host user.

Procedure

1. In the Navigation menu, select **Users**.
2. Select **+ Add Host**.
3. From the **User Name** drop-down menu, select the required host user.
4. In the **User Type** drop-down menu, select the required user type:
   - **NetworkOperator**
   - **SystemAdmin**
   - Fabric mode only:
     - **FabricAdmin**
     - **SecurityAdmin**
     - **SystemDebugger**
     - **TenantAdmin** (created dynamically per tenant)
5. Select **Save**.

User Settings

The **User Settings** page in the XCO user interface allows you to configure the LDAP and TACACS+ authentication settings and change the authentication level priority for the available authentication methods.

In the Navigation menu, select **Users** > **Settings** to access the **User Settings** page. You can access **User Settings** from all pages on User Management.

For more information, see Authentication Settings on page 100.

Authentication Settings

You can change the user authentication level priority among TACACS+, LDAP, Local, and HOST servers.

About This Task

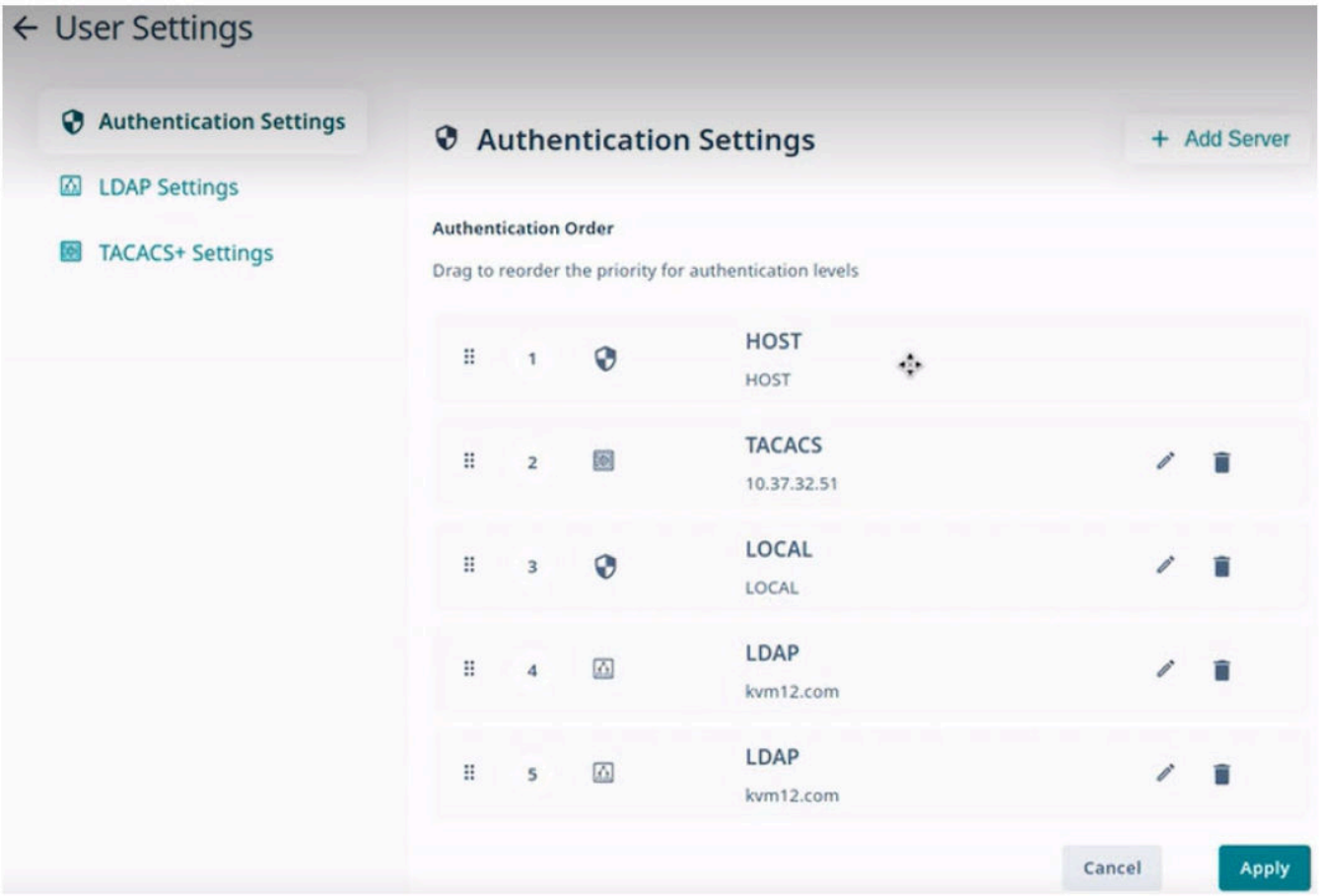
XCO supports a maximum of five authentication settings. Host is the default authentication setting.

