nGenius® PFS Fabric Manager Software 6.5.1 Administrator Guide

733-1957 Rev. B

NETSCOUT SYSTEMS, INC.
Westford, MA 01886
Telephone: 978.614.4000
Fax: 978.614.4004

Web: http://www.netscout.com

Use of this product is subject to the End User License Agreement available at http://www.NetScout.com/legal/terms-and-conditions or which accompanies the product at the time of shipment or, if applicable, the legal agreement executed by and between NETSCOUT Systems, Inc. or one of its wholly-owned subsidiaries ("NETSCOUT") and the purchaser of this product ("Agreement").

Government Use and Notice of Restricted Rights: In U.S. government ("Government") contracts or subcontracts, Customer will provide that the Products and Documentation, including any technical data (collectively "Materials"), sold or delivered pursuant to this Agreement for Government use are commercial as defined in Federal Acquisition Regulation ("FAR") 2.101 and any supplement and further are provided with RESTRICTED RIGHTS. All Materials were fully developed at private expense. Use, duplication, release, modification, transfer, or disclosure ("Use") of the Materials is restricted by the terms of this Agreement and further restricted in accordance with FAR 52.227-14 for civilian Government agency purposes and 252.227-7015 of the Defense Federal Acquisition Regulations Supplement ("DFARS") for military Government agency purposes, or the similar acquisition regulations of other applicable Government organizations, as applicable and amended. The Use of Materials is restricted by the terms of this Agreement, and, in accordance with DFARS Section 227.7202 and FAR Section 12.212, is further restricted in accordance with the terms of NETSCOUT'S commercial End User License Agreement. All other Use is prohibited, except as described herein.

This Product may contain third-party technology. NETSCOUT may license such third-party technology and documentation ("Third- Party Materials") for use with the Product only. In the event the Product contains Third-Party Materials, or in the event you have the option to use the Product in conjunction with Third-Party Materials (as identified by NETSCOUT in the Documentation provided with this Product), then such Third-Party Materials are provided or accessible subject to the applicable third-party terms and conditions contained in the "Read Me" or "About" file located in the Software, on an Application CD provided with this Product, in an appendix located in the documentation provided with this Product, or in a standalone document where you access other on-line Product documentation. To the extent the Product includes Third-Party Materials licensed to NETSCOUT by third parties, those third parties are third-party beneficiaries of, and may enforce, the applicable provisions of such third-party terms and conditions.

Open-Source Software Acknowledgment: This product may incorporate open source components that are governed by the GNU General Public License ("GPL") or licenses similar to the GPL license ("GPL Compatible License"). In accordance with the terms of the GPL Compatible Licenses, NETSCOUT will make available a complete, machine-readable copy of the source code components covered by the GPL Compatible License, if any, upon receipt of a written request. Please identify the NETSCOUT product and open source component, and send a request to:

NETSCOUT SYST, INC
Open Source Code Request
310 Littleton Road
Westford, MA 01886
Attn: Legal Department

To the extent applicable, the following information is provided for FCC compliance of Class A devices:

> *This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.*
>
> *Modifications to this product not authorized by NETSCOUT could void the FCC approval and terminate your authority to operate the product. Please also see NETSCOUT's Compliance and Safety Warnings for NetScout Hardware Products document, which can be found in the documents accompanying the equipment, or in the event such document is not included with the product, please see the compliance and safety warning section of the user guides and installation manuals.*

Contacting NETSCOUT SYST, INC.

Customer Care

The best way to contact Customer Care is to submit a Support Request:
https://my.netscout.com/mcp/Support/Pages/Home.aspx

Telephone: US Toll Free: **+1-888-357-7667**; International Toll Free: **+800 4764 3337**.
Phone support hours are 8 a.m. to 8 p.m. Eastern Standard Time (EST).

When you contact Customer Care, the following information can be helpful in diagnosing and solving problems:
— Your organization's name, contact name, phone number, and location of system
— NETSCOUT Packet Flow Switch model number
— PFS Fabric Manager Software version
— Detailed description of the problem, or source of the problem based on its symptoms
— Error text messages, supporting screen images, logs, and error files, as appropriate

Sales

Call **800-357-7666** for the sales office nearest your location.

Table of Contents

Chapter 1 About This Document and Introduction

Chapter 2 Login and Setup PFS Fabric Manager

Chapter 3 Configure Lifecycle

Chapter 4 Deploy Lifecycle

Chapter 5 Inline Lifecycle

Chapter 6 Monitor Lifecycle

Chapter 7 System Settings

Appendix A Installing PFS Fabric Manager Central Server (Software-Only Version)

Appendix B Configuring and Troubleshooting the Server Remotely

Appendix C Switch RMA Replacement

NETSCOUT

Revision History

Date	Revision	Description
June 2024	PFS FM 6.5.1 Rev B	• Added the new section Topology Notes. • Updated SNMP to include SNMP Traps and UI improvements.
April 2024	PFS FM 6.5.0 Rev A	• NMS and PFS Networking Requirements moved from PFS Fabric Manager Release Notes to this document. • Updated System Settings to include references to the new SNMP and Power Usage features. • Updated Alarms and Severities to include the alarms for the new Watermark feature. • Updated Profile > Default > Features to include the new Slicing feature. • Added the new section Mirror Session Profile in Perspective > Profile. • Updated Topology Node Statistics section. • Added the new section Mirroring on Deploy Lifecycle. • Updated Dashboard to include reference to the new Power Consumption feature. • Updated System in System Administration to include references to the new Upper/Lower Watermark limits. • Added the new section SNMP in System Administration. • Added the new section Power Usage in System Administration. • Updated Appendix A, “Installing PFS Fabric Manager Central Server (Software-Only Version)” to include the section Upgrading the Operating System on the PFS Fabric Manager NMS (CentOS 6/8 to Oracle Linux 9). • Updated Appendix B, “Configuring and Troubleshooting the Server Remotely” to reference the new R760 appliance and remove references to using a DVD drive.

Chapter 1
About This Document and Introduction

This document is intended to assist with the operation of NETSCOUT SYSTEMS, INC. (NETSCOUT®) nGenius® Packet Flow Switch (PFS) Fabric Manager Software used to manage NETSCOUT's PFS 5000, 6000 and 7000 series systems.

IMPORTANT

Please read and understand the *nGenius® PFS Fabric Manager Software 6.5.0 Administrator Guide* (this document) before operating the equipment. Failure to do so may result in incorrect usage.

Related Documentation

For information related to this publication, refer to the following:

- nGenius® PFS 5000/7000 Series Packet Flow Switch Quick Connection Guide
  This guide provides overview information for installing, cabling, and starting the nGenius 5000/7000 series systems.
- nGenius® PFS 6000 Series Packet Flow Switch Hardware Installation Guide
  This document provides information on the nGenius 6000 Series PFS system installation and hardware maintenance.
- nGenius® PFS Fabric Manager Server Hardware Installation Guide
  This guide provides information for installing, cabling, and starting the nGenius PFS Fabric Manager server.
- Packet Flow Operating Software (PFOS) User Guide
  Describes the system software and graphical user interface of the Packet Flow Operating Software (PFOS).

Contacting NETSCOUT Customer Care

Customer Care:
The best way to contact Customer Care is to submit a Support Request:
https://my.netscout.com/mcp/Support/Pages/Home.aspx

Telephone: In the US, call **888-357-7667**; outside the US, call **+8004764 3337**.
Phone support hours are 8 a.m. to 8 p.m. Eastern Standard Time (EST).

When contacting Customer Care, the following information can be helpful in diagnosing and solving problems:
— Your organization's name, contact name, phone number, and location of system
— NETSCOUT Packet Flow Switch model number
— PFS Fabric Manager Software version
— Detailed description of the problem, or source of the problem based on its symptoms
— Error text messages, supporting screen images, logs, and error files, as appropriate

NETSCOUT Web Site

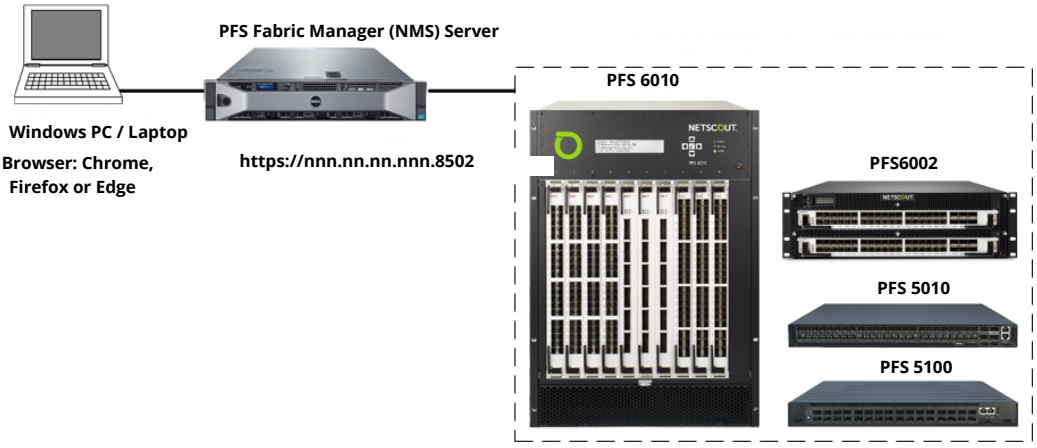
Visit our Web site at http://www.netscout.com.

PFS Fabric Manager Overview

PFS Fabric Manager is an HTML5-based application providing connectivity management of nGenius PFS 5000, 6000 and 7000 series switches with associated line cards, running PFOS software, from virtually any location. A user with an approved user name and password can access their PFS 5000, 6000 and 7000 series switches using a PC with an Internet browser (e.g., Chrome, Firefox or Edge).

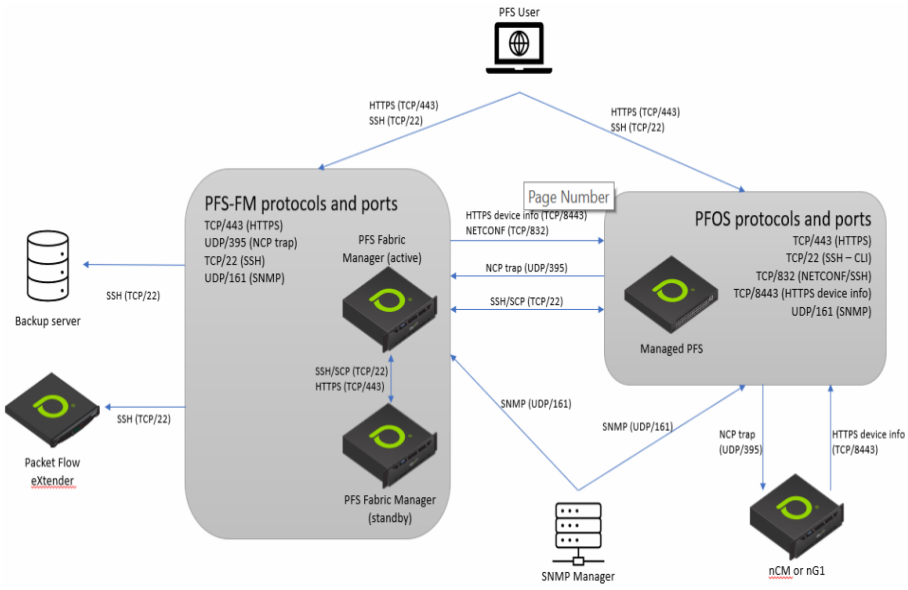
PFS Fabric Manager runs on a central server (or VM) connected to the networked PFS switches running PFOS. The PFS Fabric Manager central server is also called the NMS.

Important: NETSCOUT products are designed and tested on dedicated servers. Third-party network management software, database agents, port scanners, and security software installed on the same server may lead to port conflicts and compromise the behavior and performance of the NETSCOUT products.



NMS and PFS Networking Requirements

The arrows are from client (traffic initiator) to server; all traffic is bidirectional.



Note: Multiple optional remote servers are not shown.

NMS Ports

The following ports need to be open/accessible on the NMS:

Description	Protocol and Port	Notes
SSH	TCP/22	SSH/SCP access from the PFS to the NMS. Synchronization between active and standby NMS (when High Availability is enabled). Copying backups from the NMS to remote backup destination(s) (when remote backup destinations are enabled).
NCP trap	UDP/395	Port on which the NMS receives management requests (traps) from the PFS; the NMS will acknowledge the trap.
HTTPS	TCP/443	Fabric Manager Web UI.
SNMP	UDP/161	

Managed PFS Ports

The following ports need to be open/accessible on the PFS:

Description	Protocol and Port	Notes
NETCONF/SSH	TCP/832	Port which the NMS uses to manage the PFS.
HTTPS device info	TCP/8443	Port on which the NMS or nCM retrieve PFS device configuration.
SSH-CLI	TCP/22	Port via which the NMS transfers files to/from the PFS and PFOS CLI access.
HTTPS	TCP/443	Fabric Manager Web UI.
SNMP	UDP/161	

Chapter 2
Login and Setup PFS Fabric Manager

This section covers startup, login, and initial user setup of PFS Fabric Manager.

Important: PFS Fabric Manager is supported on a PC using Google Chrome, Firefox or Edge.

Starting / Login to PFS Fabric Manager

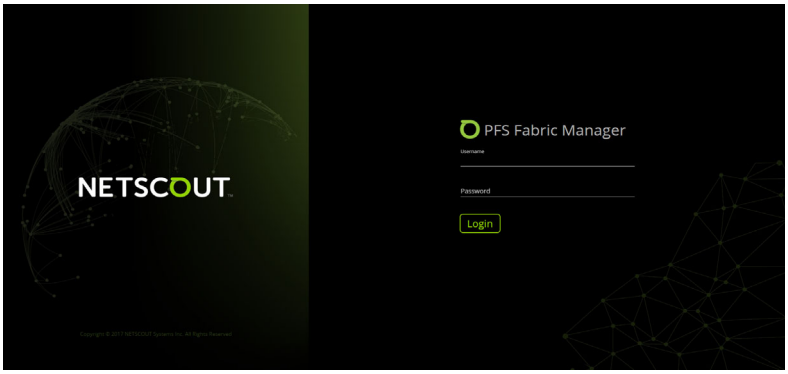
PFS Fabric Manager can be started / logged in from the PFS Fabric Manager (NMS) server.

PFS Fabric Manager (NMS) Server

1. Connect a CAT 3 (or higher) Ethernet cable between one of the network ports on the server and the PC / Laptop. We recommend that the cable length not exceed 10 feet (3 meters). If longer cable lengths are needed, use CAT 5 (or higher) shielded cable.
2. Power on the server.
3. Connect to PFS Fabric Manager by entering the IP address of the server in the web browser's URL address box. From an Internet browser, enter the assigned IP address of the nGenius PFS Fabric Manager Server (e.g., *https://nnn.nn.nn.nnn*).
4. Proceed to login (Login to PFS Fabric Manager on page 2-1).

Login to PFS Fabric Manager

1. Type in the assigned username in the **Username:** text field. The username is not case sensitive.
2. Type in the assigned password in the **Password:** text field. The password **is case sensitive**.



Note: The default Username and Password supplied by NETSCOUT is:
admin / **admin**

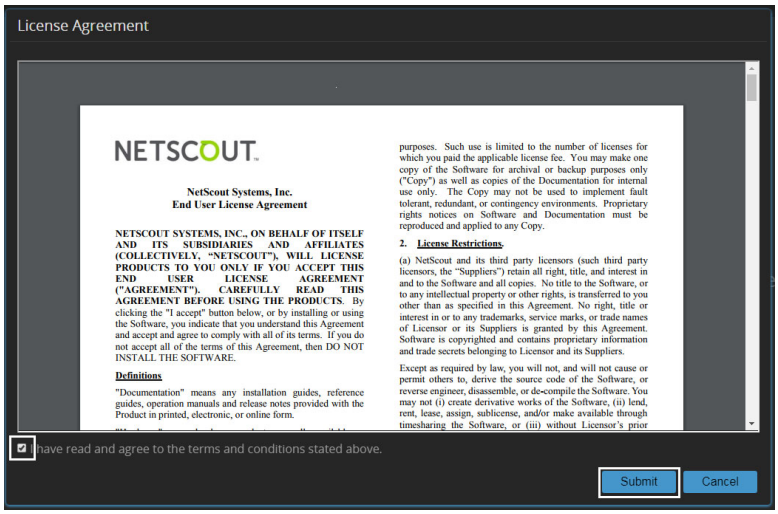
Important: The first time the admin user logs in to a Fabric Manager appliance, the user will be required to change their password.

Note: Password minimum length is 8 characters and must contain at least 1 uppercase and 1 lowercase character.

Important: The account is locked after three (3) consecutive unsuccessful password login attempts. The lockout times out after 15 minutes, allowing the user to re-attempt to login at that time.

6 Click **Login**.

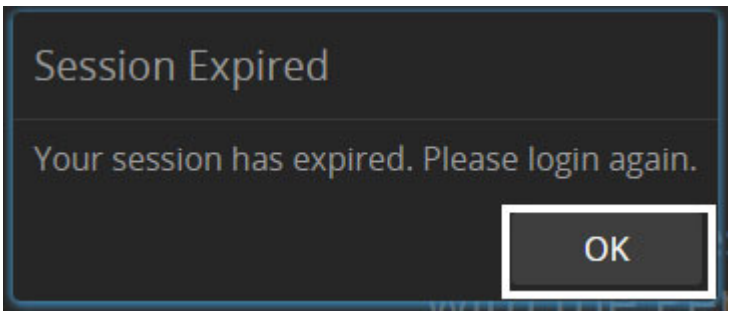
7 Click on the End User License Agreement acceptance statement check box then click **Submit**.



8 The PFS Fabric Manager interface displays (refer to PFS Fabric Manager Interface Screen on page 2-2).

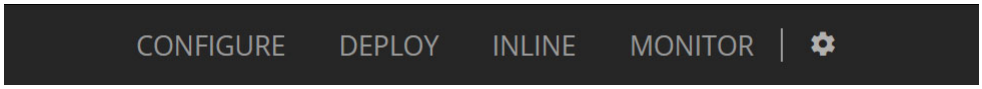
PFS Fabric Manager Session Expiration

After approximately 30 minutes of session inactivity, PFS Fabric Manager automatically logs you out of the current session, displaying a message informing you that your session has expired and to login again to continue. Clicking **OK** to acknowledge the message sends you back to the PFS Fabric Manager login screen.



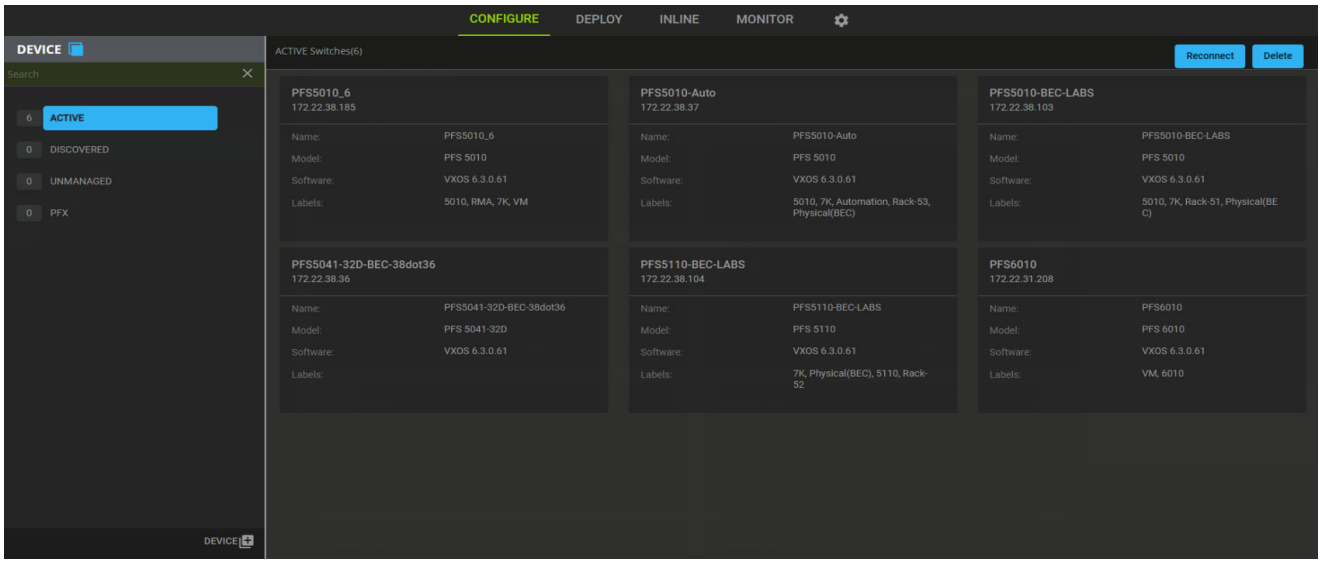
PFS Fabric Manager Interface Screen

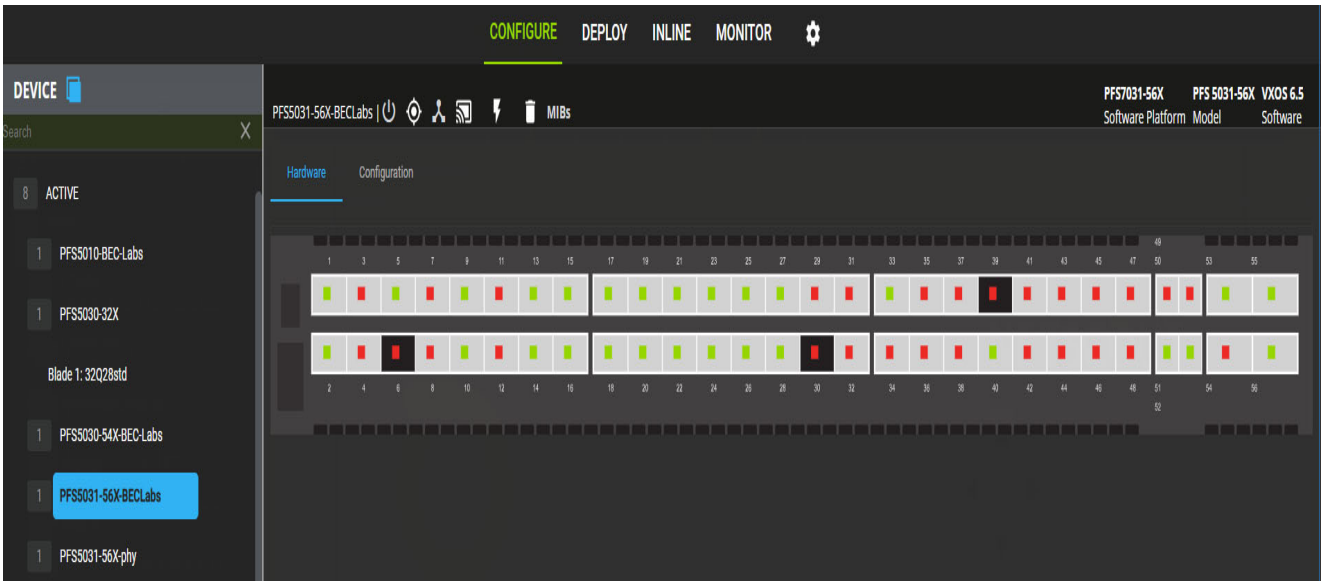
After logging on to PFS Fabric Manager, the interface screen displays. At the top of the screen are four main sections / lifecycles plus the Settings cog. These sections are described, at a high level, in this section.

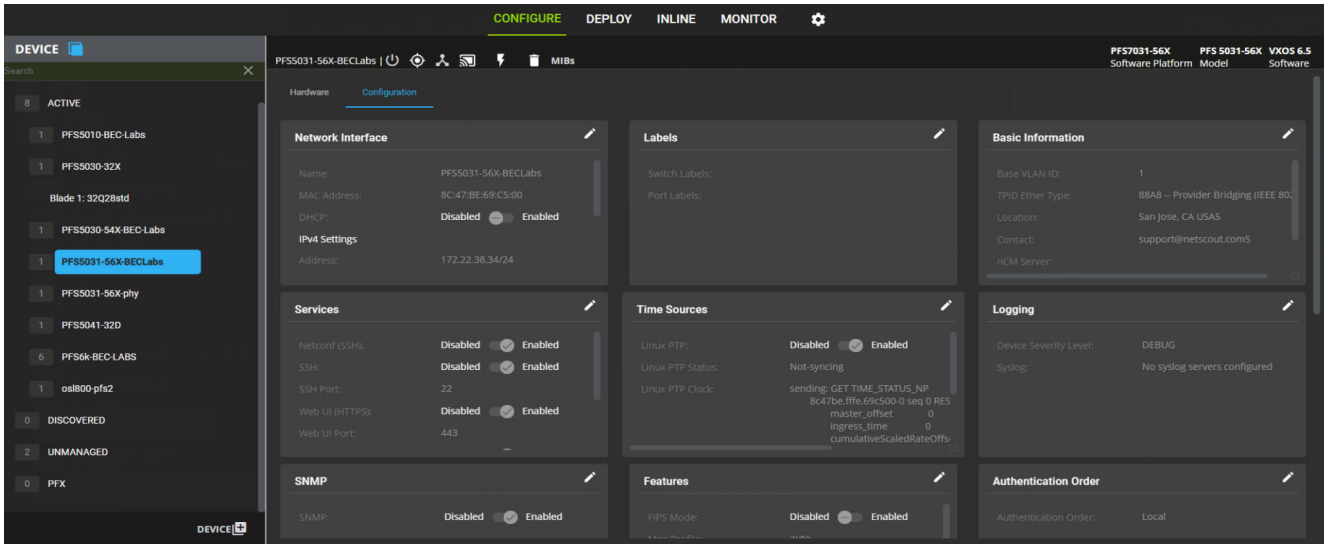


Configure Lifecycle

Configure Lifecycle allows discovering all connected switches and line cards on the network and defining the configuration properties of switches / devices, ports, port groups, port profiles, and filters. See Configure Lifecycle on page 3-1 for details.




CONFIGURE
DEPLOY
INLINE
MONITOR
DEVICE
Search
8 ACTIVE
1 PFS5010-BEC-Labs
1 PFS5030-32X
Blade 1: 32Q28stdd
1 PFS5030-54X-BEC-Labs
1 PFS5031-56X-BECLabs
1 PFS5031-56X-phy
PFS5031-56X-BECLabs | MIBs
PFS7031-56X Software Platform
PFS 5031-56X Model
VXOS 6.5 Software
Hardware
Configuration

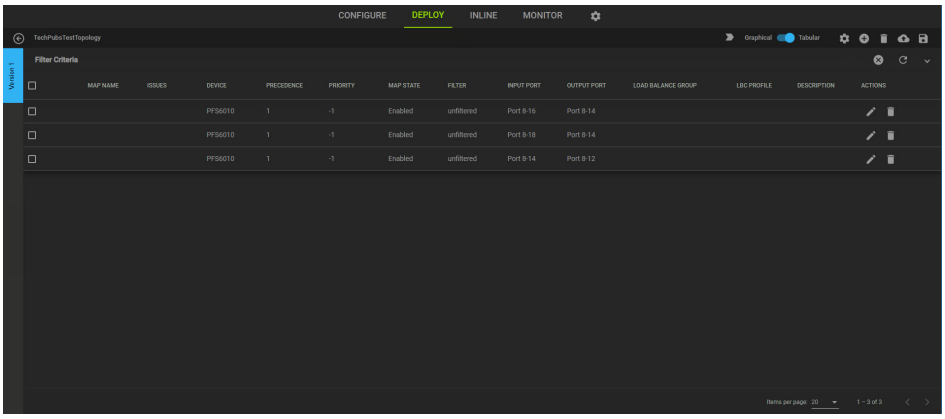

CONFIGURE
DEPLOY
INLINE
MONITOR
DEVICE
Search
8 ACTIVE
1 PFS5010-BEC-Labs
1 PFS5030-32X
Blade 1: 32Q28stdd
1 PFS5030-54X-BEC-Labs
1 PFS5031-56X-BECLabs
1 PFS5031-56X-phy
1 PFS5041-32D
6 PFS6k-BEC-LABS
1 osl800-pfs2
0 DISCOVERED
2 UNMANAGED
0 PFX
DEVICE
PFS5031-56X-BECLabs | MIBs
PFS7031-56X Software Platform
PFS 5031-56X Model
VXOS 6.5 Software
Hardware
Configuration
Network Interface
Name: PFS5031-56X-BECLabs
MAC Address: 8C:47:BE:69:C5:00
DHCP: Disabled Enabled
IPv4 Settings
Address: 172.22.38.34/24
Labels
Switch Labels:
Port Labels:
Basic Information
Base VLAN ID: 1
TPID Ether Type: 88A8 -- Provider Bridging (IEEE 802.
Location: San Jose, CA USA5
Contact: support@netscout.com5
nCM Server:
Services
Netconf (SSH): Disabled Enabled
SSH: Disabled Enabled
SSH Port: 22
Web UI (HTTPS): Disabled Enabled
Web UI Port: 443
Time Sources
Linux PTP: Disabled Enabled
Linux PTP Status: Not-syncing
Linux PTP Clock: sending: GET TIME_STATUS_NP
8c47be.fffe.69c500-0 seq 0 RES
master_offset 0
ingress_time 0
cumulativeScaledRateOffs
Logging
Device Severity Level: DEBUG
Syslog: No syslog servers configured
SNMP
SNMP: Disabled Enabled
Features
FIPS Mode: Disabled Enabled
Authentication Order
Authentication Order: Local

Deploy Lifecycle

Deploy Lifecycle allows creating, versioning, and publication of topologies. The Deploy Lifecycle provides two view for a topology: graphical and tabular. See Deploy Lifecycle on page 4-1 for details.

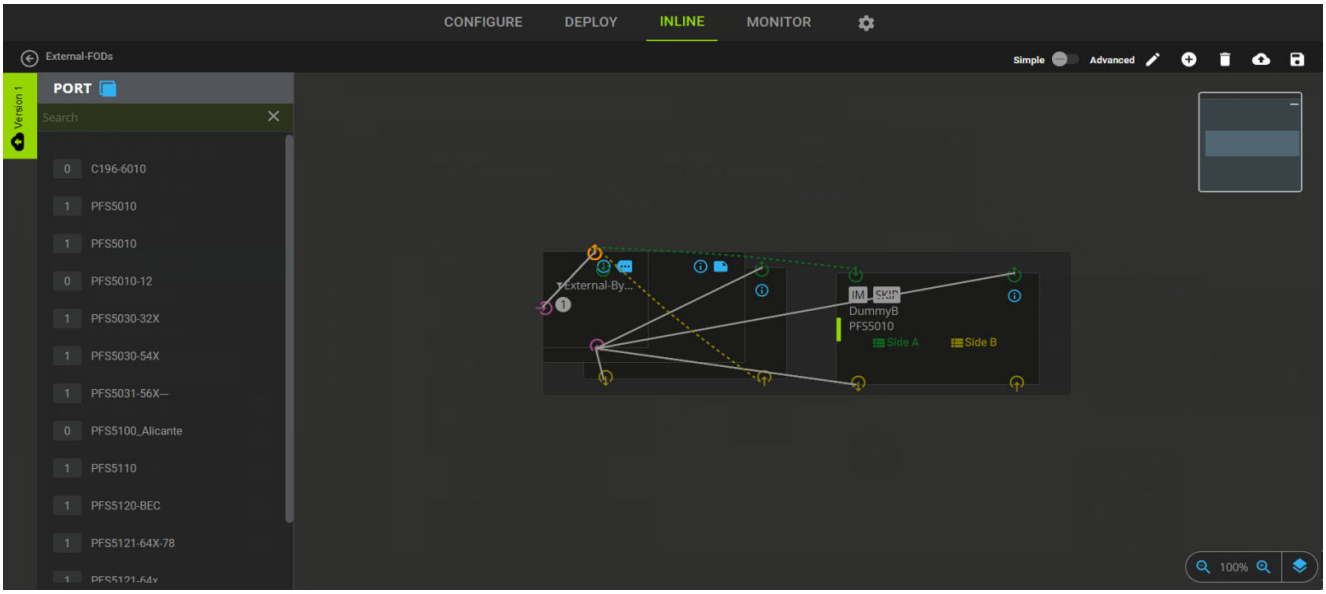
Graphical

Tabular



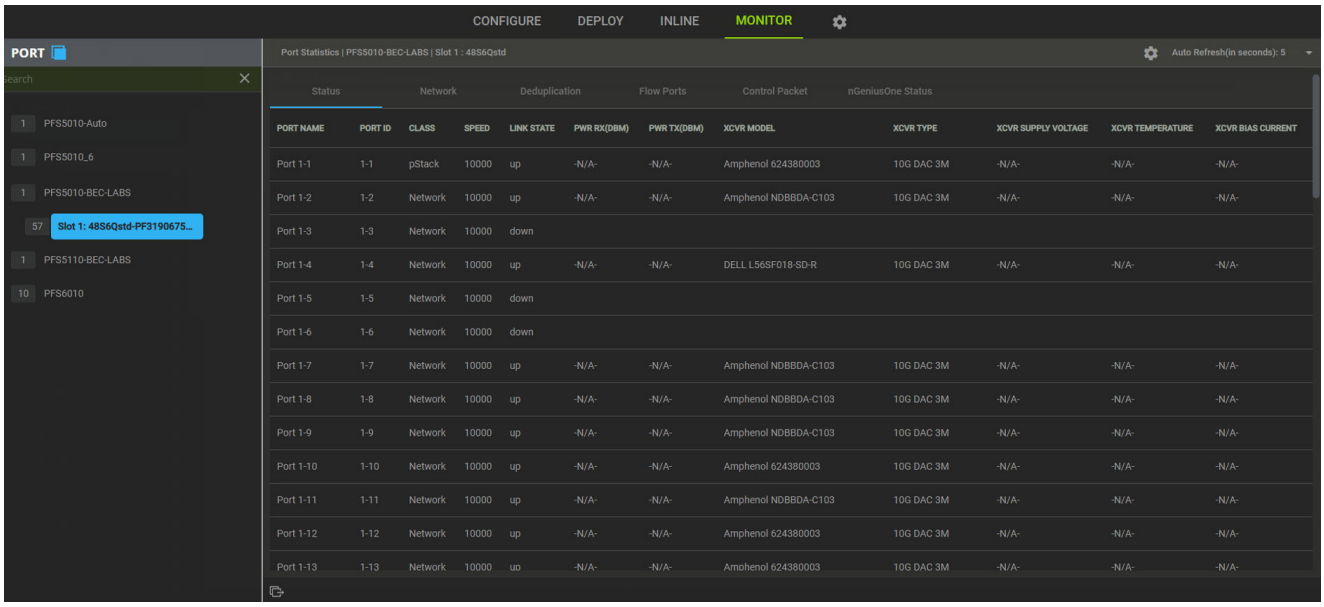
Inline Lifecycle

Inline Lifecycle allows creating, versioning, and publication of Inline topologies. See Inline Lifecycle on page 5-1 for details.



Monitor Lifecycle

Monitor Lifecycle allows viewing the operational status and statistics of devices and ports. See Monitor Lifecycle on page 6-1 for details.

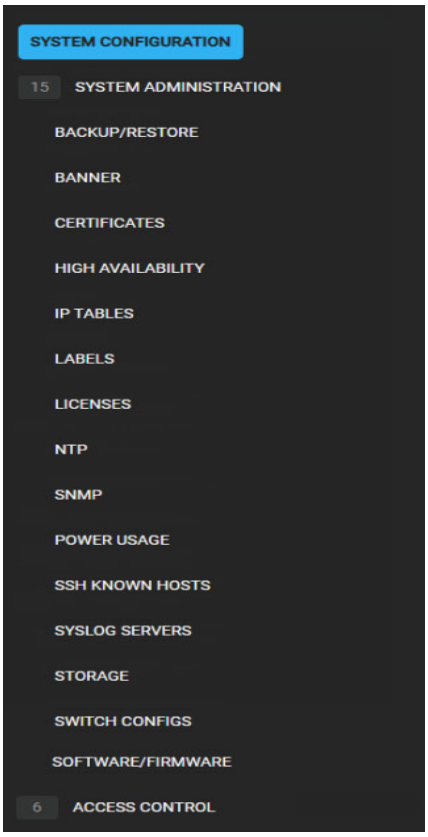


System Settings

Clicking on the **Settings** (COG) icon provides the following functions:

- System Administration
  - Backup/Restore
  - Banner
  - Certificates
  - High Availability
  - IP Tables
  - Labels
  - Licenses
  - NTP
  - SNMP
  - Power Usage
  - SSH Known Hosts
  - Syslog Servers
  - Storage
  - Switch Configs
  - Software/Firmware

- Access Control
  - User Management
    - My Account
    - All Users
  - Access Policy
  - Authentication Order
  - Authentication Servers
  - Roles
  - Managed Devices -



See System Settings on page 7-1 for details.

Bringing a PFS into Central Management

There are two ways to connect a PFS to a PFS Fabric Manager Central Server; these are described in the following sections.

Connecting to the PFS from the NMS

1. Log in to the NMS.
2. Go to the Configure Lifecycle (see Configure Lifecycle on page 3-1 for more details).
3. Select the Device Perspective (see Perspective > Device on page 3-5 for more details).
4. Click on + Device in the lower right of the Perspective pane.
5. Select the PFOS Switch Device Type.
6. In the slideout that appears, enter the IP address or hostname of the PFS to which the NMS should connect.
7. Accept the changes.

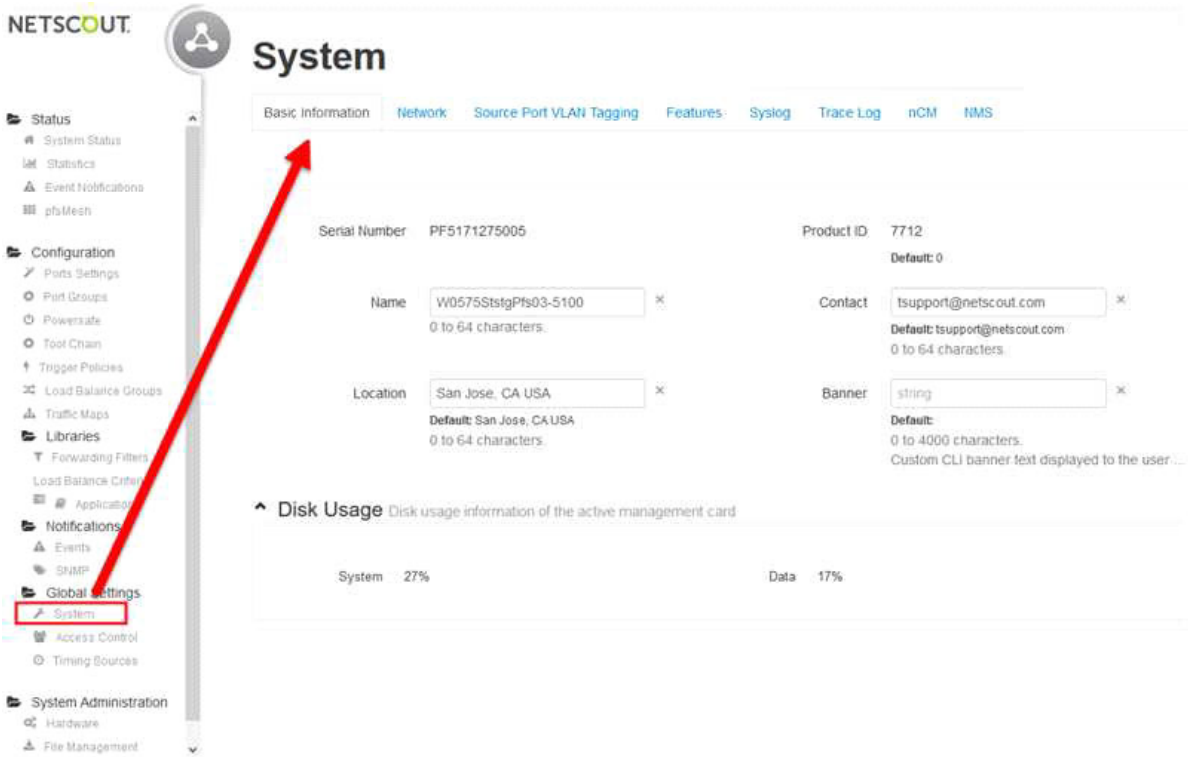
The NMS will now connect to the PFS, retrieve basic information about the switch, and place it in the list of Discovered switches. Proceed to Accepting Switches into Central Management on page 2-9 to accept the switch into the list of devices managed by the NMS.

Note: The NMS Server address (described in the next section) will be automatically configured by the NMS once the device is accepted into central management.

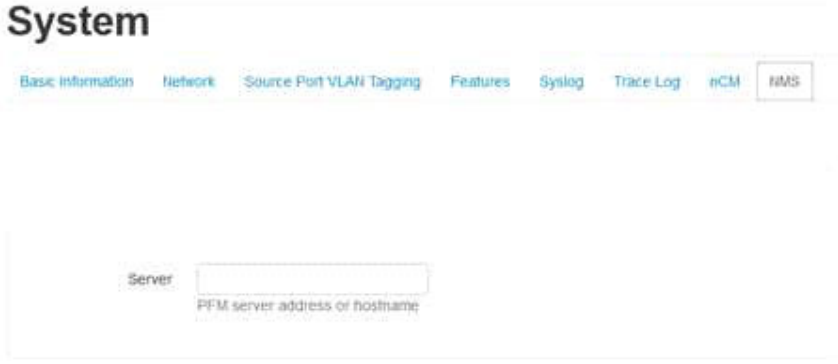
Configuring the NMS address in the PFS

Users can also configure the PFS to connect to the NMS. This is an alternative workflow to that presented in Connecting to the PFS from the NMS above; if that workflow was followed the steps in this section are not necessary.

1. Connect to the web UI of the PFS (configuring is also possible via other interfaces but is not covered here; refer to the PFOS documentation for details).
2. In the web UI, click on the Global Settings -> System link.



3. Click on the NMS tab.



4 Enter the IP address or hostname of the NMS to which the PFS should connect.

5 Click Apply to save the configuration change.

The PFS will now send a message to the NMS to ask to be managed. The NMS will connect to the PFS, retrieve basic information about the switch, and place it in the list of Discovered switches. Proceed to Accepting Switches into Central Management on page 2-9 to accept the switch into the list of devices managed by the NMS.

Accepting Switches into Central Management

Once the NMS has connected to a PFS, it will show up in the list of Discovered switches in the Configure Lifecycle, Device Perspective. For more details on the Configure lifecycle, see Configure Lifecycle on page 3-1.

To accept a Discovered switch into Central Management:

1 Log in to the PFS Fabric Manager Central Server.

2 Go to the Configure Lifecycle.

3 Go to the Device Perspective.

4 Select the list of Discovered devices.

5 Select a device in the list then click Accept. The verification/confirmation process begins.

Once the PFS is successfully accepted it will move to the list of Active devices. The device is now ready for use/configuration.

Note: There will be a brief delay, after accepting the device, during which the switch is being learned from the PFS Fabric Manager (configuration/hardware learning).

Importing the PFS Configuration into the NMS

Once a PFS is accepted into management, PFS Fabric Manager will automatically learn the configuration of the PFS.

The configuration of the PFS, its ports, and any filters, load balance groups, and other entities can be viewed in the Configure lifecycle. See Configure Lifecycle on page 3-1 for details.

Any traffic maps configured on the PFS will be visible on the Device Topology for that PFS. Users will normally want to copy these traffic maps to user topologies for day-to-day use. See Saving Imported Traffic Maps as User Topologies on page 4-2 for details.

Note: PFS Fabric Manager continually learns about changes made to the PFS via other interfaces. The configuration import described in this section is effectively performed continuously.