If a configured authentication level priority server is unreachable, failover to the next server occurs. If all servers decline to authenticate the user, the other configured authentication methods are attempted in the authentication order, and eventually the user is denied.

Procedure

1. In the Navigation menu, select **Users** > **Settings**.

2. In the **Authentication Settings** page, drag and drop the required server settings to reorder the authentication level priority.



3. Select **Apply** to save the changes.
4. To add a server to the existing authentication settings, select **Add Server**.
5. Select an authentication level and then select **Apply**.

LDAP Settings

XCO supports Lightweight Directory Access Protocol (LDAP). The **Settings** page in the user interface allows viewing and managing of LDAP server configurations.

LDAP is an open-source protocol used for centralized authentication through directory service. If the configured LDAP servers decline to authorize the user, the other authentication methods are attempted in the order they are configured.

Active Directory (AD) is a directory service that supports a number of standardized protocols such as LDAP, Kerberos authentication, and Domain Name Server (DNS), to provide various network services. AD uses a structured data store as the basis for a logical, hierarchical organization of directory information. AD includes user profiles and groups as part of directory information, so it can be used as a centralized database for authenticating third-party resources.

XCO supports the following LDAP methods to authenticate users:

- The user role is included directly as an attribute in the user definition entry.
- The user has the `memberOf` entry or any appropriate group definition attribute to identify the groups assigned.
- The user entries are present in the LDAP group definition.
- If the user entry is not present or not mapped to the correct predefined role in XCO, the user login fails. For more information, see Map an LDAP User Role on page 104.

Note
If LDAP group definition methods are used for user authentication, the corresponding LDAP group must be mapped to an user role in XCO.

- XCO supports up to five auth preferences and LDAP servers can be added accordingly. If any LDAP server addition fails due to auth preference limit, delete the unnecessary auth preference and add a new LDAP config.
- The LDAP configuration name must be unique for configuring the authentication policy.

Add LDAP Server

You can add LDAP connection details so that LDAP users can sign in to the XCO user interface.

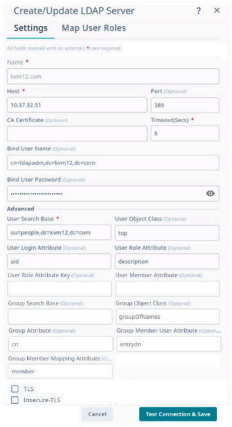
About This Task

When a new LDAP server is added, XCO automatically adds it to the authentication preference settings if the authentication preference limit of five entries is not exceeded.

Procedure

1. In the Navigation menu, select **Users**.
2. Select **Settings** > **LDAP Settings** > **Add LDAP Server**.

   Alternatively, you can select **LDAP** > **Connect LDAP** to configure the first LDAP server.



3. In the **Name** field, enter a name for the LDAP server.

   The name can contain up to 32 alphanumeric characters without spaces.