Removing a PFS from Central Management

To remove a PFS from Central Management:

1 Log in to the PFS Fabric Manager Central Server.

2 Go to the Configure Lifecycle.

3 Select the Device Perspective.

4 Select the PFS to be deleted from among the Active devices.

5 Click on the "…" to the right of the PFS' name.

6 Select Delete Switch.

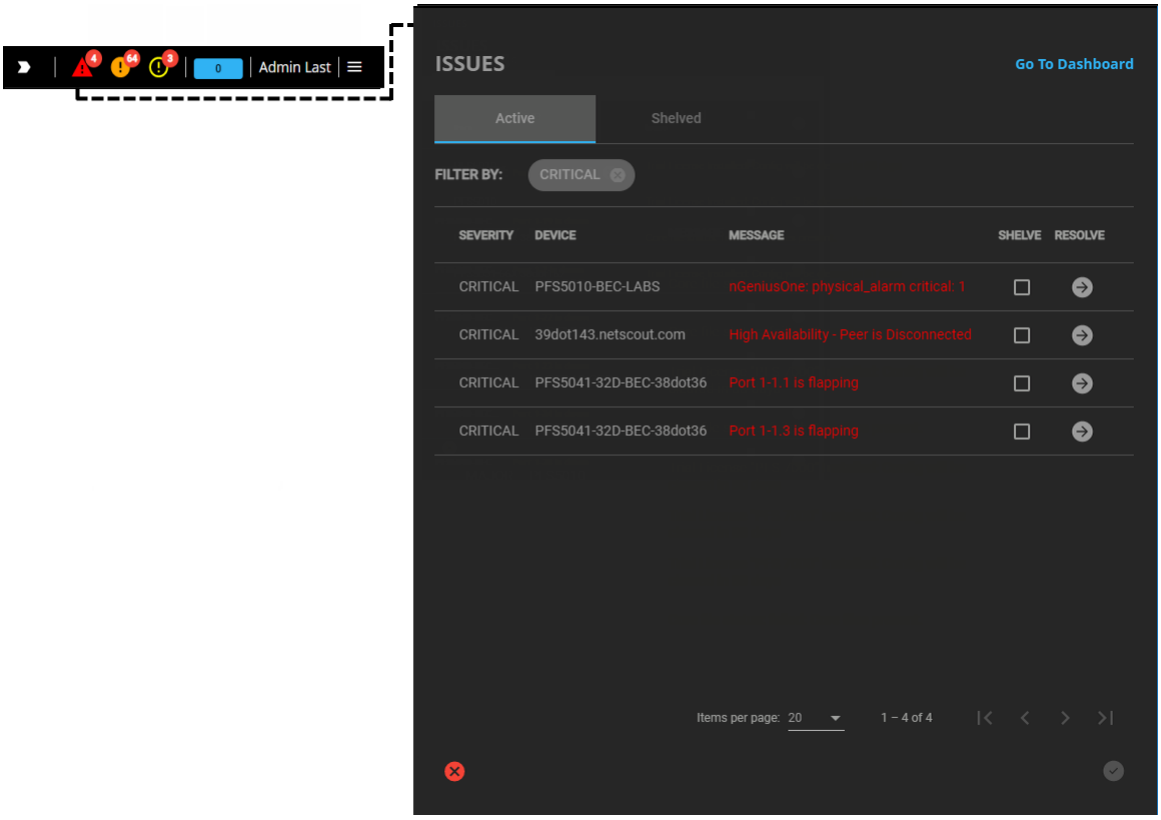
Note: As part of the switch deletion process, PFS Fabric Manager will remove itself from the NMS server address configuration in PFOS. If the PFS is currently disconnected, PFS Fabric Manager will delete the switch but will not be able to modify the switch's configuration. If the PFS is later reconnected to the network and still has the NMS server address configured, it will appear as a Discovered device on the Central Server.

Issues

Clicking on the issues indicator displays alarms broken out by the following categories:

- Active
- Shelved

The issue indicator displays a color-coded list of Critical, Major or Info badges with the count of the alarms for each severity level.

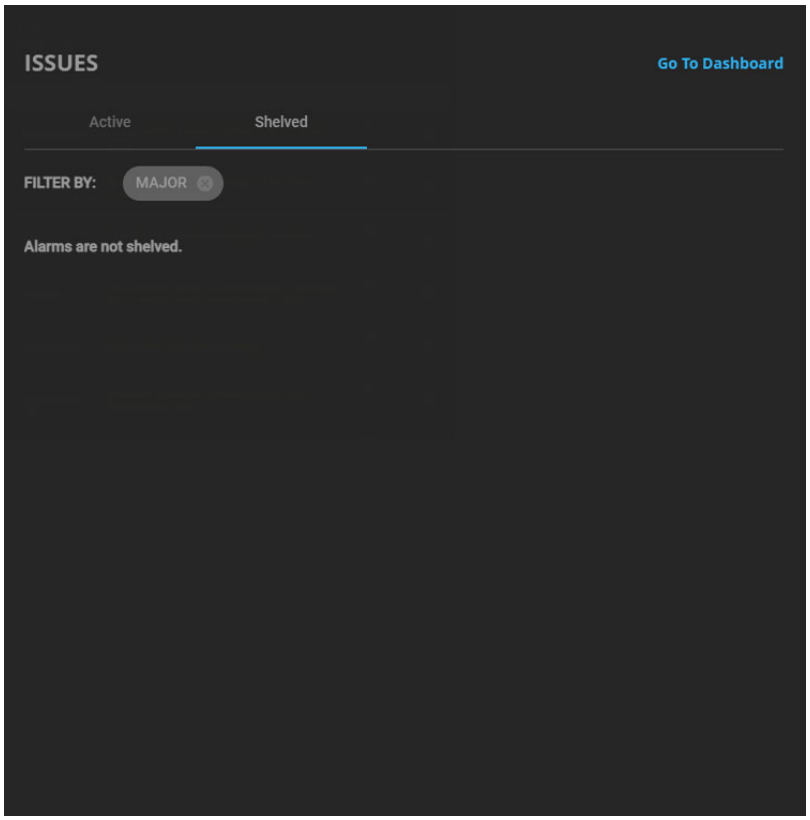


From the Active tab, the user can chose to acknowledge or shelve the alarm. When an alarm is shelved it is no longer displayed in the active tab. A shelved alarm may still be in the active state, but is not shown by default.

Shelved alarms are displayed in the Shelved tab, where the user can acknowledge or unshelve the alarm.

Clicking on **Resolve** for an nGeniusOne alarm navigates the user to the nGeniusOne Alarms dashboard, which matches to the nGeniusOne notification center. The nGeniusOne Alarms dashboard displays alarms for all switches that have been added to nGeniusOne.

Clicking on **Go to Dashboard** navigates the user to the Alarms dashboard.



Alarms and Severities

The following table lists the alarms and their default severities.

Alarm	Severities	Description
Backup	**MAJOR** - Backup failed completely. No devices backed up. **WARNING** - Some devices not backed up **OK** - Backup is OK	Backup failure alarm
Certificate	**MAJOR** - Certificate is expired **WARNING** - Certificate expires soon **OK** - Certificate is OK	Certificate expiration alarm. The "soon" is controlled by system config parameter. Should probably make distinction for different types, like syslog.
Device Down	**CRITICAL** - Device is disconnected (no NETCONF connection) **MAJOR** - Device is connected but not learned **OK** - Device is connected and learned	Device has been accepted but has not become fully managed by PFM

Device Generated	**CRITICAL** - Device alarm is **FAILED**, unit needs immediate attention. Specific units that invoke this severity when failed: • disk-01 • disk-02 **MAJOR** - Device alarm is **FAILED** or **EMPTY**, unit needs eventual attention. Specific **EMPTY** units that are ignored: • i2c-xx - Line card and other slots • temp-xx - Temperatures for i2c-xx slots. **OK** - Device alarm state is OK	Alarms reported by device "unit" such as fan speed, temperature, etc. Reported alarm states: • OK- monitored, within range – Clear PFM alarm if any • FAILED- monitored, out of range – Raise PFM alarm • ACKNOWLEDGED - unmonitored, out of range – Shelve PFM alarm • INIT- unmonitored, unit results not ready – Clear PFM alarm if any • EMPTY- monitored, unit not present – Raise PFM alarm
Disk Full	**CRITICAL** - Disk space is more than 95% **WARNING** - Disk space is less than 95% **OK** - Disk space is OK	Disk full alarm.
High Availability	**CRITICAL** - Peer is not connected. **MAJOR** - Peer is connected but not synchronized **OK** - HA is OK. Peer connected and synchronized.	High Availability failure alarm.
License	**CRITICAL** - License is an expired TRIAL license **MAJOR** - TRIAL license expires soon. **MAJOR** - License is a TRIAL license **MAJOR** - Full License is expired **WARNING** - Full License expires soon **OK** - License is OK	License expiration alarm. The "soon" is controlled by system config parameter.
Port Flapping	**CRITICAL** - Port is flapping **OK** - Port is not flapping	A port is flapping. Pstack routing ramifications, notifications.
Port Down	**MAJOR** - Port is down unexpectedly **OK** - Port is up	A port with link state "down" that is on an active blade, with a transceiver, that has not been manually brought down, is down unexpectedly.
Remote Monitor Group	**WARNING** - Remote Monitor Group is not visible **OK** - Remote Monitor Group is visible	Remote monitor group alarm. When a port group is used as an RMG in a map, an alarm is raised if the group is not visible to the source device. This alarm detection does not consider mesh visibility, in case the RMG is not mesh visible.

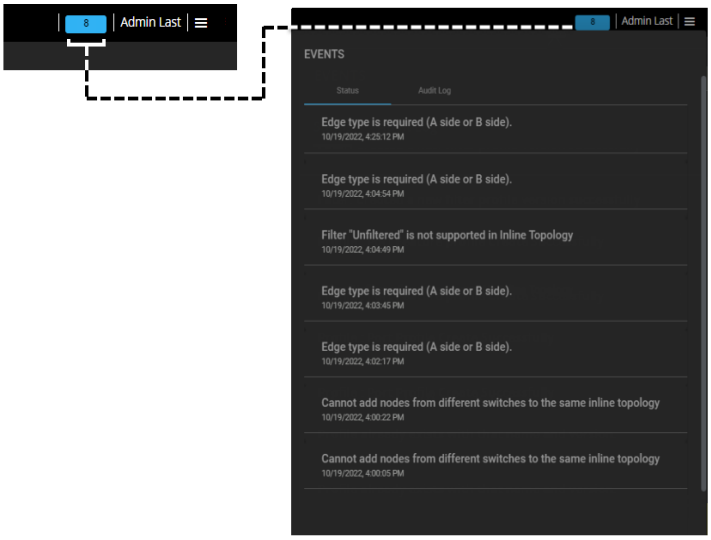
Restore	**MAJOR** - Restore failed completely. No devices were restored. **WARNING** - Some devices not restored **OK** - Restore is OK	Restore failure alarm.
Sync	**MAJOR** - Sync failed completely. Backups were not synced to any sync destination. **WARNING** - Sync failed on some destinations **OK** - Sync succeeded on all destinations.	Backup sync failure.
Traffic Map	**CRITICAL** - Map status error code **OK** - Traffic map status is OK	Traffic map status alarm.
Watermark	**CRITICAL** - Based on upper watermark limit. Notifies the user that the upper watermark level has been reached and cleanup will start, only if the Historical Stats are in an enabled state. **WARNING** - Based on lower watermark limit. Notifies the user that the lower watermark limit of the disk storage for the partition is satisfied.	Upper/Lower Watermark level limit alarm.

Viewing Events

Clicking on the small numbered indicator displays recorded events broken out by the following categories:

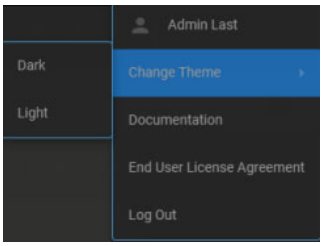
- Audit Log
- Status

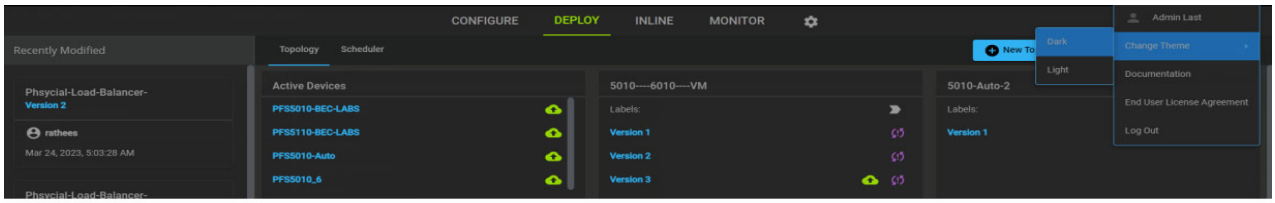
The number indicates the number of recorded events listed. The events can be archived, exported, or removed as required.

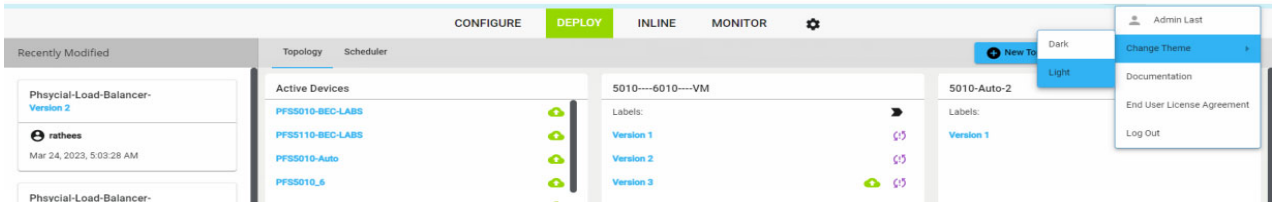


Changing the Theme

You can change the default background color scheme of PFS Fabric Manager by selecting the menu icon and click on **Change Theme**.

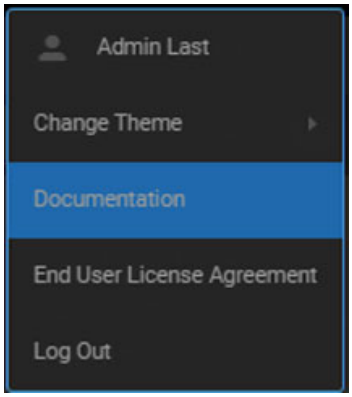




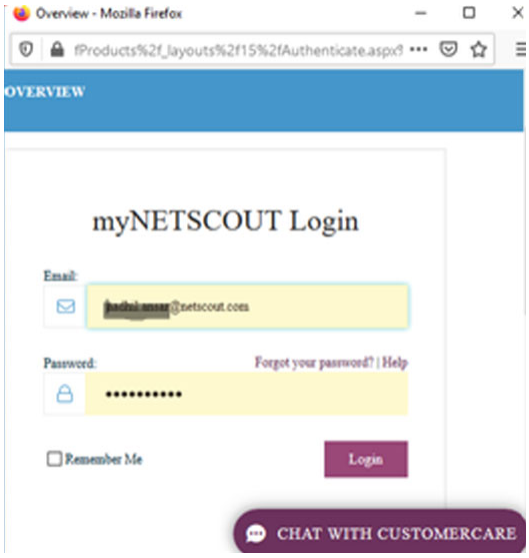


Documentation

You can view PFS Fabric Manager documentation by selecting the menu icon and click on **Documentation**.

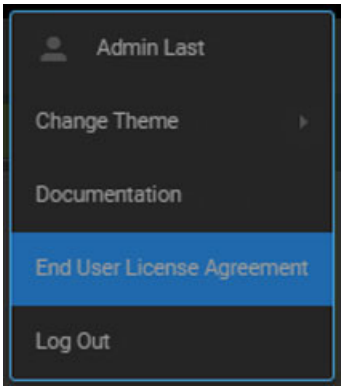


A popup browser window will appear. Enter your NETSCOUT credentials to view and download PFS Fabric Manager documents.

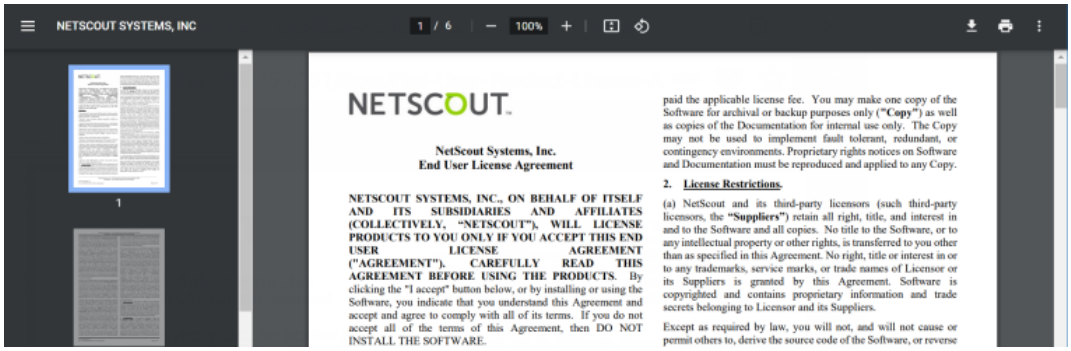


End User License Agreement

You can view End User License Agreement (EULA) by selecting the menu icon and click on **End User License Agreement**.



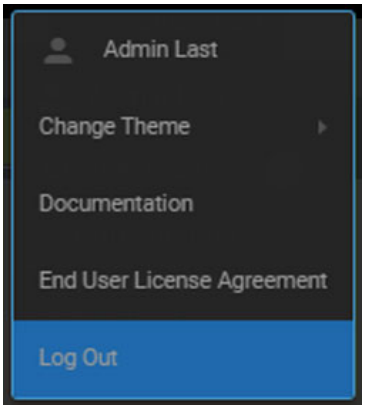
A popup browser window will appear displaying the EULA.



Logout of PFS Fabric Manager

To end the current user's PFS Fabric Manager session:

On the right side of the interface screen, select the menu icon and click on **Logout**.

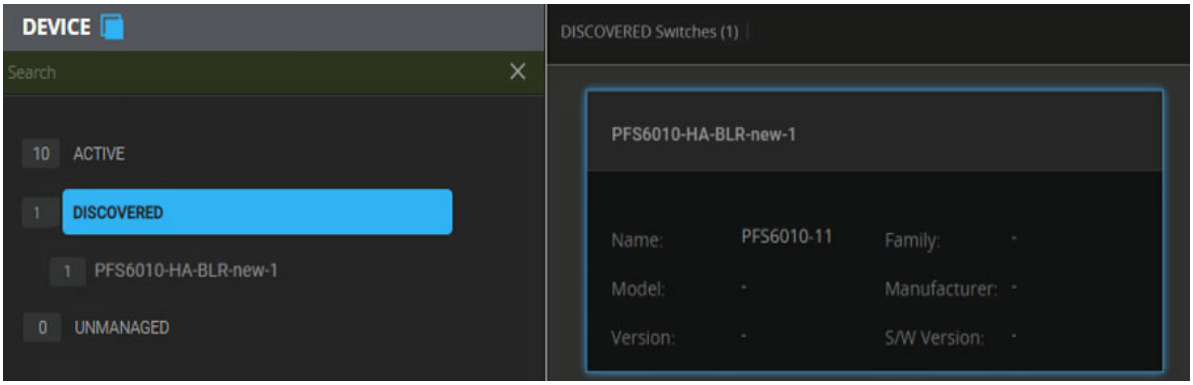


Chapter 3
Configure Lifecycle

This chapter describes how to discover, configure and activate switches, line card ports, and filters on your system.

Discover Switches

From the Perspective > Device menu, selecting Discovered lists the identified switches on the network. Clicking on a switch displays a tree view and graphic of the line cards installed in the switch.



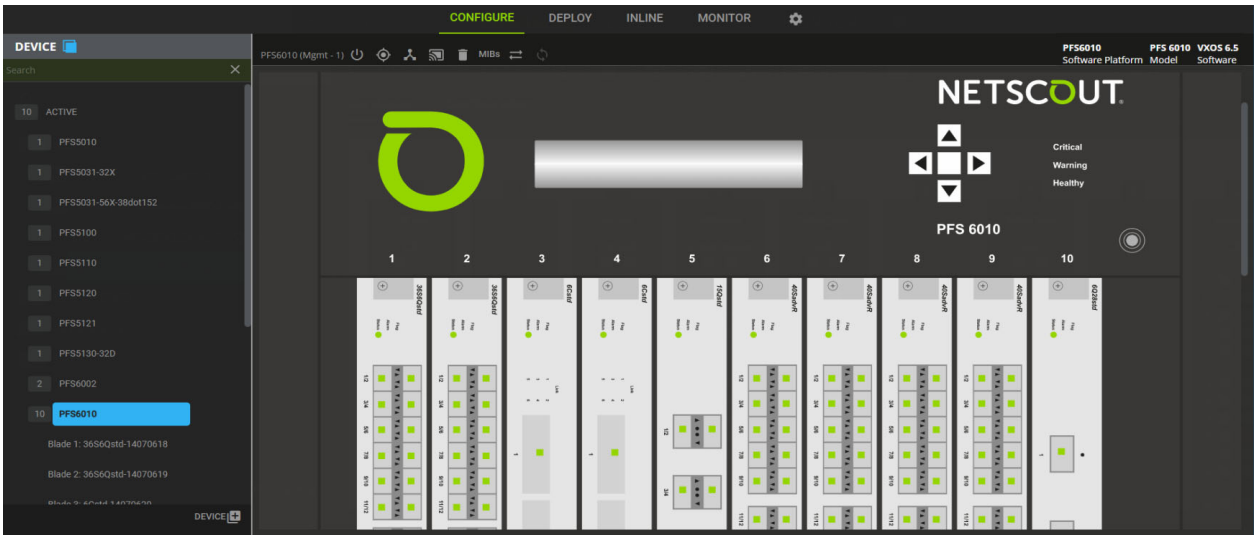
Device > Switch Acceptance

Switches must be accepted into management before use. Once a switch is accepted, it will appear under the Active tree-view folder with all attributes associated with the switch available for configuration and publication.

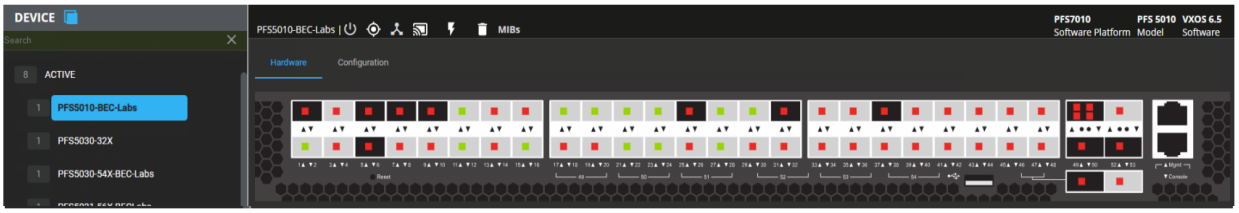
From the Discovered list, select a device (switch) name - not a blade associated with the device, then click **Accept**. The verification / confirmation process begins.

Once the verification process completes, the switch is made active with the line cards and ports now available for usage. Clicking on **Hardware** displays a graphic of the line cards installed in the accepted switch. Clicking on the active switch displays a list of the installed line cards.

PFS 6010 Switch



PFS 5010 Switch



PFS 5110 Switch

Perspective Menus

The Perspective menus provide access to all devices (switches), ports, groups, profiles, filters, and triggers.