4. (Optional) If multiple LDAP servers are available, proceed to the next step. Else, go to step 6.
5. In the **Host** field, enter the host name, IPv4, or IPv6 address of the LDAP server.
6. (Optional) In the **Port** field, enter the TCP port used for authentication.
7. (Optional) In the **CA Certificate** field, enter the CA certificate location.

   Select the CA certificate to use when validating the server certificate that the LDAP server sends. The CA certificate must be issued by the same CA that issued and signed the server certificate for the LDAP server.
8. In the **Timeout(Secs)** field, enter the timeout value in seconds.

   The default timeout value is 5 seconds.
9. (Optional) In the **Bind User Name** field, enter the LDAP server user name.

   The Bind User Name is used for authenticating the LDAP server when initiating a connection.
10. (Optional) In the **Bind User Password** field, enter the password for the LDAP server.

    The Bind User Password is used for authenticating the LDAP server when initiating a connection.
11. In the Advanced section, complete the following fields as required:
    - **User Search Base**: Specifies the name of the node from which to start searching for users.
    - (Optional) **User Object Class**: Specifies the name of the user object class. The default value is `inetOrgPerson`.
    - (Optional) **User Login Attribute**: Specifies the login username attribute. The default value is `uid`.
    - (Optional) **User Role Attribute**: Specifies the user role attribute.
    - (Optional) **User Role Attribute Key**: Specifies key to the user role attribute.
    - (Optional) **User Member Attribute**: Specifies the member attribute of the user.
    - (Optional) **Group Search Base**: Specifies the name of the node from which to start searching for groups.
    - (Optional) **Group Object Class**: Specifies the name of the group object class. The default value is `groupOfNames`.
    - (Optional) **Group Attribute**: Specifies the group attribute. The default value is `cn`.
    - (Optional) **Group Member User Attribute**: Specifies the group member user attribute. The default value is `entrydn`.
    - (Optional) **Group Member Mapping Attribute**: Specifies the group member mapping attribute. The default value is `member`.
    - (Optional) **TLS check box**: Enables LDAP over SSL/TLS
    - (Optional) **Insecure-TLS check box**: Enables LDAP without certificate verification
12. Select **Test Connection and Save** to save your selections.

    The **Authentication Settings** page displays the new configuration.

What to Do Next

Map an LDAP User Role on page 104

Map an LDAP User Role

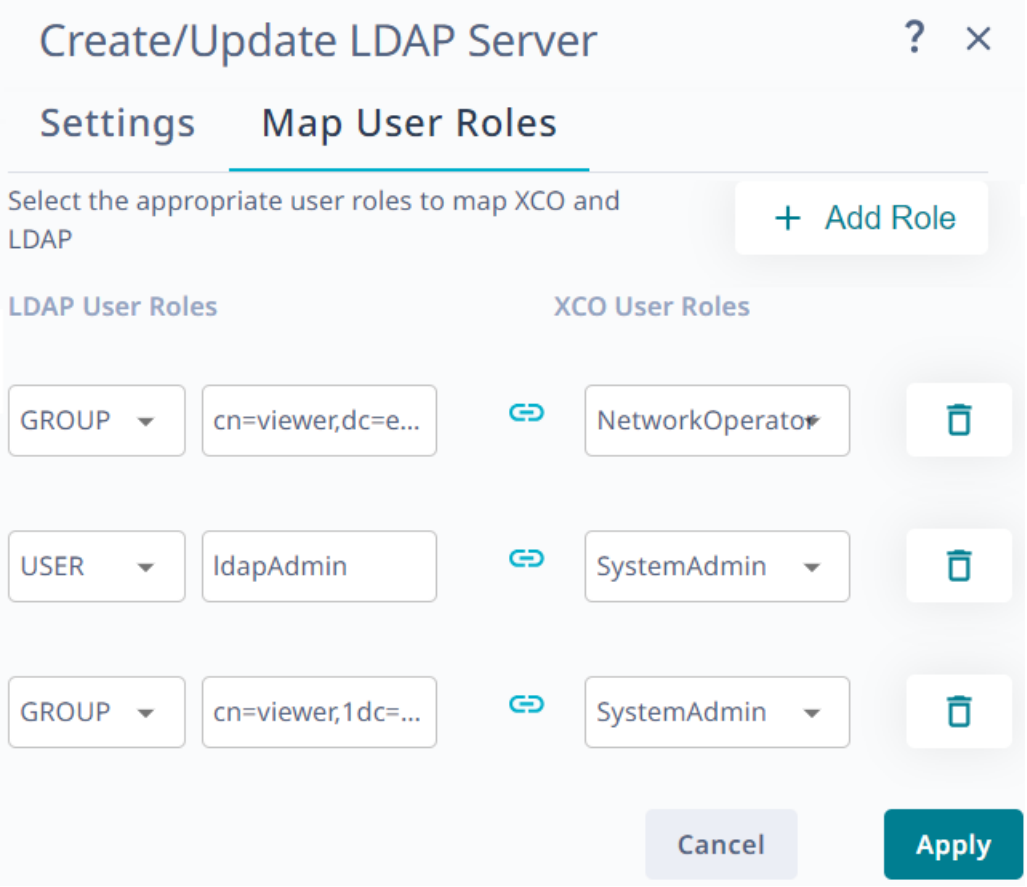
You can map a local LDAP role to one of the pre-defined XCO roles.

About This Task

The LDAP server `name` is used as `auth-identifier` for mapping a LDAP user role.

Procedure

1. In the Navigation menu, select **Users**.
2. Select **Settings** > **LDAP Settings**.
3. Select an LDAP server.
4. Select **Map User Roles**.



5. Select the required **LDAP User Roles**.
   - **GROUP**
   - **USER**
6. Select the required **XCO User Roles** to map the local LDAP role.
7. Select **Apply**.

   The LDAP server page displays the new mapping.

TACACS+ Settings

Terminal Access Controller Access-Control System Plus (TACACS+) is an external authentication server used for verifying user credentials.

The TACACS+ protocols support environments that are configured for authentication, authorization, and accounting (AAA) services. When TACACS+ is configured through the XCO interface, TACACS+ users can log in to the XCO interface.

XCO supports TACACS+ authentication in the following ways.

- XCO supports up to five auth preferences and TACACS+ servers can be added accordingly. If any TACACS+ server addition fails due to auth preference limit, delete the unnecessary auth preference and add a new TACACS+ config.
- The user roles specified in the TACASCS+ server configuration can be one of the following.
  - One of the supported XCO roles: NetworkOperator and SystemAdmin. For more information, see User Roles on page 95.
  - A local TACACS+ role that you can map to XCO. For more information, see Map a TACACS+ User Role on page 106.
  - The `xco-role` attribute must be included in the TACACS+ configuration file.
  - If the `xco-role` attribute is not present or not mapped to the correct predefined role in ExtremeCloud Orchestrator, the user login fails.
- TACACS+ authentication must be enabled. If TACACS+ authentication is not enabled, only local authentication is used.
- If remote authentication fails, XCO attempts to use local authentication, which is successful only if the user is in the XCO database.
- The secret key configured for XCO must be the same as the secret key from the TACACS+ server configuration file. Authentication fails if the two values do not match.
- XCO supports two TACACS+ authentication protocols.
  - **CHAP**: Challenge Handshake Authentication Protocol
  - **PAP**: Password Authentication Protocol

Add TACACS+ Server

You can add TACACS+ connection details so that TACACS+ users can sign in to the XCO interface.