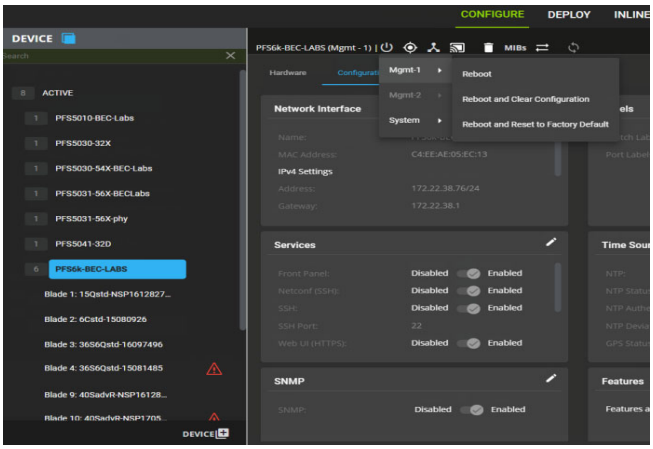
Five categories are available from the Perspective menu:

- Device - refer to Perspective > Device on page 3-5
- Port - refer to Perspective > Port on page 3-33
- Group - refer to Perspective > Group on page 3-47
- Profile - refer to Perspective > Profile on page 3-54
- Filter - refer to Perspective > Filter on page 3-78
- Trigger - refer to Perspective > Trigger on page 3-87

Rebooting Selected Management Cards/Entire Chassis

From Configure Lifecycle > Device the user has the ability to reboot a specific management card or the entire chassis. Options include:

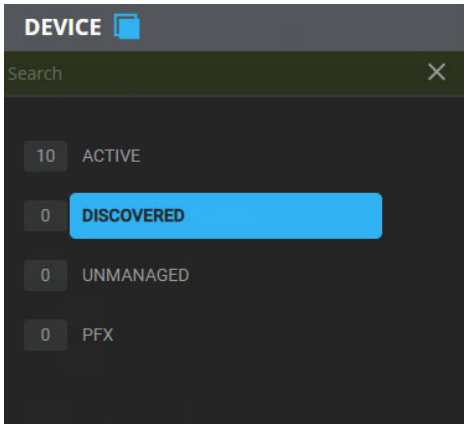
- Reboot: Reboot the system.
- Reboot and Clear configuration: Clears all settings except basic system and networking settings (such as IP addresses).
- Reboot and Reset to factory default: Clears all settings including system and networking settings.



Perspective > Device

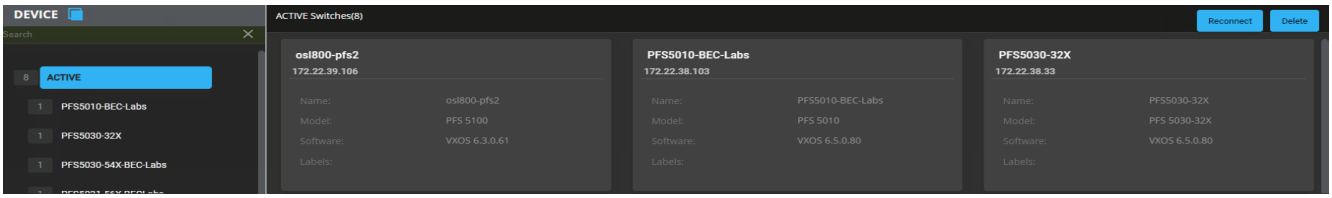
Selecting Device from the Perspective menu displays the devices (switches) connected to the PFS network.

Four categories are defined under the Device view:



Active

Lists the accepted devices. Clicking on Active displays the name / model / installed PFOS software and IP address of each of the accepted devices.



Clicking on a device displays the Hardware / Configuration screen allowing detailed viewing of each device and installed line cards (refer to Device > Switch Acceptance on page 3-2) and updating the configuration settings (refer to Configure / Update Devices on page 3-12) of the device.

Active Switch Sub-Menu

Each displayed active switch has a menu with the following functions:

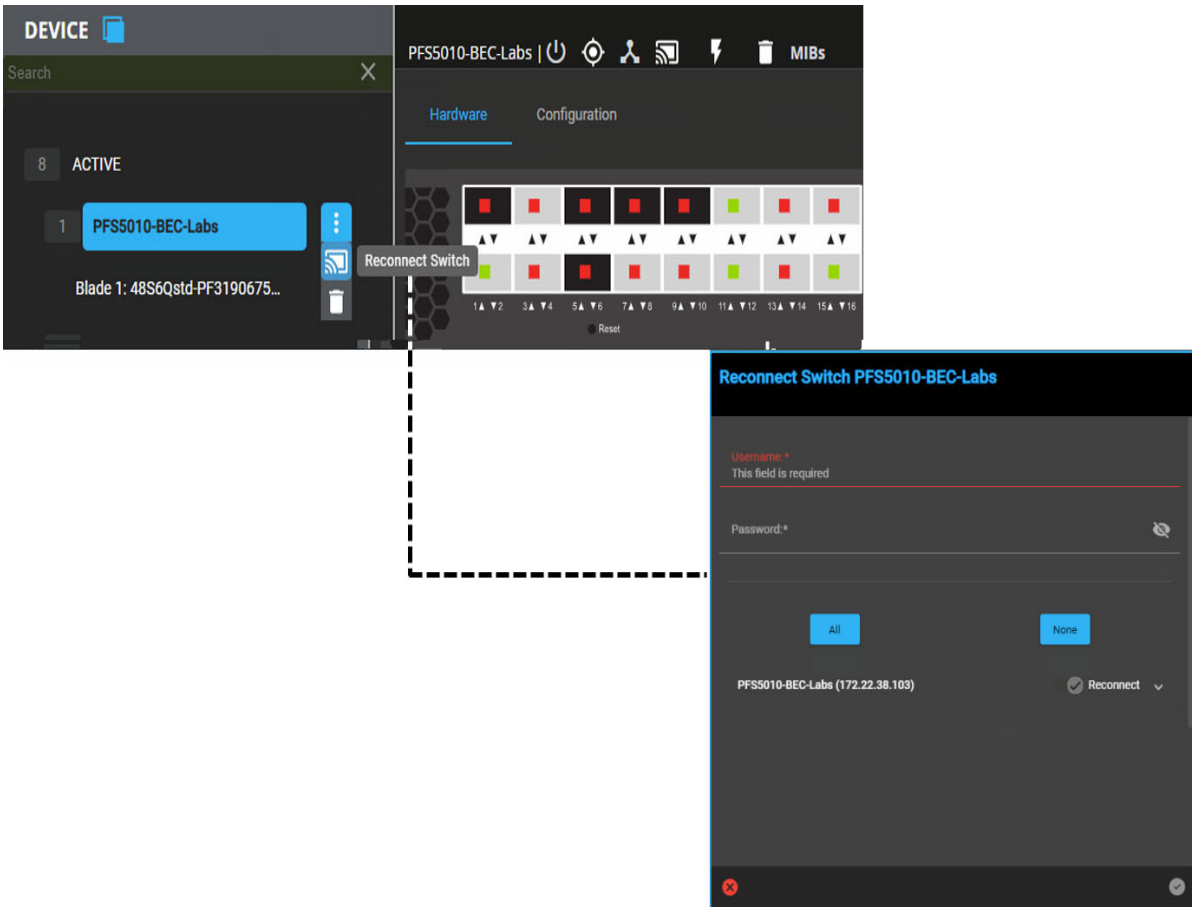
- Reconnect Switch
- Delete Switch

Reconnect Switch

Selecting Reconnect Switch will shut down the active connection to the switch (if any), reconnect to the switch, and resync all configuration and state information

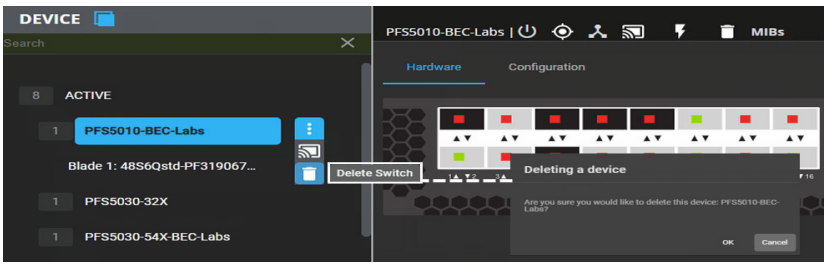
Reconnecting to a switch is required when the NMS has received an authentication failure when trying to communicate with the switch.

Reconnecting requires a user with admin-level credentials to the switch. These credentials are used only once to re-establish communication with the switch and are not stored; once communication is established, public-key cryptography is used for subsequent connections.



Delete Switch

Any switch that appears under the Active folder can be deleted.

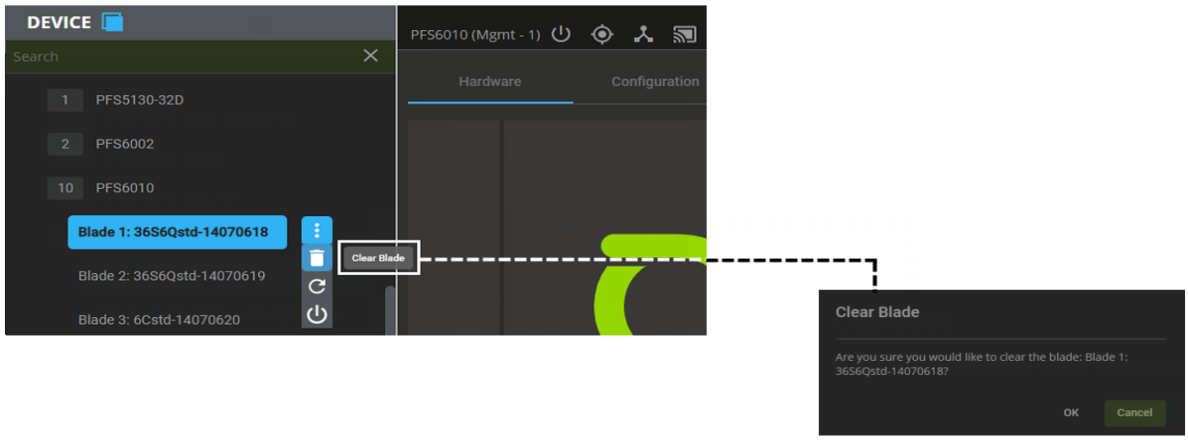


Blade Sub-Menu

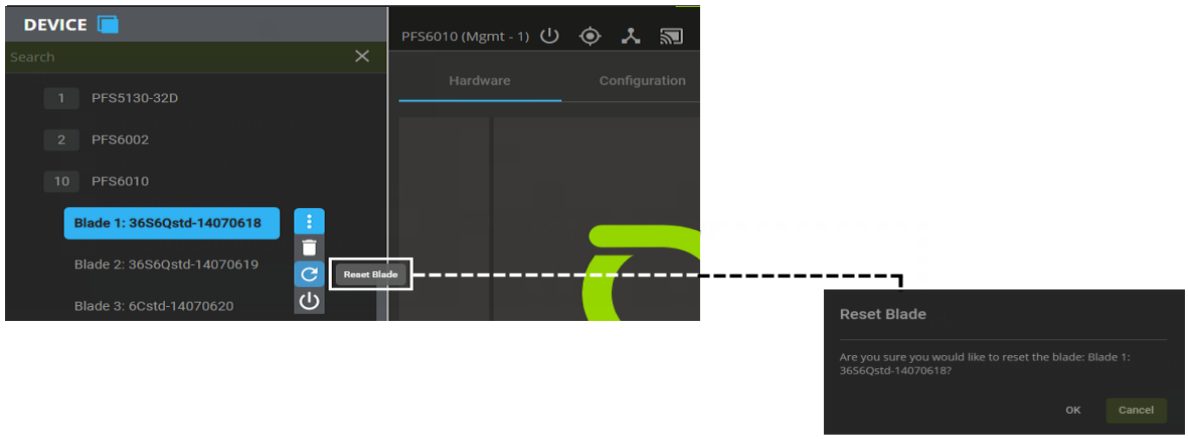
Each displayed active switch has a menu with the following functions:

- Clear Blade
- Reset Switch
- Shutdown Blade

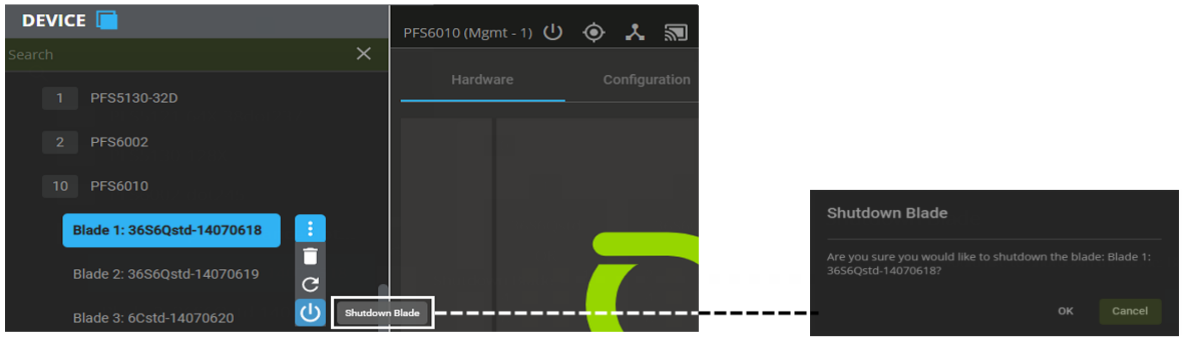
Clear Blade



Reset Blade



Shutdown Blade



Line Card Display Details

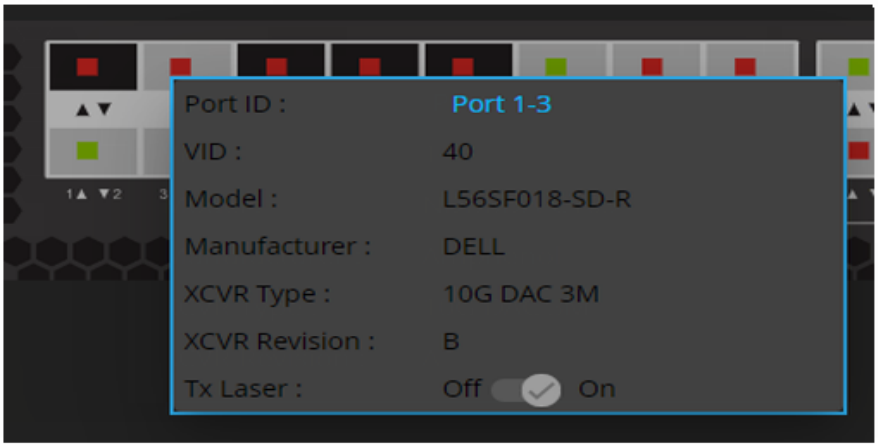
The graphical view of a PFS 6000 series line card includes a representation of the LEDs on the card, for example:

The LED statuses indicate the state of the line card:

State/LED	Status	Alarm	Flag
Empty			
Init	amber		
OK	green		
Shutting Down	green	red	
Shutdown		red	
Failed	amber	red	amber
Out of Service	amber	red	amber

Port Display Details

Port attributes are accessible from the Hardware graphic view. Clicking on an active line card port displays the details of the installed transceiver.



Line Card Port Indicators

Transceiver information of the physical ports is displayed as follows:

- Grey background - Transceiver is installed
- Black background - No transceiver is installed

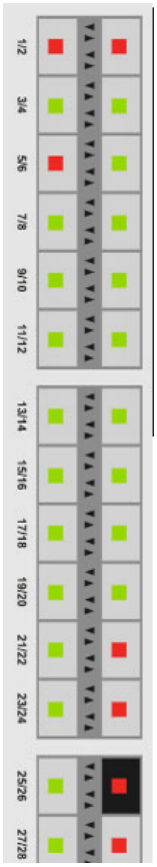
Each physical port may have one to four port status indicators, one for each subport. The port status indicators are displayed as follows:

o Green - Port is up

o Red - Port is down

o Amber - Port is flapping

Note: A port without a transceiver will be shown as “up” if its Link State is set to Force Up or if its port class is set to Service.



Port Flapping State

This release improves Fabric Manager behavior when one or more ports are flapping.

Detection (set flapping state):

Port flapping will be detected when link state changes for a specific port more than 10 times within 1 minute.

When a port flapping state is detected, a “flapping” message will be inserted into the syslog history. This message is specific to the central server and will not be present on the switch.

In addition, the port link state will change to “Flapping” and will have a yellow indicator.

Reset (turn off) the flapping:

The port will exit the flapping state when the link state does not change for 2 minutes. For example: XCVR is changed or Force Down or Up on Port is done (via pfos or NMS).

Syslog Updates Due to Flapping:

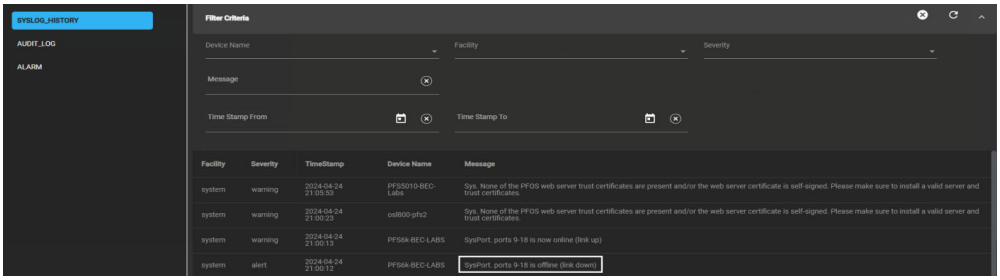
Syslog updates to the port for Sysport Up/Down are suppressed when link is continuously flapping, or until flapping is off.

system	alert	5/27/2021, 4:28:49 PM	pfs6010-1.3CPU-Bangalore	SysPort. ports 10-15 is flapping (link flapping)
system	warning	5/27/2021, 12:12:43 PM	pfs6010-1.3CPU-Bangalore	SysPort. ports 9-22 is now online (link up)
system	alert	5/27/2021, 12:12:43 PM	pfs6010-1.3CPU-Bangalore	SysPort. ports 9-22 is offline (link down)
system	warning	5/27/2021, 11:51:35 AM	pfs6010-1.3CPU-Bangalore	SysPort. ports 9-22 is now online (link up)
system	alert	5/27/2021, 11:51:35 AM	pfs6010-1.3CPU-Bangalore	SysPort. ports 9-22 is offline (link down)

Syslog Updates Due to Flapping:

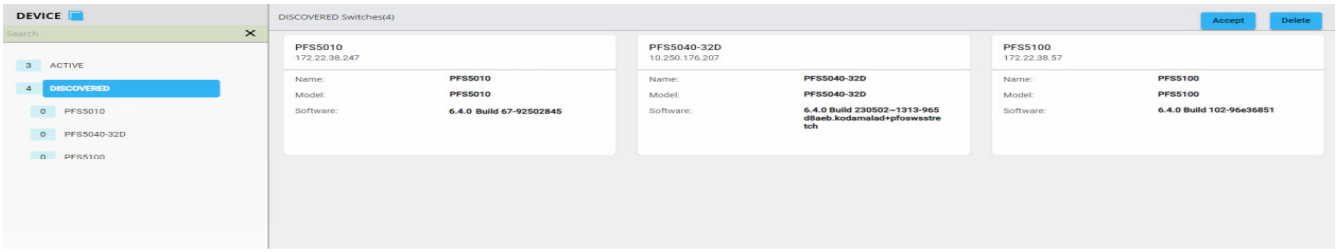
While the port is in a flapping state, additional syslog messages about the port link state will be discarded and the port link state will not change.

When a port exits the flapping state, a "flapping stopped" message will be inserted into the syslog history and the last syslog message about link state will be released. The port will be updated to the current link state and all changes and messages will be processed



Discovered

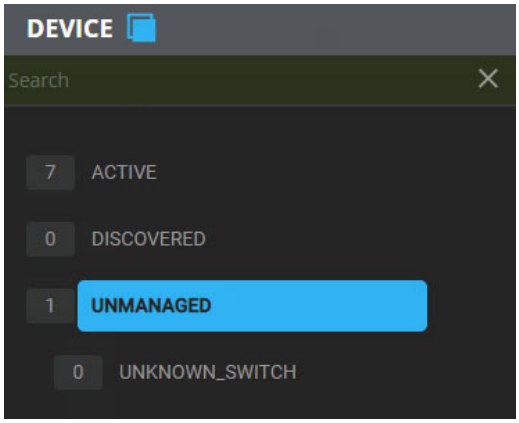
Lists the devices available but not managed by PFS Fabric Manager. Clicking on Discovered displays the name / model / installed PFOS software and IP address of each device.



Clicking on a device displays a Hardware screen allowing detailed viewing of each device and installed line cards (refer to Device > Switch Acceptance on page 3-2).

Unmanaged

Lists the devices (with or without PFS Fabric Manager) that are discovered through pfsMesh and not directly managed by the local PFS Fabric Manager. Devices not managed by PFS Fabric Manager are marked with an **RS** indicator.



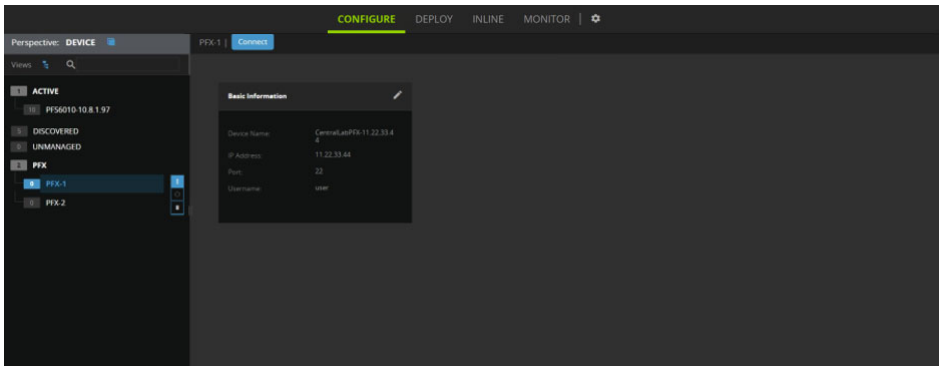
Clicking on a device displays a Hardware screen allowing detailed viewing of each device and installed line cards (refer to Device > Switch Acceptance on page 3-2).

Note: A device can appear in both Discovered and Unmanaged lists when a device that is not yet managed is connected through pStack.

PFX

Lists the PFX devices managed by PFS Fabric Manager. Clicking on PFX displays currently available configuration and a button to connect to this device (via CLI session).

Note: You must disable popup blockers before starting a CLI session.