About This Task

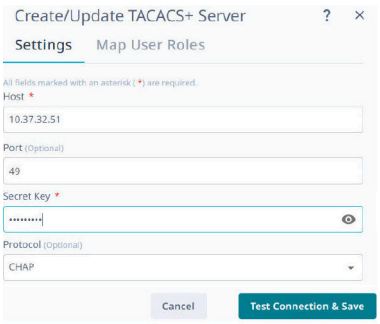
When a new TACACS+ server is added, XCO automatically adds it to the authentication preference settings if the authentication preference limit of five entries is not exceeded.

Procedure

1. In the Navigation menu, select **Users**.

2. Select **Settings** > **TACACS+ Settings** > **Add TACACS+ Server**.

   Alternatively, you can select **TACACS+** > **Connect TACACS+** to configure the first TACACS+ server.



3. In the **Host** field, enter the IPv4 or IPv6 address of the TACACS+ server, in CIDR format.
4. In the **Port** field, enter the TCP port used for authentication.

   The default authentication port is 49.
5. In the **Secret Key** field, enter the shared secret that enables messages between the client and the TACACS+ server.

   The value you enter must match the shared secret in the TACACS+ server configuration file.
6. In the **Protocol** field, select one of the following authentication protocols.
   - **CHAP**: Challenge Handshake Authentication Protocol
   - **PAP**: Password Authentication Protocol
7. Select **Test Connection and Save** to save your selections.

   The Settings page displays the new configuration.

What to Do Next

Map a TACACS+ User Role on page 106

Map a TACACS+ User Role

You can map a local TACACS+ role to one of the pre-defined XCO roles.

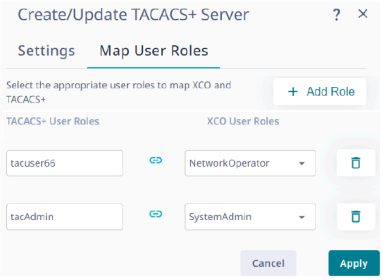
About This Task

The TACACS+ server `host` is used as `auth-identifier` for mapping a TACACS+ user role.

Procedure

1. In the Navigation menu, select **Users**.
2. Select **Settings** > **TACACS+ Settings**.
3. Select a TACACS+ server.

4. Select **Map User Roles**.



5. Select the required **TACACS+ User Roles**.
6. Select the required **XCO User Roles** to map the local TACACS+ role.
7. Select **Apply**.

   The TACACS+ server page displays the new mapping.

Change a Server Configuration

You can change the configuration of a LDAP or TACACS+ server for accessing the XCO interface.

Procedure

1. In the Navigation menu, select **Users**.
2. Select **Settings** > **LDAP Settings** or **Settings** > **TACACS+ Settings** as required.

   Alternatively, you can select **LDAP** or **TACACS+** tab.
3. Select **Edit** for the server configuration that you want to change.
4. Update the server configuration as required.
5. Save your selections.
6. Select **Apply**.

   The Authentication Settings page displays the changed configuration.

Delete a Server Configuration

You can delete the configured LDAP and TACACS+ host servers.

Procedure

1. In the Navigation menu, select **Users**.
2. Select the **TACACS+** or **LDAP** tab.
3. Select **Delete** for the server configuration that you want to delete.

   Alternatively, you can delete the LDAP and TACACS+ server configurations from **Users** > **Settings** > **Authentication Settings**

Change Password

Logged-in users can change their own passwords.

Procedure

1. From the User Profile menu, select **Change Password**.
2. Update the password.

Logout

Procedure

From the User Profile menu, select **Logout**.

Logs

The XCO user interface enables viewing of System logs and User logs. The System logs persist for two hours, and User logs persist for a week.

Exporting System logs and User logs is not supported in XCO.

System Logs

System logs describe the status of monitored devices.

About This Task

System logs are based on RASLog notifications. The system logs are stored for a duration of two hours.

Procedure

1. In the Navigation menu, select **Logs** > **System**.

   The system logs provide the following information:

   - Hostname
   - IP address
   - Severity
   - Message
   - Date

2. Use the **Search** bar to look up a system log.

3. Use the refresh icon to reload the system logs.
4. Use the filter option to view the system logs by **Severity** or **Message**.
   a. In the **System Logs** widget, select .
   b. Select a system log value between **Severity** or **Message**, and then enter the filter value.
   c. Select **Add Filter** to include more filter options, or **Apply Filter** to view the system logs based on your previous selection.