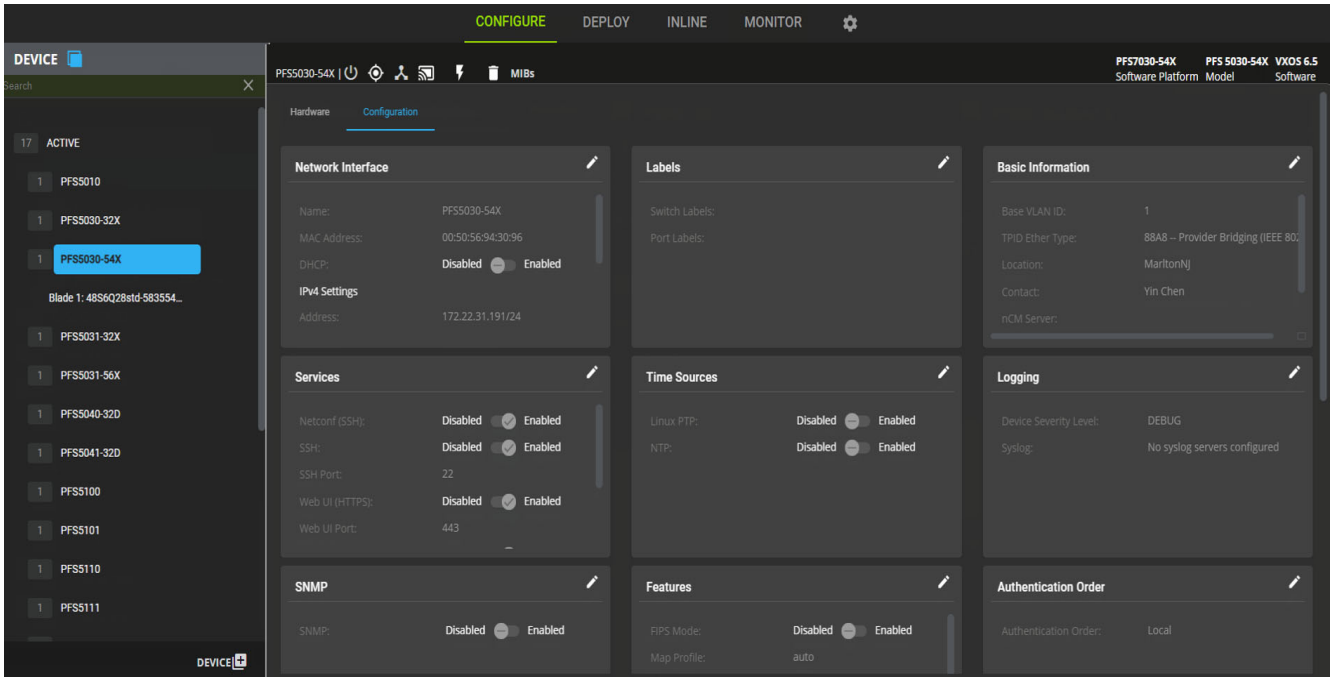
Clicking on a device displays basic information about the PFX.

Configure / Update Devices

From the Perspective > Device menu, you can select an active switch or PFX device and update the default settings for the switch/PFX device:

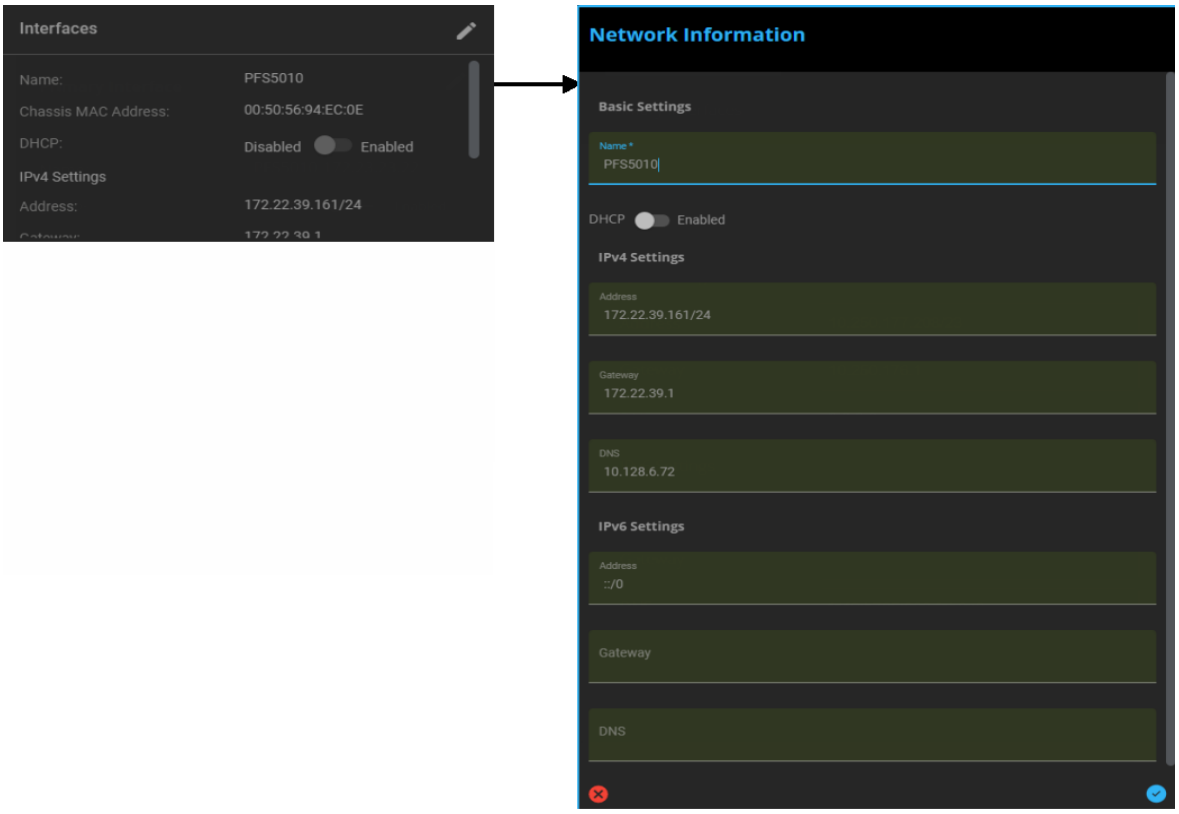
- Interfaces > Primary Interface - modify the IPv4 / IPv6 addresses.

- Profile: Default - includes the following:
  - Interfaces
  - Labels
  - Basic Information
  - Services
  - Time Sources
  - Logging
  - SNMP
  - Feature
  - Authentication Order
  - TACACS Server
  - RADIUS Server
  - LDAP Server
  - Stripping
- PFX > Basic Information



Interfaces > Network Information

Click the edit icon to make any changes to the current IP address settings. Click on the blue circled checkmark to save the changes or click the red **X** to cancel the changes.

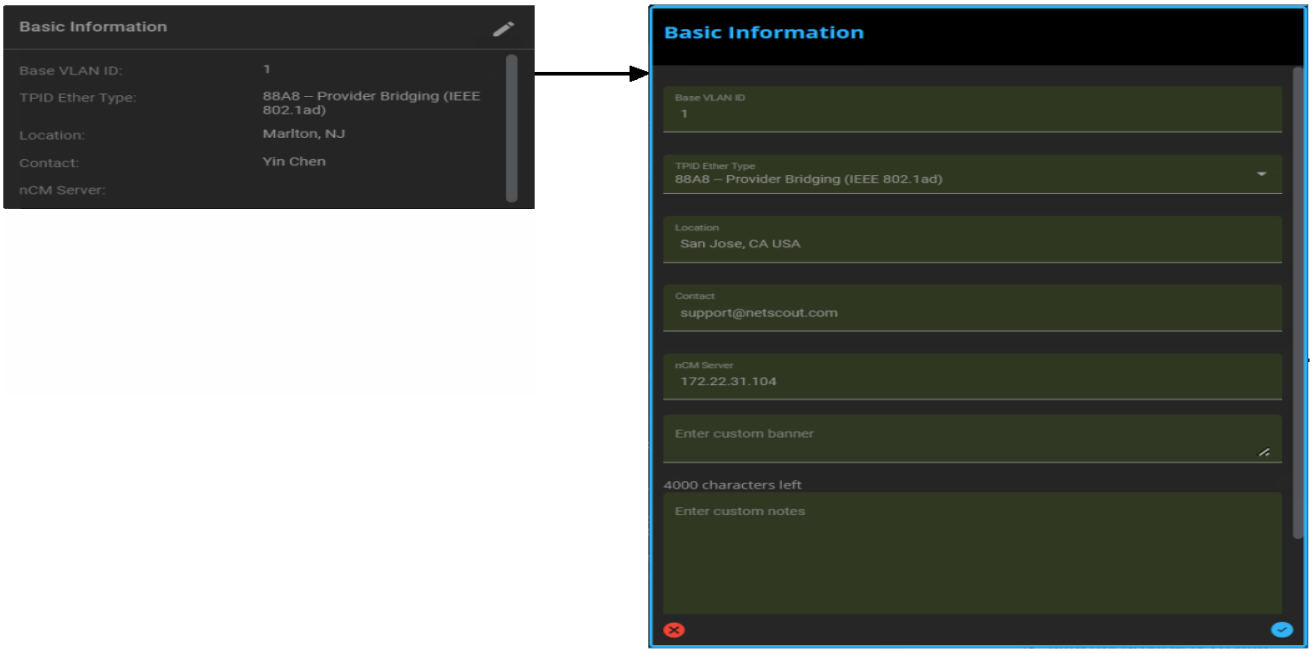


Primary Interfaces		
Name		Name of the device / switch.
DHCP		Enable/Disable DHCP
IPv4 Settings	Address	Devices network IPv4 address (e.g., 192.168.255.11/24)
	Gateway	Devices network gateway address (e.g., 10.250.176.1)
	DNS	DNS server address (e.g., 10.200.96.11)
IPv6 Settings	Address	Device IPv6 address (e.g., fc00:0:3:1ad3::23:a/64)
	Gateway	Device network gateway address (e.g., fc00:0:3:1ad3::23:a/64)
	DNS	DNS server address (e.g., fc00:0:3:1ad3::23:b/64)

Profile > Default > Basic Information

Click the edit icon to make any changes to the basic switch information settings.

Click on the blue circled check mark to save the changes or click the red **X** to cancel the changes.

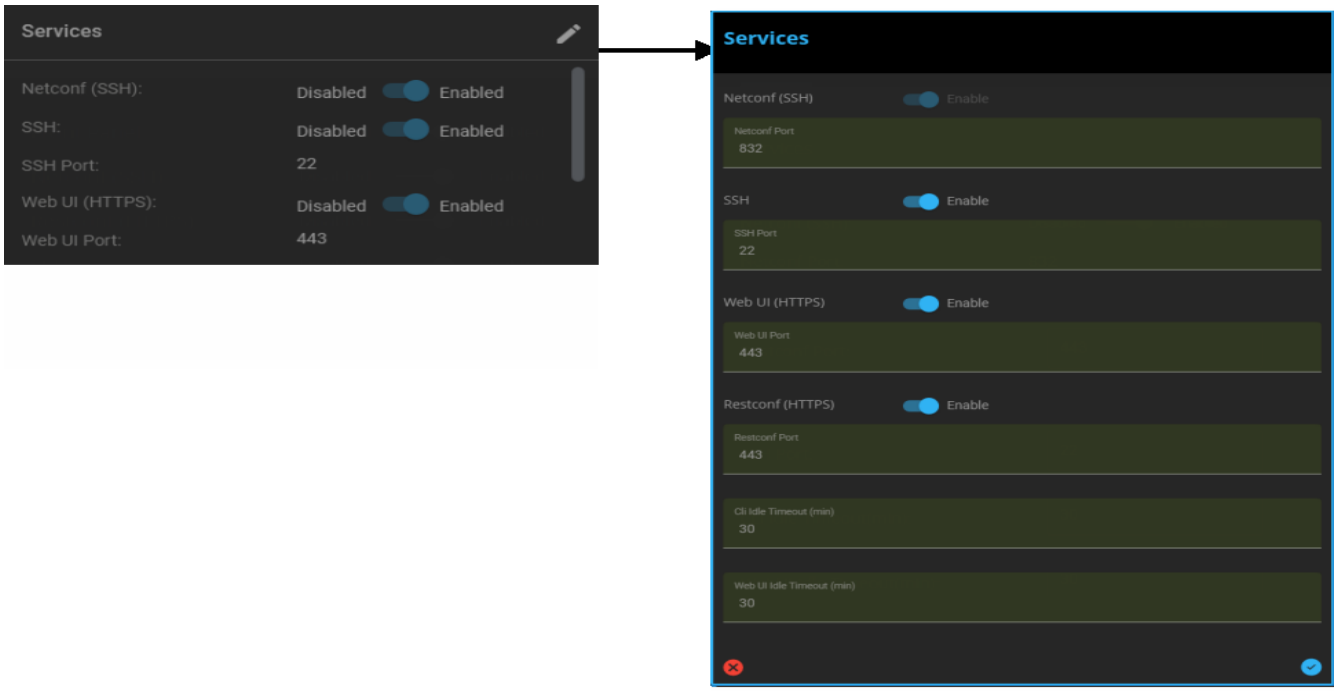


Basic		
Parameters	Base VLAN ID	The first VLAN ID used when numbering VLANs on the system.
	TPID Ether Type	Select the TPID Ether Type: • 0x88A8 - Provider Bridging (IEEE 802.1ad) • 0x8100 - VLAN-tagged frame (IEEE 802.1Q) • 0x9100 - Q-in-Q
	Location	Physical location of device.
	Contact	Contact information.
	nCM Server	nGeniusOne server where this switch is reporting ASI data
	Custom Banner	Add a banner message on the switch.
	Custom Notes	Add detailed notes for a switch.

Profile > Default > Service Profile

Click the edit icon to make any changes to the service profile settings.

Click on the blue circled check mark to save the changes or click the red **X** to cancel the changes.

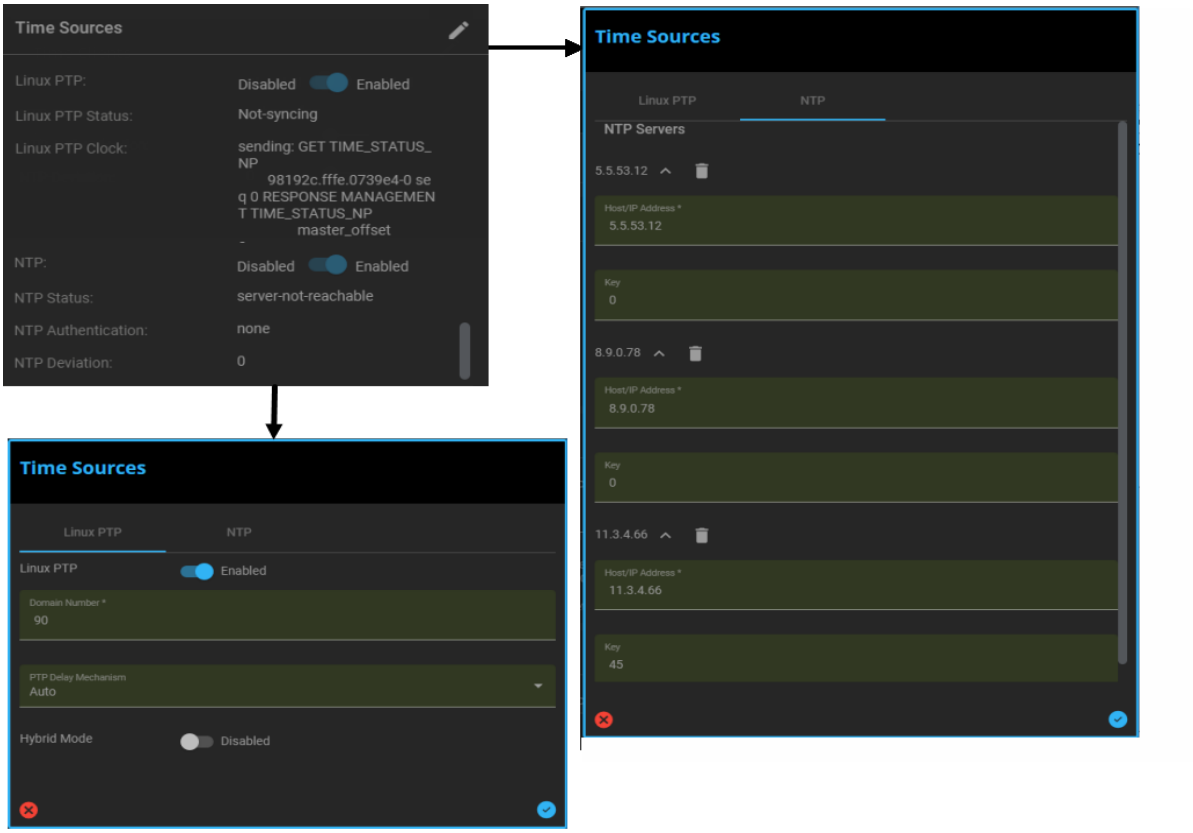


Service	
Netconf (SSH)	Disabled (Do not change this parameter).
Netconf Port	Default port = 832 for Netconf over SSH. Do not change this parameter.
SSH	Enable or Disable SSH access.
SSH Port	Enter port number (default = 22) for SSH access.
Web UI (HTTPS)	Enable or Disable Web UI(HTTPS).
Web UI Port	Port number for Web UI over HTTPS.
Restconf (HTTPS)	Enable or Disable Restconf (HTTPS).
Restconf Port	Port number for Restconf over HTTPS.
CLI Idle Timeout (min)	Enter the amount of time for the PFS CLI to timeout.
WebUI Idle Timeout (min)	Enter the amount of time for the PFS WebUI to timeout.

Profile > Default > Time Sources

Click the edit icon to make any changes to the time sources settings for Network Time Protocol (NTP), Global Positioning System (GPS), and Precision Time Protocol (PTP).

Click on the blue circled check mark to save the changes or click the red **X** to cancel the changes.

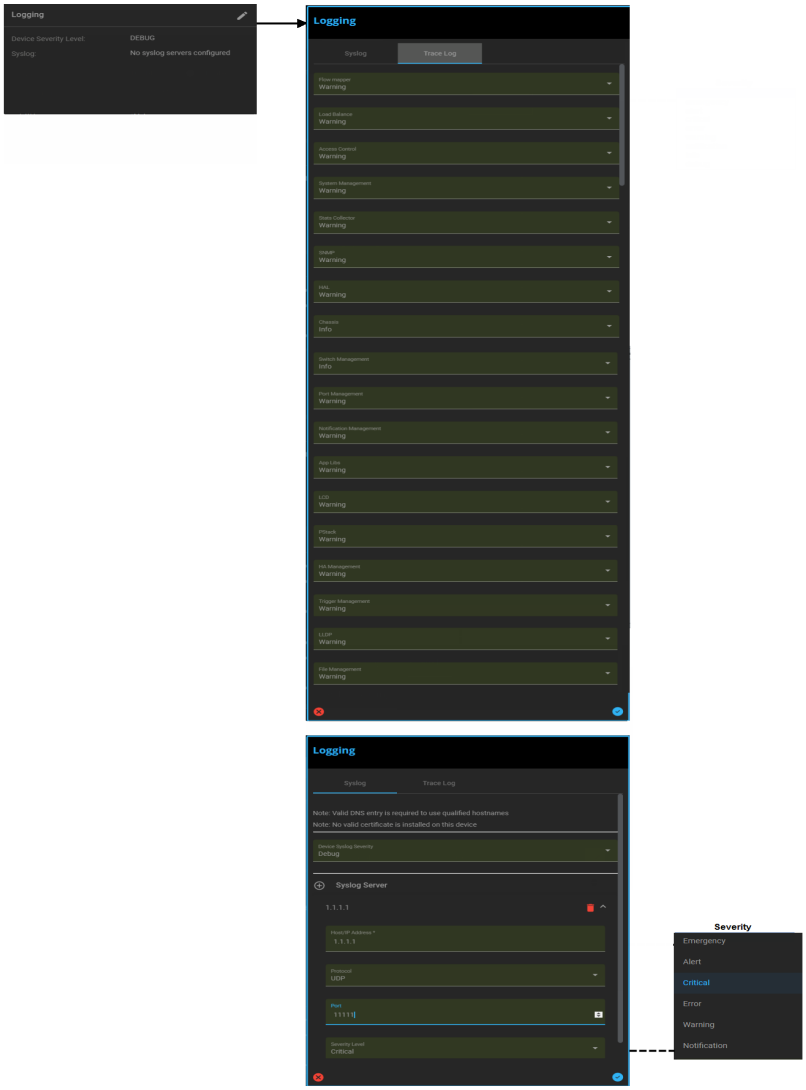


Time Clients		
NTP	NTP Server 1 / 2 / 3	Select up to three NTP server IP addresses. Note: Entering and saving an address for NTP Server 1, Server 2, and/or Server 3 sets NTP to Enabled mode.
Linux PTP		• Linux PTP - Enable/Disable • Domain Number - numerical value • PTP Delay Mechanism – Auto – E2E – P2P – None • Hybrid Mode - Disable

Profile > Default > Logging

Click the edit icon to make any changes to the settings for Trace Logging and Syslog.

Click on the blue circled check mark to save the changes or click the red **X** to cancel the changes.

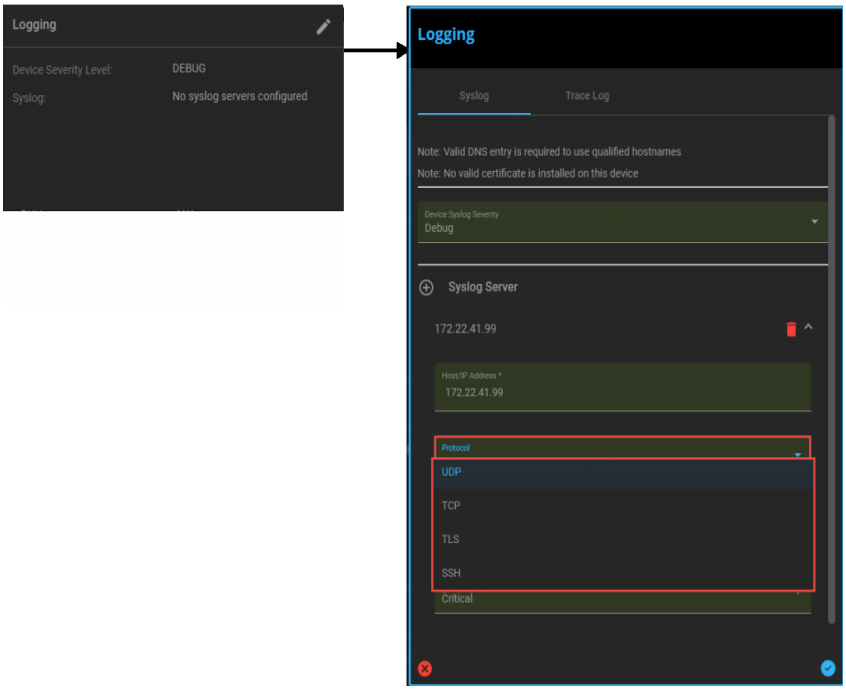


Logging		
Trace Log	Facility / Severity	This section allows defining the current severity level of the trace logs for specific pre-defined functional areas (facilities). You can change the severity level of a facility, but you cannot delete a facility. To change the severity level of a facility, select the Facility name, then select the new Severity level (Emergency, Alert, Critical, Error, Warning, Notification, Info, or Debug).
Syslog	Server 1 /Server 2/Server 3	Enter the server IP addresses. Note: Entering and saving an address for one or more servers sets Syslog to Enabled mode.

Profile > Default > Logging (Secure Syslog)

Click the edit icon to make any changes to the settings for Trace Logging and Syslog.

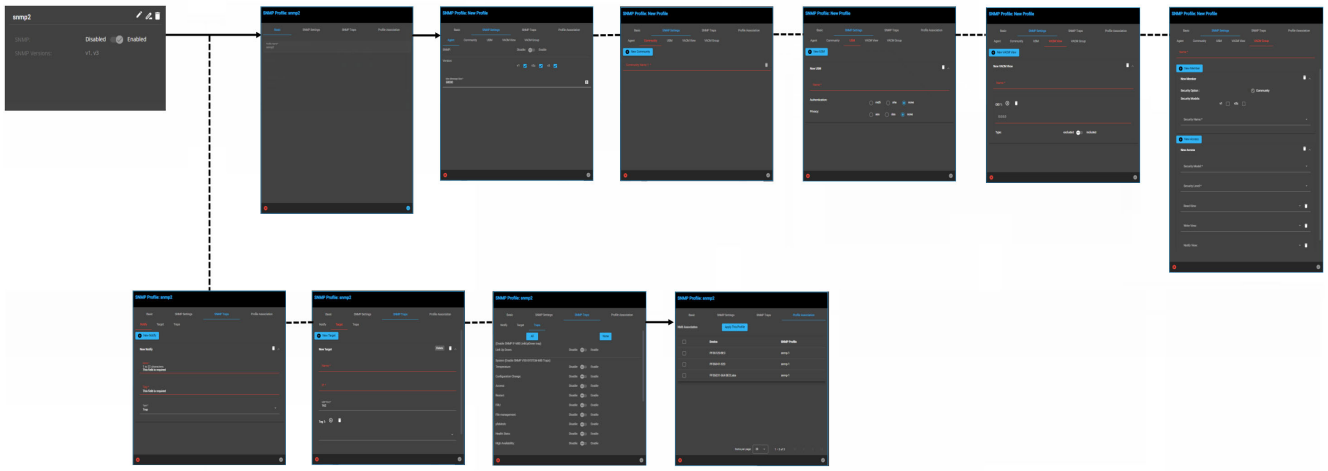
Click on the blue circled check mark to save the changes or click the red **X** to cancel the changes.



Profile > Default > SNMP Feature

Click the edit icon to make any changes to the settings for SNMP, VACM, USM, and Target.

Click on the blue circled check mark to save the changes or click the red **X** to cancel the changes.

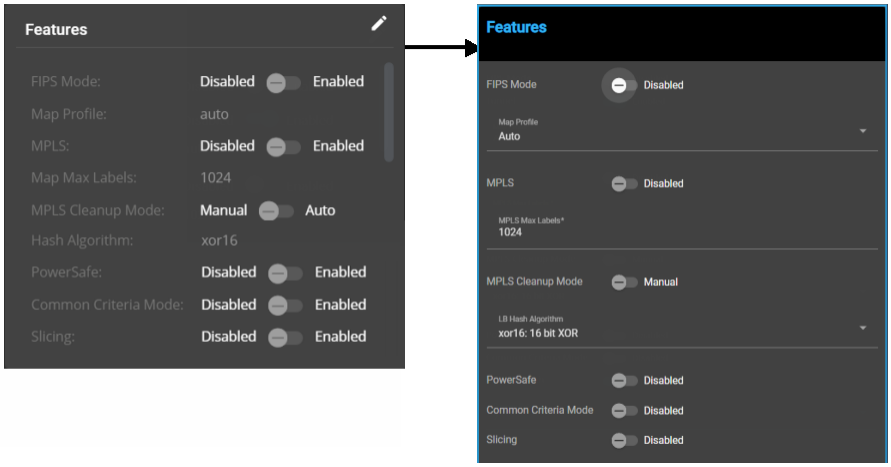


SNMP		
Basic		
	Profile Name	Enter the SNMP profile name.
SNMP Settings		
Agent	Enable / Disable	Enable or Disable this feature.
	Version	Select which versions (v1, v2c, and/or v3) of SNMP to use - one or more versions can be selected.
	Maximum Message Size	Enter the maximum message size (default = 50,000).
Community	Community String: User id or password that allows access to a router's or other device's statistics. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device simply discards the request and does not respond. Note: SNMP Community strings are used only by devices which support SNMP v1 and v2c protocols.	
USM	User-based Security Model: Add users and set authentication and privacy settings in the User-based Security Model.	
VACM	From VACM Settings, enter the following: • View-based Access Control Model groups and MIB views. • Member of the VACM group and define access rights for groups. • Subtree for each view.	
	Group	Add and edit members of the VACM group and define access rights.
	View	Add and edit new subtree views.
SNMP Traps		
Notify	Specify which SNMP target addresses will receive notifications.	
Target	Specify the SNMP target addresses and security model(s) to use.	
Traps	Specify which SNMP traps will be enabled.	
Profile Association		
NMS Association	Select and apply an SNMP profile to a device.	

Profile > Default > Features

Click the edit icon to make any changes to the features settings.

Click on the blue circled check mark to save the changes or click the red **X** to cancel the changes.



Note: FIPS Mode and Common Criteria Mode are not supported in the 6000-series servers and these options do not appear in the **Features** display window.

Features	
FIPS Mode	Enable or disable FIPS mode
Tunnel	Enable or Disable tunneling
LB Hash Algorithm (PFS 5000/ 7000 series only)	Configure the LB Hash Algorithm
Map Profile	Configure the Map profile
MPLS Max Labels	Configure the MPLS maximum number of labels
MPLS Cleanup Mode	Configure the MPLS Cleanup mode for Manual or Auto
MPLS	Enable or disable MPLS mode
Powersafe	Enable or disable Powersafe mode
Common Criteria Mode	Enable or disable Common Criteria mode
Custom Hash	Enable or disable Custom Hash mode
Custom Bytes	Configure the number of custom hash bytes reserved in memory
Slicing	Enable or disable Slicing mode

- FIPS Mode: When operating in FIPS mode, PFS Fabric Manager uses only cryptographic algorithms that comply with the Federal Information Processing Standard.
- LB Hash Algorithm: Allows the user to view and configure a load balancing harsh algorithm for PFS 5000/7000 series.
- MAP Profile: Configure the MAP profile to use the Sip, Dip, Sip IPv6, Dip IPv6 or Legacy mode.
- MPLS Max Labels: This feature enables you to control the number of MPLS labels that PFS Fabric Manager automatically defines for MPLS Standard Stripping.
- MPLS Cleanup Mode: Configure the clean-up method used to clear auto-defined MPLS labels when the maximum limit is reached.
- MPLS: To enable or disable the MPLS feature.

- Powersafe: To enable or disable the feature, either select or deselect the Powersafe checkbox. This feature requires a PowerSafe device.
- Common Criteria Mode: To enable or disable the Common Criteria mode.
- Custom Hash Mode: To enable or disable the Custom Hash mode for load balancing of PFS 5000/ 7000 series devices.

> **Note:** Custom Hash Mode does not support the following servers: 5031-32X, 5031-56X, 6002 and 6010. The option does not appear in the **Features** display window.
>
> Custom hash and UDF filters share the same Custom offset bytes.
>
> The Custom Hash functionality enables users to configure up to four bytes of packet data (configurable using Load Balance Criteria) to be used in a custom hashing mechanism for traffic distribution.

- Custom Bytes: Configure the number of custom hash bytes reserved in memory. Options are 2 or 4 (default = 2).

> **Note:** This parameter is only applicable when the Custom Hash is enabled on the switch.

- Slicing: To enable or disable the Slicing mode.

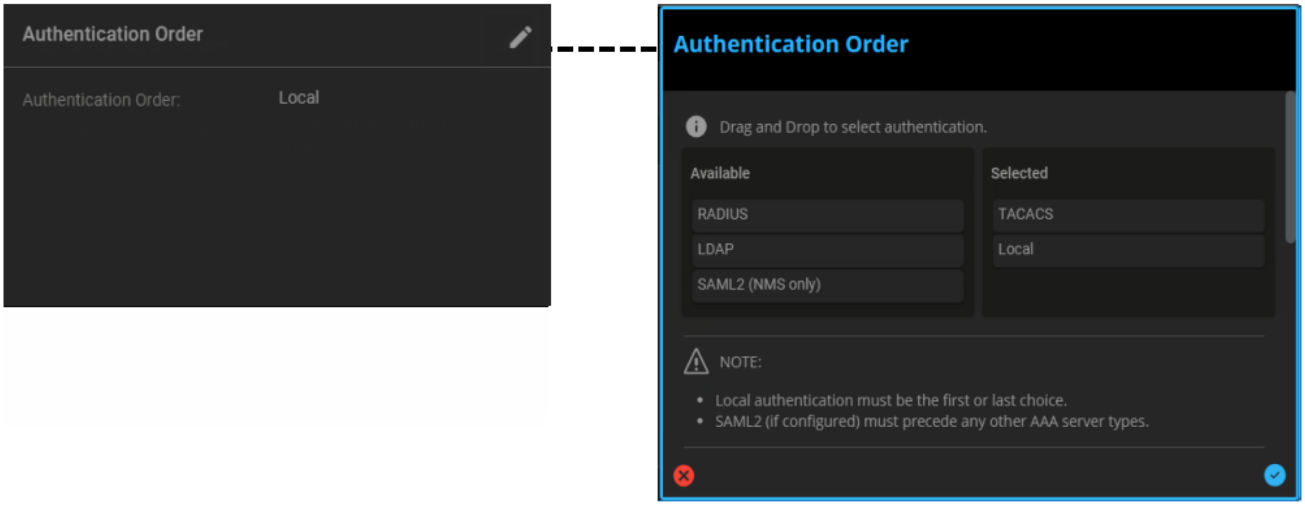
Profile > Default > Authentication Order

Clicking the Edit icon on Authentication Order allows modifying settings made under the Settings > Authentication Order (refer to Managed Devices on page 7-61) for a managed switch.

Select / unselect the authentication types and the order in which they are used.

> **Important:** Local authentication must always be either a first or last choice. Local cannot be in the middle.

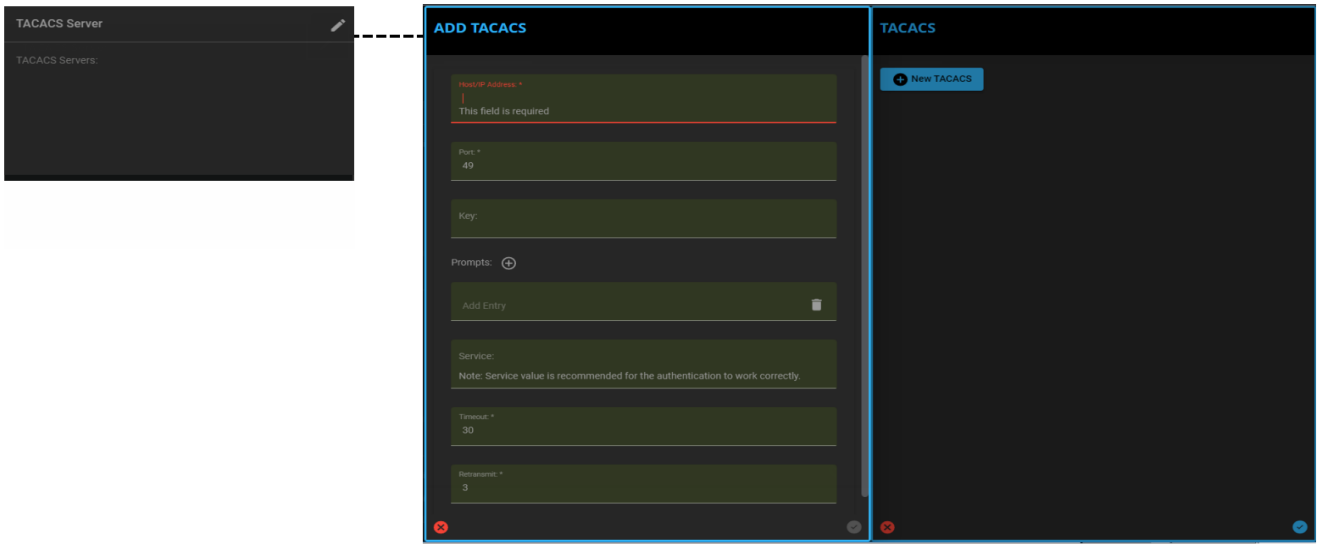
Click on the blue circled check mark to save the changes or click the red **X** to cancel the changes.



Profile > Default > TACACS Server

Clicking the Edit icon on TACACS Server allows modifying settings made under the Settings > TACACS Server (refer to Configuring TACACS on page 7-52) for a switch.

To add a new TACACS server click on the **+ New TACACS** link to open an Add TACACS screen. Specify the following settings based on the configuration of your TACACS server, then click on **Apply** to save the new server settings.

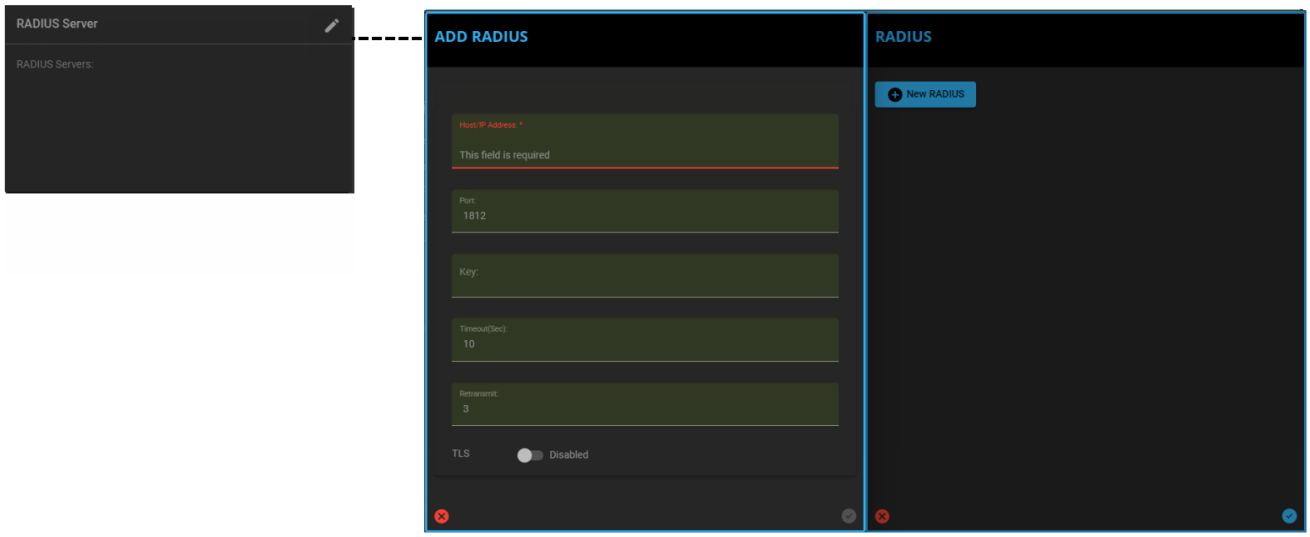


Settings	
Host / IP Address	IPv4/IPv6 address or a fully qualified domain name of the TACACS server.
Port	Port for access to the server (default 49).
Key	AES encrypted string to authenticate to the server.
Prompts	TACACS prompts parameter.
Service	TACACS service parameter. Note: Service value is recommended for the authentication to work correctly.
Timeout	Time after which requests to the server time out (default 30 seconds).
Retransmit	Number of times PFOS attempts to contact the TACACS server (default 3).

Profile > Default > RADIUS Server

Clicking the Edit icon on RADIUS Server allows modifying settings made under the Settings > RADIUS Server (refer to Configuring RADIUS on page 7-54) for a switch.

To add a new RADIUS server click on the **+ New RADIUS** link to open an Add RADIUS screen. Specify the following settings based on the configuration of your RADIUS server, then click on **Apply** to save the new server settings.

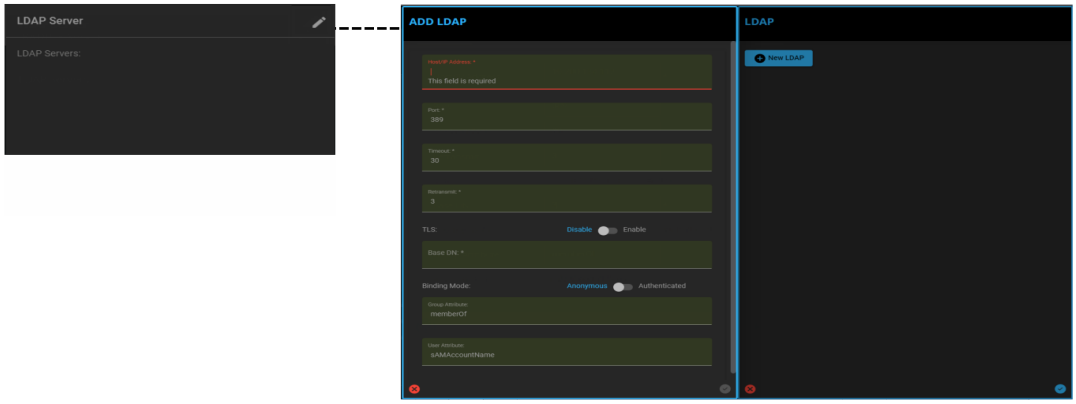


Settings	
Host / IP Address	IPv4/IPv6 address or a fully qualified domain name of the RADIUS server.
Port	Port for access to the server (default 0).
Key	AES encrypted string to authenticate to the server.
Timeout	Time after which requests to the server time out (default 30 seconds).
Retransmit	Number of times PFOS attempts to contact the RADIUS server (default 3).
TLS	Enable/Disable TLS. If TLS is enabled for Radius, the switches require the Radius Certificate to be available and uploaded via Certificate management or directly at PFOS webUI.

Profile > Default > LDAP Server

Clicking the Edit icon on LDAP Server allows modifying settings made under the Settings > LDAP Server (refer to Configuring LDAP on page 7-55) for a switch.

To add a new LDAP server click on the **+ New LDAP** link to open an Add LDAP screen. Specify the following settings based on the configuration of your LDAP server, then click on **Apply** to save the new server settings.



Settings	
Host / IP Address	IPv4/IPv6 address or a fully qualified domain name of the RADIUS server.
Port	Port for access to the server (default 389 for non_TLS/636 for TLS).
Timeout(Sec)	Time after which requests to the server time out (default 30 seconds).
Retransmit	Number of times PFOS attempts to contact the TACACS server (default 3).
TLS	Disable/Enabale TLS mode (When TLS is enabled, you can choose to validate against CA. To enable validation, enable authorize certificate.)
Base DN	Enter the distinguished name (DN) to search tokens on groups associated with that DN.
Binding Mode	Select Anonymous or Authenticated for LDAP binding. By default, binding mode is anonymous. If you enable authenticated mode, then the PFS-FM prompts you enter username and password for LDAP Binding. If binding mode is set to Authenticated, then Binding DN and Password are required. This is used when LDAP/AD mode requires a lookup user before query logged in user.
Group Attribute	Defines the group the user is a member of (typically set in LDAP AD as memberOf) and maps to one of the roles defined in the NMS (if no role mapping is found the user is denied access).
User Attribute	Defines the lookup for the user when querying the server, for example: sAMAccountName or userPrincipalName. When logging in, the user is validated by using this lookup on the LDAP/AD server.

Upon configuring the above parameters, you can choose to apply the configuration to the NMS only or to the NMS and its managed devices. When managed devices are selected, the PFS-FM publishes the LDAP server configuration to the selected devices.

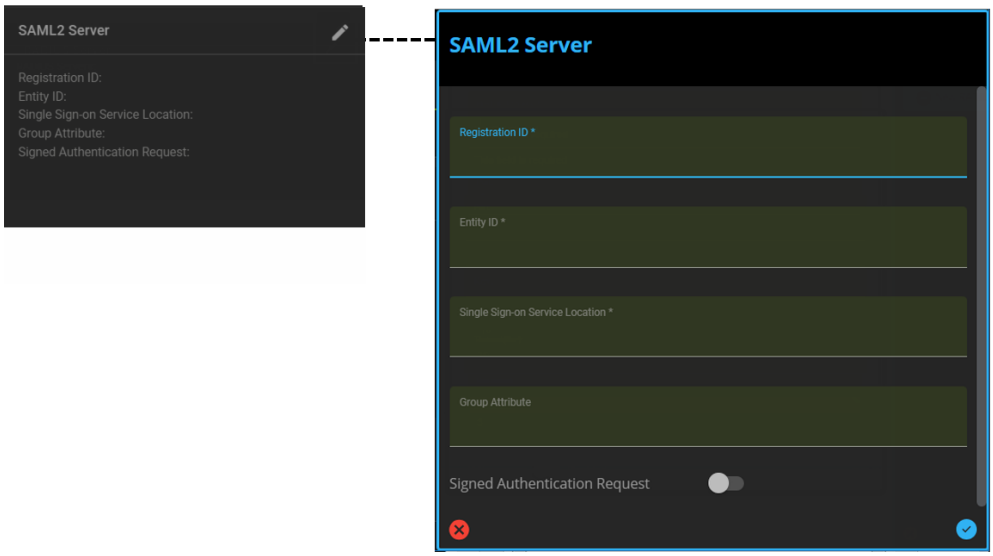
A maximum of three TACACS, RADIUS or LDAP Server instances can be configured and the order in which these instances are created is maintained for validation. The PFS-FM will authenticate against whichever instance is reached first.

Note: If the server is reachable but the user is not authenticated, then there are no retries to the next server in the sequence.

Profile > Default > SAML2 Server

Clicking the Edit icon on SAML2 Server allows modifying settings made under the Settings > SAML2 Server (refer to Configuring SAML2 (NMS only) on page 7-56) for a switch.

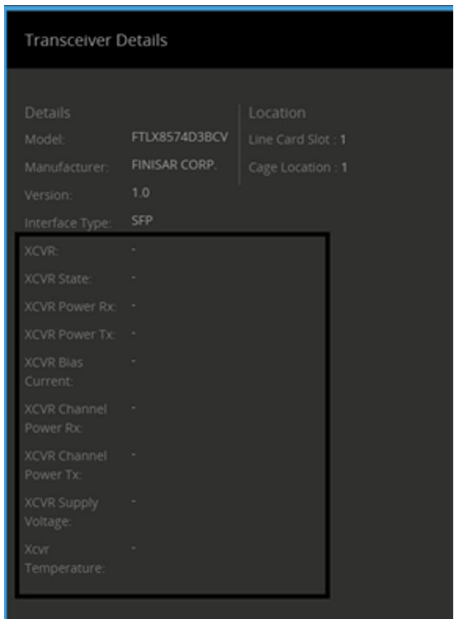
To add a new SAML2 server, specify the following settings based on the configuration of your SAML2 server, then click on **Apply** to save the new server settings.