User Logs

You can view user logs to understand the transactions that a user has performed.

About This Task

XCO offers several types of logs related to user transactions: Device, Device Config, and User Login. These logs provide the following information.

Procedure

1. In the Navigation menu, select **Logs** > **User**.
2. To view user transactions on devices, select **Device**.

   The device logs provide the following information:

Table 10: User device logs

Log Type	Description
Device	Device add or delete transactions: • User name • Action, such as delete or discover a device • IP address • Location • Status, such as success or failed • Error message to explain a failure • Date

3. To view user transactions related to configuration, select **Device Config**.
   The device config logs provide the following information:

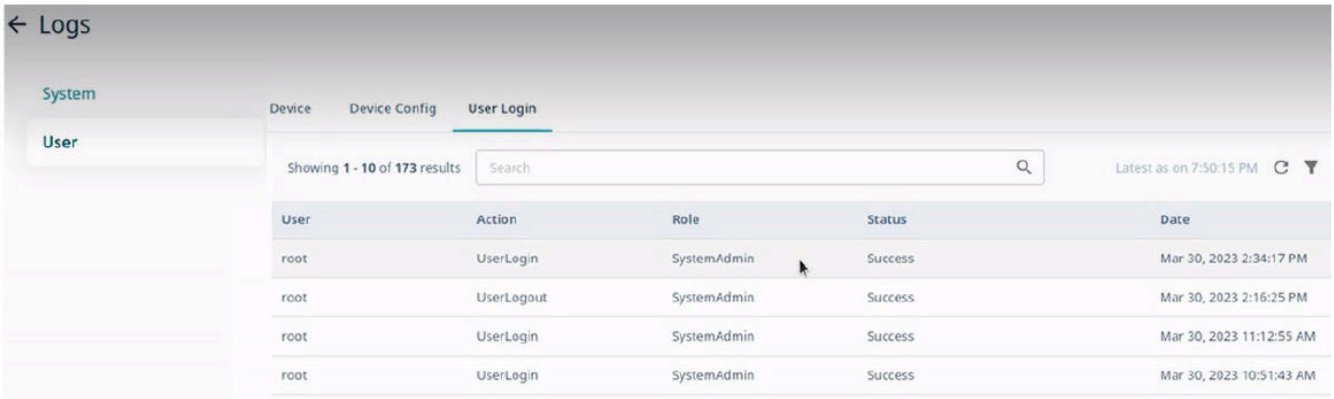
Table 11: User device config logs

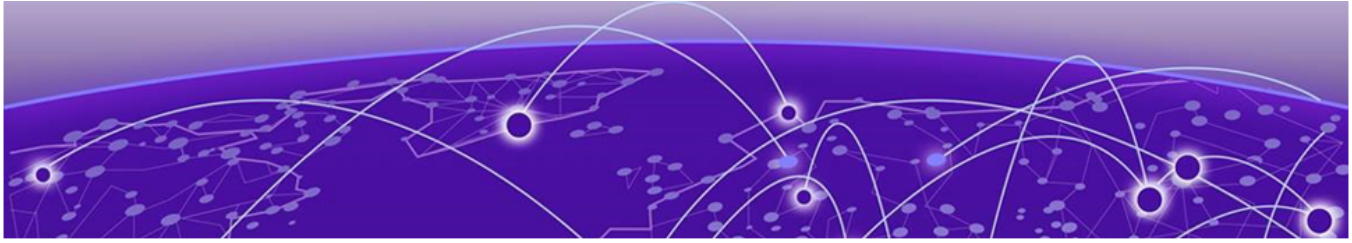
Log Type	Description
Device Config	Device configuration transactions: • User name • Action, such as add, update, clearing counters, packet capture, or delete a configuration • IP address • Location • Status, such as success or failed • Error message to explain a failure • Date

4. To view user transactions related to logging in, select **User Login**.
   The user login logs provide the following information:

Table 12: User login logs

Log Type	Description
User Login	User login and logout transactions: • User name • Action, such as log in or log out • User role • Log in time • Whether the action was successful





FAQs

Where are the Inventory Service logs located?