Settings	
Registration ID	Unique RegistrationID assigned by your Identity Provider for your PFS-FM (as a Service Provider/App)
Entity ID	EntityID assigned by your Identity Provider
Single Sign-on Service Location	SSO Endpoint for the Identity Provider
Group Attribute	Attribute maps to Role Mapping in Identity Provider (for example: the memberOf attribute maps to Group Names in Identity Provider)
Signed Authentication Request	Enable/Disable (always set to Disable)

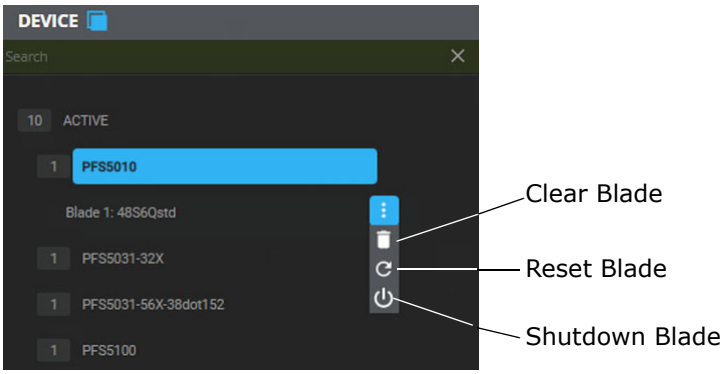
Transceiver Details

Display the transceiver details on the Configure tab > Device perspective > Hardware > Port > Information.



Blade/Line Card Control

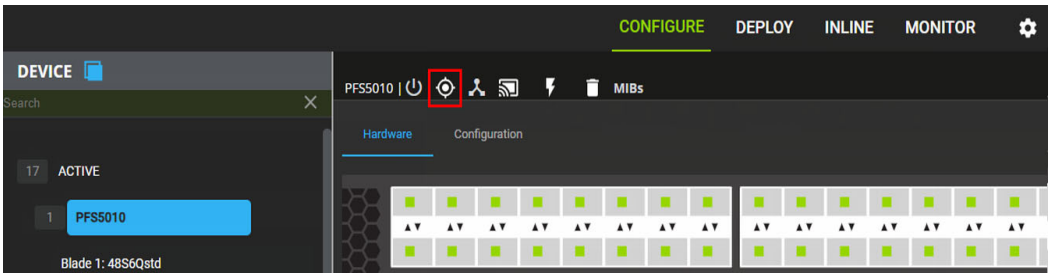
Allows the user to clear, reset, or shutdown a blade/line card.



Note: This can also be performed from the Port perspective, at the slot level.

Locate Me

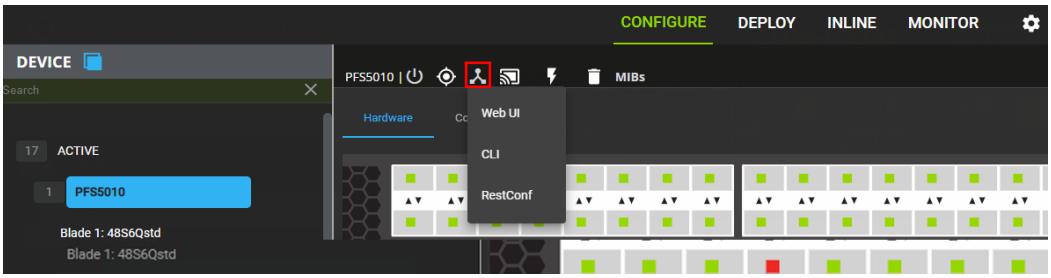
Identifies the selected switch by clicking on the Locate Me icon. The respective switch will blink it's lights continuously for 2 minutes then turn off. A "System Locator Activated for <Switch Name>" will be displayed in a message prompt.



Connect to the Device

You can connect to either the PFOS Web UI, CLI or RestConf via the Connect To menu.

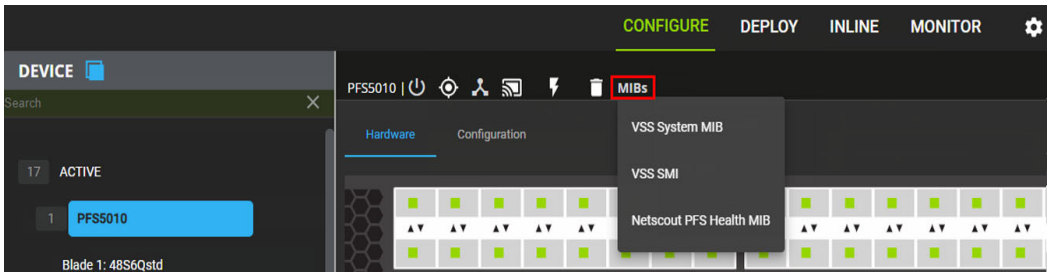
Note: You must disable popup blockers before launching a CLI session.

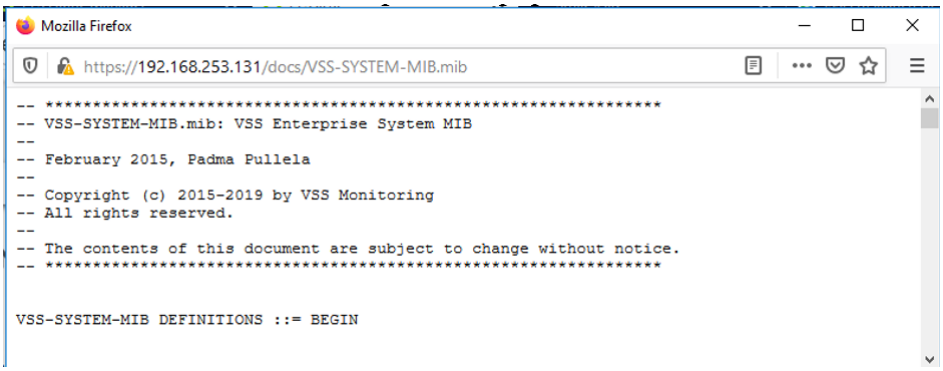


MIB File Viewing

View MIB files by clicking on the MIBs icon. Select the desired MIB from the options displayed and the MIB will be displayed in a popup window.

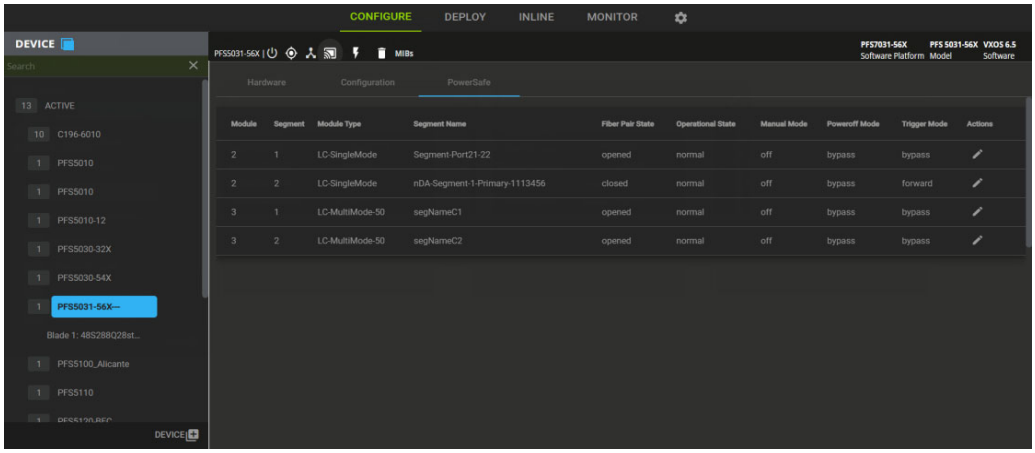
Note: You must disable popup blockers before viewing MIB files.





External PowerSafe TAPs Configuration

After the PowerSafe option has been enabled (see Profile > Default > Features) you can now view and configure the PowerSafe modules. From Perspective > Device > PowerSafe Module, select a module to configure and click on the Edit icon.

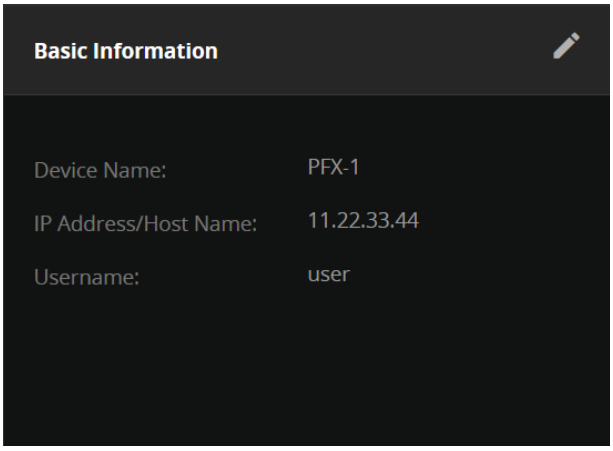


A Configuration window is displayed.

Settings	
Module Type	Enter the module type
Manual Mode	Select from Off, Bypass, Forward, Block, or InPairDown
Bypass Mode	Select from Bypass, Forward, Block, or InPairDown
Inline Network Ports	
Port 1	Select the desired port from the device
Port 2	Select the desired port from the device
Trigger Override	
Trigger Mode	Select from Disable, Bypass, or Forward
Trigger Name	Select the trigger name
Trigger State	Active/Inactive

PFX > Basic Information

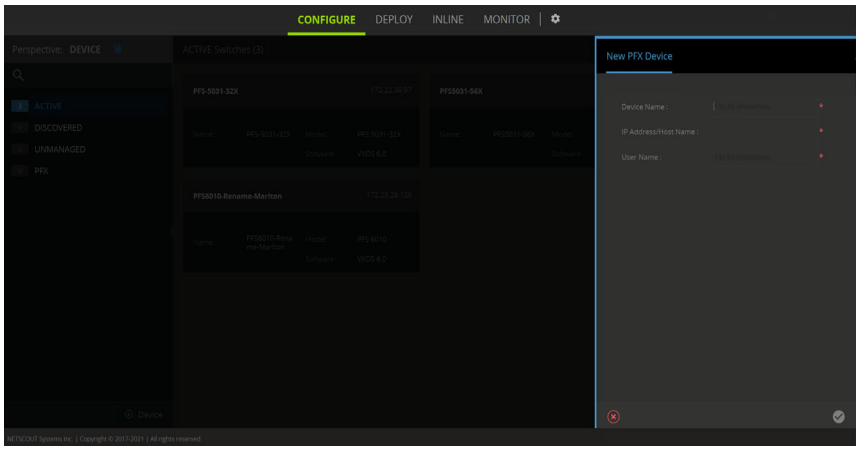
Display the PFX details on the Configure tab > Device perspective > PFX > Basic Information.



Settings	
Device Name	Name of the PFX device
IP Address/Host Name	IPv4/IPv6 address or a fully qualified domain name of the PFX device
User Name	User name for CLI connectivity

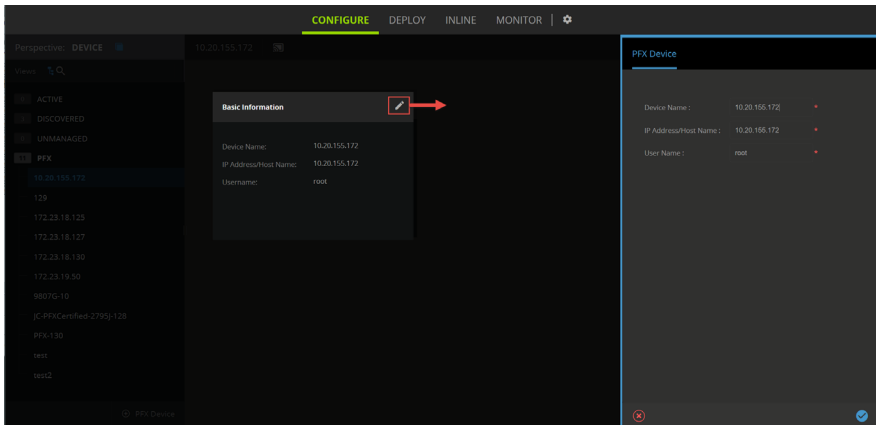
Adding a PFX Device

To add a PFX device, click on the **Add** button located at the bottom of the Perspective > Device pane.



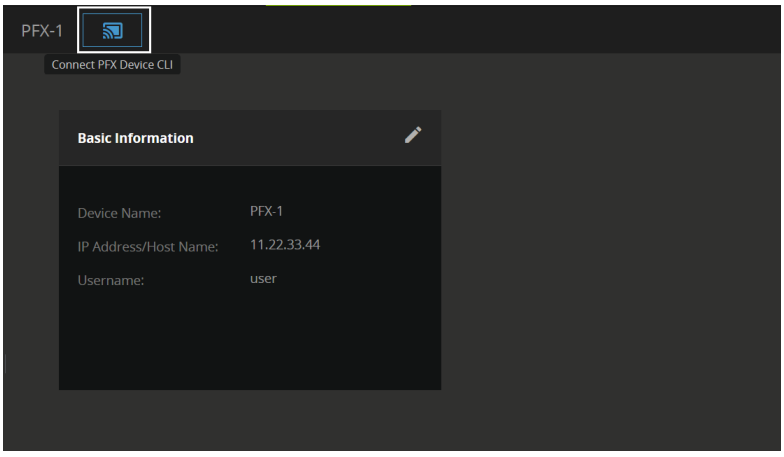
A slide out appears to add a PFX device. After all the PFX information is entered and submitted, a new PFX device is displayed in the perspective tree.

When you attempt to edit an existing/managed PFX device, the same slide out opens but with pre-populated fields.



Click the Connect button to connect to a selected PFX device via CLI.

> **Note:** You must disable popup blockers before starting a CLI session.

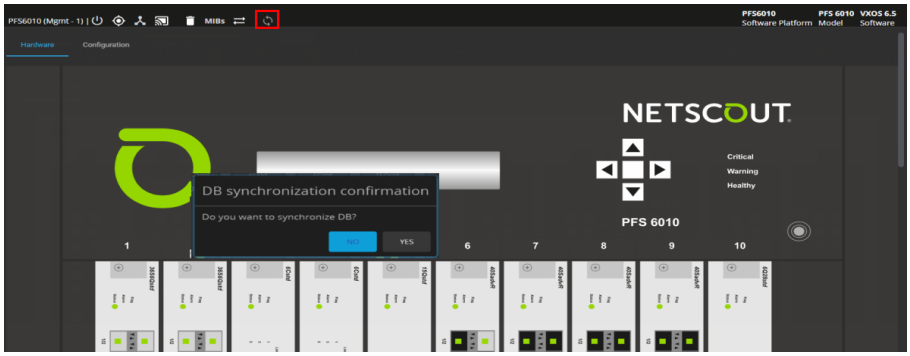


Managing Database Sync (PFS6010 Devices Only)

The user can manage database sync by using the DB Sync button on the Configuration lifecycle main landing page.

- Hovering on the DB Sync button displays a tool tip with text.
- The DB Sync button is enabled when two management cards are available, otherwise it is disabled.

Clicking the **DB Sync** button displays the DB synchronization confirmation dialog. Click **Yes** to start the synchronization.

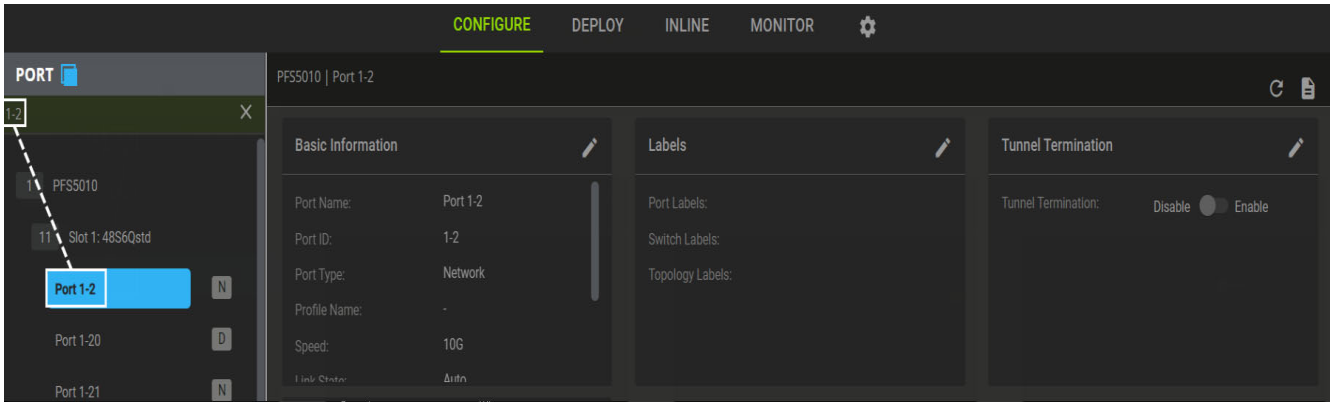


Configure Search Filter

The Configure Lifecycle search filter allows searching for ports, filters, and devices by name. Search results are displayed in tree format under the Perspective menu. Clicking on a found entry directs you to the corresponding page.

Port Perspective

From Configure Lifecycle, enter a port name in the Search text field. Any port containing either the full port designation / name (or a portion of the designation) is listed in the tree view - broken out by switch > blade > port name.

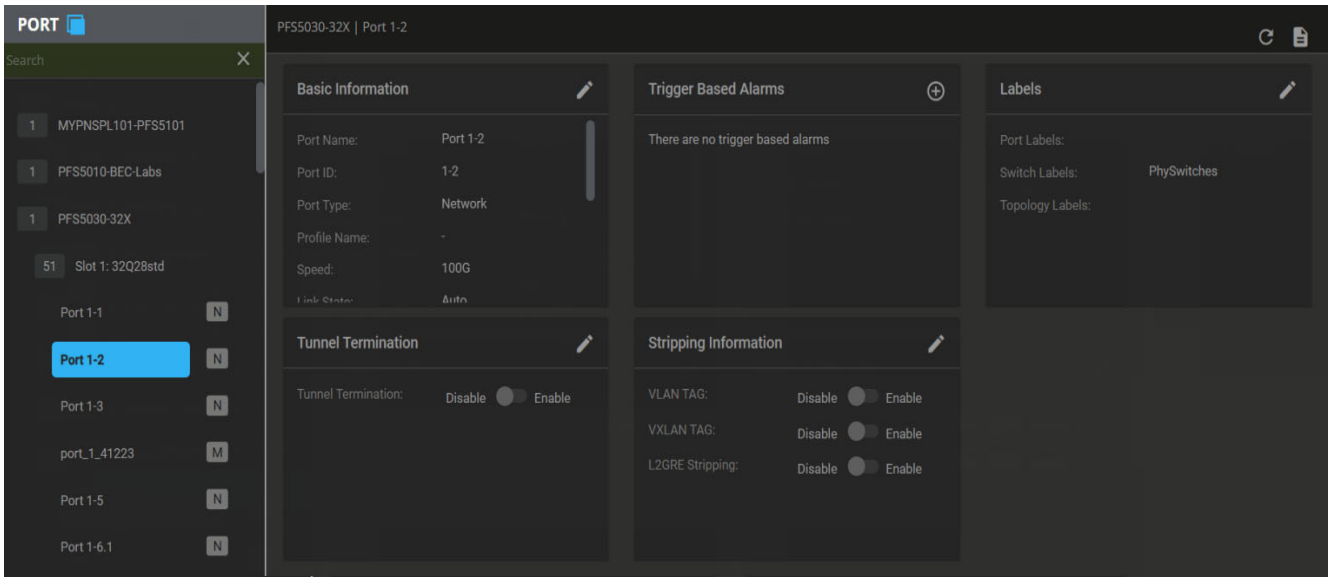


The search filter allows for easy and specific matching by using a textual search which treats multi-token (multi-word) search phrases as a search for something that contains each token, though not necessarily in the order presented by the user.

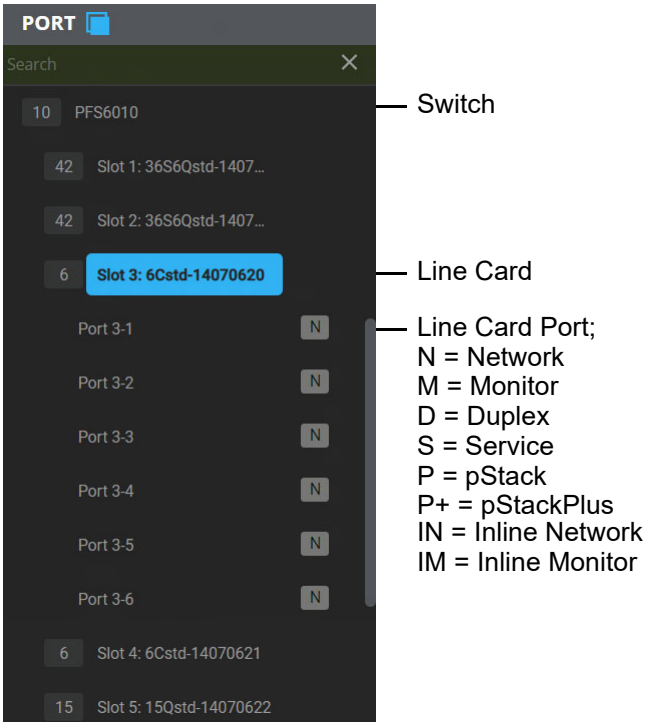
Perspective > Port

Selecting Port from the Perspective menu allows viewing and editing the configuration / features of the ports in each line card installed in the switch including:

- Basic Information
- Trigger Based Alarms
- Labels
- Tunnel Termination Port Feature Profile
- VLAN Tag Stripping Port Feature Profile
- Deduplication Port Feature Profile
- Monitor_Stamping

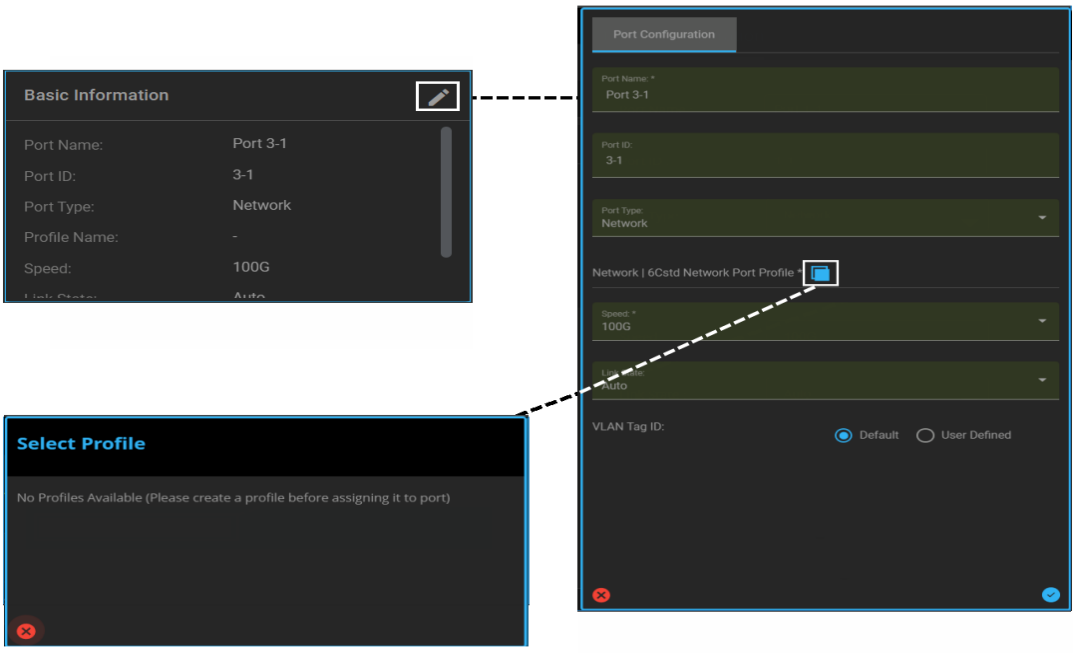


To display ports on a particular line card, select Port > Switch Type. The installed line cards in the switch are displayed. Clicking on a line card expands the port listing for that card. Select a port to view / edit the current configuration settings.