Debug logs: `/var/log/efa/inventory/inventory-server.log`

Error logs (with panic trace): `/var/log/efa/inventory/inventory-server_err.log`

Where are the Installer logs located?

`/var/log/efa/installer/<installer_.....log>`

All installation failures are reported in this log.

What are some common reasons for installation failures?

- The operating system version is incorrect.
- The amount of available hard disk space is insufficient. At least 50 GB should be available.
- In a multi-node installation, the operating system and clock do not match. Or, both nodes have the same host name.

Why does the web user interface not load on the browser?

The most probable reason is that TCP port 443 is blocked through a firewall. Unblocking this port should enable the UI to be loaded.

What are some common reasons for XCO log-in failures?

- The user credentials are entered incorrectly.
- TACACS+ or LDAP is not reachable or not configured correctly for the `xco-role`.
- The `xco-role` in TACACS+ or LDAP is not mapped to a predefined role such as NetworkOperator or SystemAdmin.

Where are authentication failures captured?

Debug logs: `/var/log/efa/auth/auth-server.log`

Error logs (with panic trace): `/var/log/efa/auth/auth-server_err.log`

What are possible reasons for device registration failures?

- The device is not reachable from ExtremeCloud Orchestrator.
- The device credentials are incorrect.
- The HTTPS, SSH, NETCONF, or GNMI ports are blocked.
- The device versions are not supported.
- The device has exceeded the maximum limit on SSH connections. Free up some existing connections that are used by other tools and try to register again.

Why is there a delay in loading the dashboard or statistics in the web UI?

It can take from 20 seconds to 1 minute to load live statistics from a device.

Why is the device configuration blocked from the web UI?

The device can have missed a heartbeat and subsequently transitioned to a degraded state. The device should be accessible when connectivity is restored.

What are possible reasons for configuration failures?

- The XCO user does not have permission to make changes to the device.
- The web UI reports validation errors or errors received from the device.
- The credentials used for device registration do not have permission to make changes to the device.

How do I check that all services are up and running?

Run the following command on the XCO device:

```
k3s kubectl get pods -n efa
```

The following is sample output.

```
NAME                              READY   STATUS    RESTARTS   AGE
efa-api-docs-84cwl                1/1     Running   0          20d
ui-service-54dbbb47fd-vzfrw       1/1     Running   0          20d
gosystem-service-dw4vj            1/1     Running   0          20d
rabbitmq-4tgsv                    1/1     Running   0          20d
gorbac-service-j6lp8              1/1     Running   0          20d
goevm-service-sjckq               1/1     Running   0          20d
gonotification-service-grvx9      1/1     Running   0          20d
gofaultmanager-service-nstwf      1/1     Running   0          20d
goauth-service-qffvs              1/1     Running   0          20d
goraslog-service-s7mwt            1/1     Running   0          20d
goinventory-service-q5sdl         1/1     Running   0          20d
```

Why are the device syslogs not visible?

Other tools that are registered with the device could have exceeded the maximum limit for syslogs. Free up any stale syslog entries on the device and then re-register the device.

How to collect the SupportSave data for troubleshooting?

Run the following command on the XCO device:

```
efa system supportsave
```

The following is a sample output.

```
SupportSave File Location: /var/log/efa/efa_2022-11-17T18-40-41.008.logs.zip
--- Time Elaspsed: 21.584259642s ---
```

To collect the SupportSave data using the XCO GUI, see Support Save on page 24.