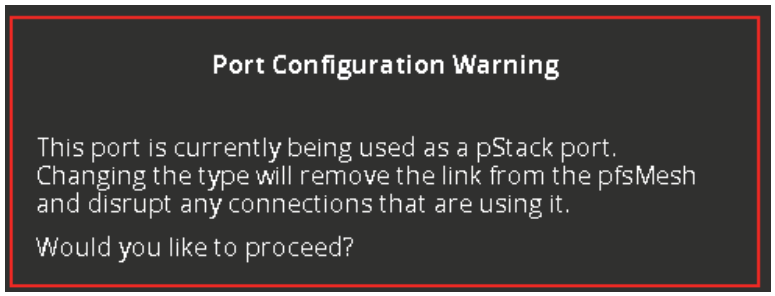
Basic Information

Click the edit icon to make any changes to the selected port's settings. Click on the blue circled check mark to save the changes or click the red **X** to cancel the changes.



Basic Information	
Port Name	Use the default name or assign a name for the port to help identify the devices or network segments connected to the unit.
Port ID	Use the default ID or assign an ID for the port to help identify the devices or network segments connected to the unit.
Port Type (refer to Port Types on page 3-35)	Specify the port type: • Network • Monitor • Service • Duplex • pStack • pStackPlus • Inline Network • Inline Monitor
Network | Port Profile	(Optional) Select a port profile name.
Speed	Select the transceiver port speed, if the inserted transceiver supports more than one speed.
Link State	Select the link state for the port: • Auto – Normal operation • Force Down – Force the link down • Force Up – Force the link up
VLAN Tagging	Enable / Disable VLAN Tagging in this port. Note: VLAN ID setting is ignored on pStack ports.
VLAN ID	Use the default VLAN ID (if VLAN Tagging is set to Enable), or to specify the starting VLAN ID, select User Defined and enter a starting VLAN ID.
LLDP TX	Enable/Disable LLDP TX in this port.
LLDP RX	Enable/Disable LLDP RX in this port.

Note: Changing a port currently configured as a pStack port to another port type warns the user:



Port Types

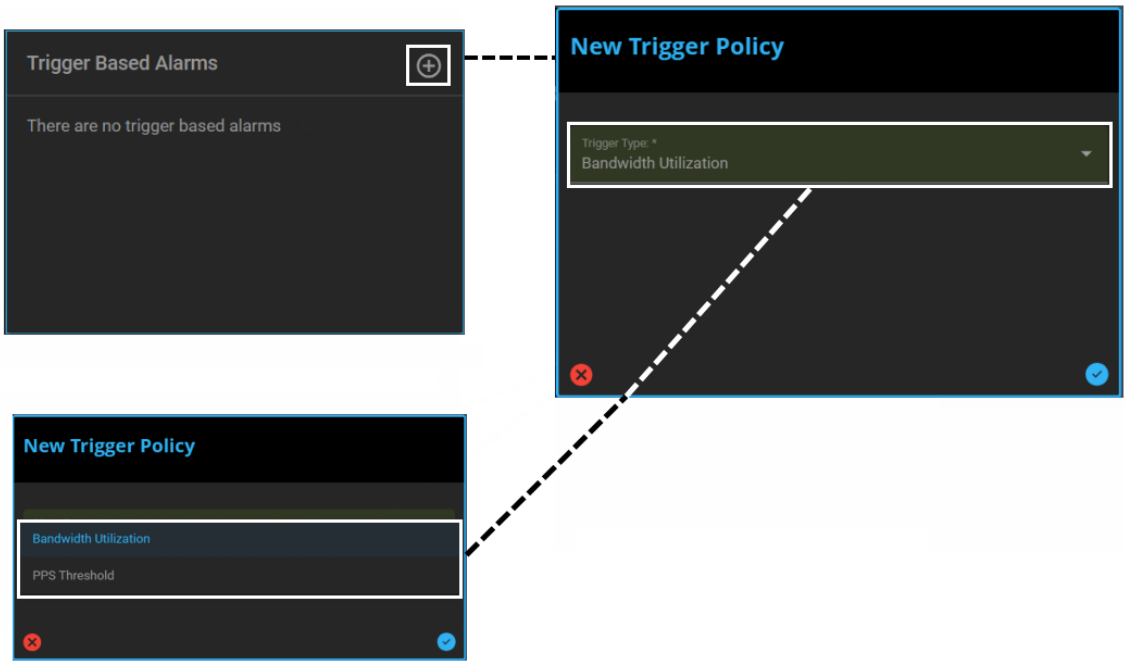
The following port types are supported on PFS Fabric Manager:

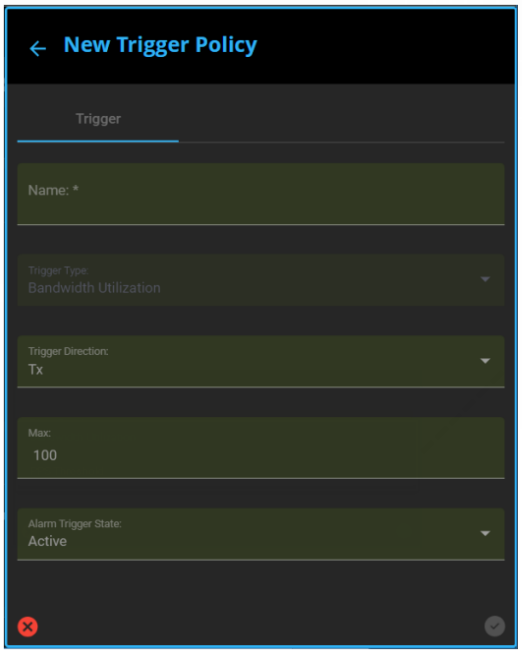
- Network (**N**) - A unidirectional class of input port that is used to connect to a single output port, such as a service port or another monitor port.

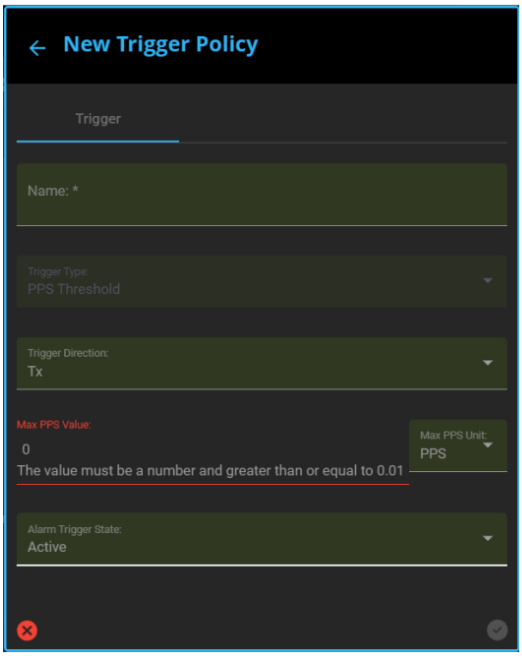
- Monitor (**M**) - A unidirectional output port class that is used to connect to either the Network port on another packet flow switch or network packet broker, or to a single input port on a passive monitoring and/or analysis tool, such as an intrusion detection system.
- Duplex (**D**) - Allows a single fiber port to act as a dual-function port class, where the Rx side acts as a Service port and the Tx side acts as a Monitor port.
- Service (**S**) - A unidirectional class of an internal port that acts as an intermediary resource supporting the base feature set and special functions when the hardware is present, such as packet de-duplication and fragment reassembly.
- pStack (**P**) - A bidirectional class of port that is used to interconnect systems for providing an auto-sensing, self-healing, topologically pfsMesh architecture for traffic capture.
  Broken-out ports can be set as pStack:
  - First configure the port as Breakout Mode = Enable
  - Configure any additional features (i.e., Speed, Link State)
  - Finally, select Port Type = pStack then save the settings.
- pStackPlus (**P+**) - ports for both directly connected ports and for ports connected over IP. If ports are connected over an IP interface, the user specifies the Source IP and Destination IP addresses while configuring port class as pStack+. For directly connected ports, PFOS determines the Source and Destination IP on pStack+ ports.
- Inline Network (**IN**) - ports used in pairs and connect inline with a network link. The primary purpose of each port in the pair is to forward network traffic to one or more inline active monitoring or analysis tools via Inline Monitor ports. User-defined VLAN IDs are be disabled for Inline Network ports. Every Inline Network port can be paired with only one other Inline Network port.
- Inline Monitor (**IM**) - ports used in pairs and connect to an inline active monitoring or analysis tool. The primary purpose is to forward traffic from one or more Inline Network ports to the connected inline tool. Because the outer VLAN in the packet is used to determine the A and B ports in a tool chain,every Inline Monitor Port can be paired with only with one other Inline Monitor port. VLAN tagging is disabled on Inline Monitor ports.

Trigger Based Alarms Port Feature Profile

A user can configure a custom alarm for a specific port based on (user created) PFOS triggers. Click the edit icon to make any changes to the settings. Click on the blue circled check mark to save the changes or click the red **X** to cancel the changes.

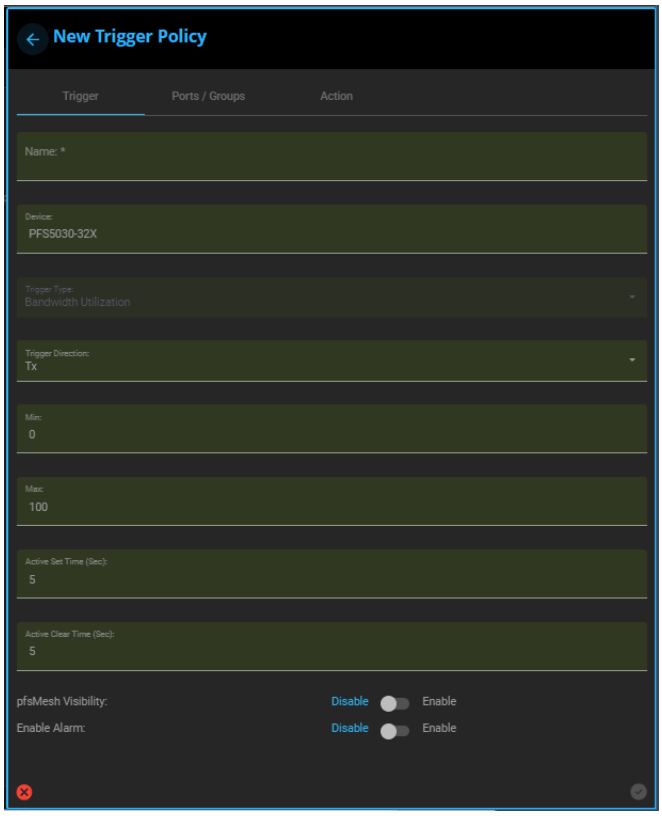


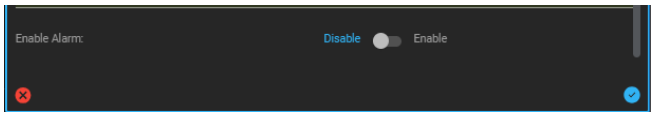




Trigger Based Alarms Port Feature Profile	
Trigger Type	Bandwidth Utilization/PPS Threshold
Bandwidth Utilization	
Name	Name for the Trigger Policy
Trigger Direction	Tx/Rx - Choose the direction to which the trigger applies (only applies to ports that receive and transmit)
Max	Number value
Alarm Trigger State	Active/Inactive
PPS Threshold	
Name	Name for the Trigger Policy
Trigger Direction	Tx/Rx - Choose the direction to which the trigger applies (only applies to ports that receive and transmit)
Max PPS Value	Number value greater than or equal to 0.01 (PPS, KPPS,MPPS)
Alarm Trigger State	Active/Inactive

Trigger configuration now has an additional toggle to enable an alarm. After the alarm is enabled, users can select the trigger state for when the alarm should be triggered and the severity for that alarm.



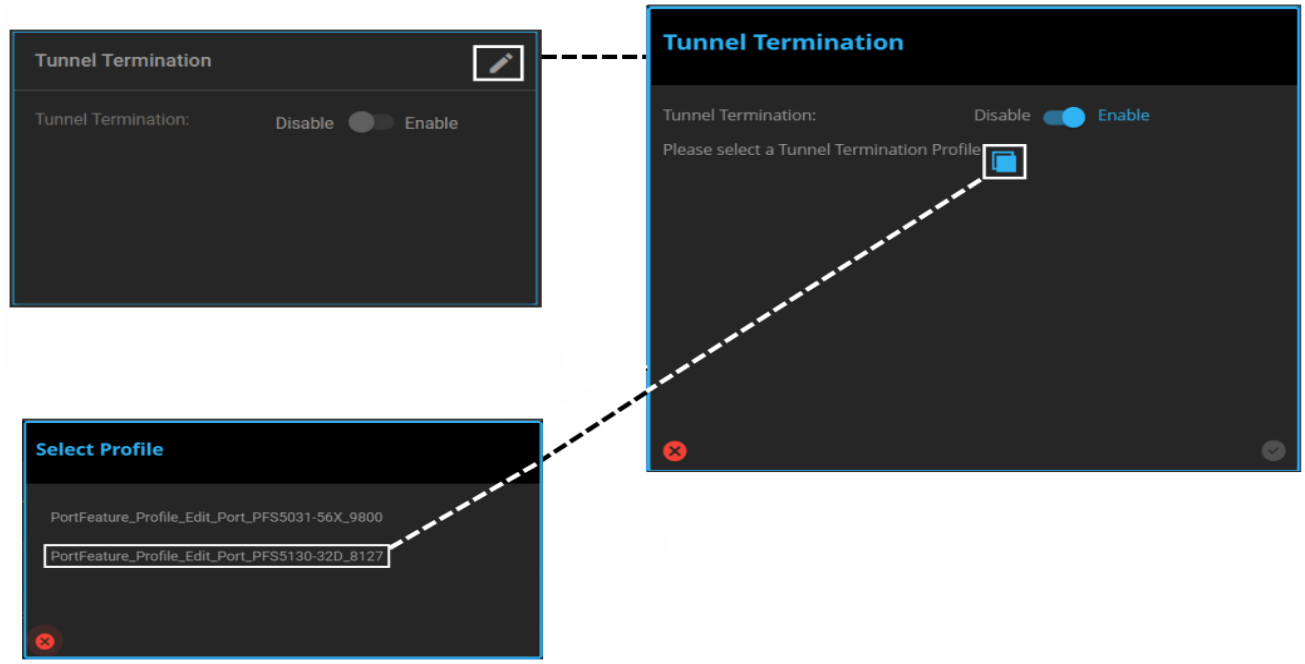


Tunnel Termination Port Feature Profile

The Tunnel Termination Port Feature Profile option is available when a port is designated as either Network or Duplex.

Note: In PFOS 5.5 and later, tunnel termination can be disabled per switch.

Click the edit icon to make any changes to the settings. Click on the blue circled check mark to save the changes or click the red **X** to cancel the changes.



Tunnel Termination Port Feature Profile	
Tunnel Termination	Enable / Disable IP tunnel termination on this port.
Tunnel Termination Port Feature Profile	(Optional) Select a profile name.
IP Address	IPv4/IPv6Address being used as an IP tunnel destination. Multiple addresses can be assigned to the port.

IP Tunnel Termination

IP Tunnel termination allows the PFS to perform encapsulated forwarding of mirrored traffic. This allows, for example, the PFS to act as a remote mirroring destination, using IP tunneling protocols such as encapsulated remote port analyzer (ERSPAN), generic routing encapsulation (GRE), or network virtualization GRE (NVGRE). As a destination endpoint, designated ports on a system running PFS Fabric Manager will receive traffic from one or more remote mirroring source ports. A remote mirroring source port mirrors, encapsulates, and transmits the traffic to a destination port over a local area network. The traffic is typically encapsulated in some form of GRE (using IP as its transport) and is, therefore, routable across a Layer 3 network between the source node and the destination node. Common GRE, NVGRE, and ERSPAN sources include L2/L3 switches or virtual environments.

Acting as an IP endpoint, each defined PFS port responds to ARP and ICMP (ping) messages so that upstream switches and routers can forward the tunneled traffic to the PFS port. You must configure at least one IP address for each port that will act as a tunnel destination.

IP Tunnel termination is available on Span and Span-Monitor class ports on all models of line cards supported by PFS Fabric Manager. However, advanced ports of class Span, Span-Monitor, Service, or Monitor on a 40SadvR line card are required to de-encapsulate tunneled traffic before forwarding the frames to the monitoring tools. Refer to the Protocol De-encapsulation and Stripping section for how to set this up. Conducting the de-encapsulation on a Service or Monitor class port might be desirable, depending on the monitoring tools being used.

To use tunnel termination:

- Enable tunnel termination on the desired port(s), then associate a previously created tunnel termination library, and add an IP address for the enabled feature.

Tunnel Termination Considerations And Limitations

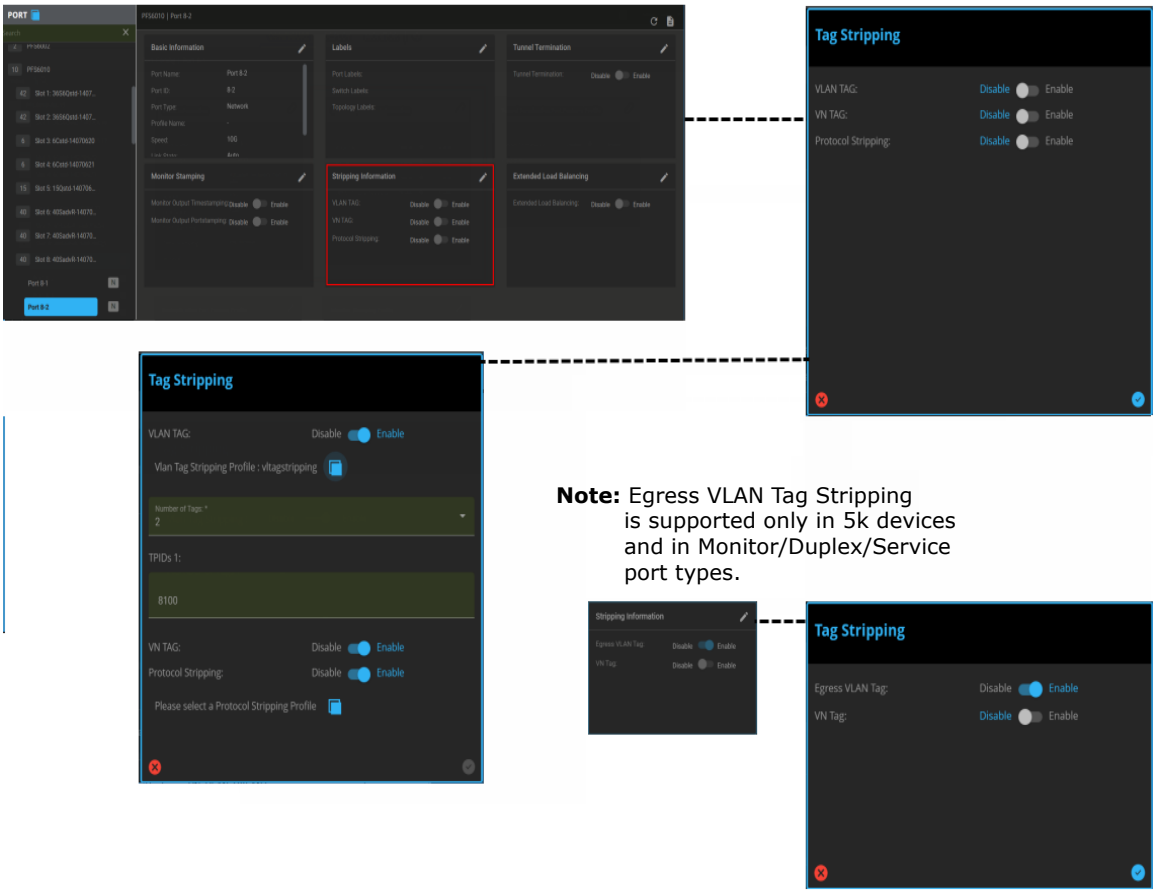
The following considerations apply to the current release of tunnel termination:

- After an IP address has been added to a tunnel termination library, any ARP request packet with that IP address as the target will be consumed by the packet flow switch running PFS Fabric Manager. These packets will not be forwarded, but will be analyzed and counted as ARP packets on that port displayed under Control Packets Statistics. Such ARP requests will be responded to.
- After an IP address has been added to a tunnel termination library, any ICMP packet with that destination MAC address and that destination IP address will be consumed by the packet flow switch running PFS Fabric Manager. Those packets will not be forwarded, but will be analyzed and counted as ICMP packets on that port displayed under Control Packets Statistics. Such ICMP requests will be responded to.
- Each tunnel termination library supports a maximum of 16 IP addresses.
- Tunnel termination is rate-limited to 20 control (ARP, ICMP) packets per second on all channels. Extra packets are dropped and are counted as dropped packets on that port displayed under Control Packets Statistics.
- The tunnel termination destination does not respond to fragmented control (ARP, ICMP) packets.
- Jumbo control packets (larger than 8,500 bytes) are not supported.

VN, VLAN, VXLAN, MPLS Tag Stripping Port Feature Profile

VN, VLAN, VXLAN, MPLS Tag Stripping Port Feature Profile (UI for 5000/7000 Series Platforms)

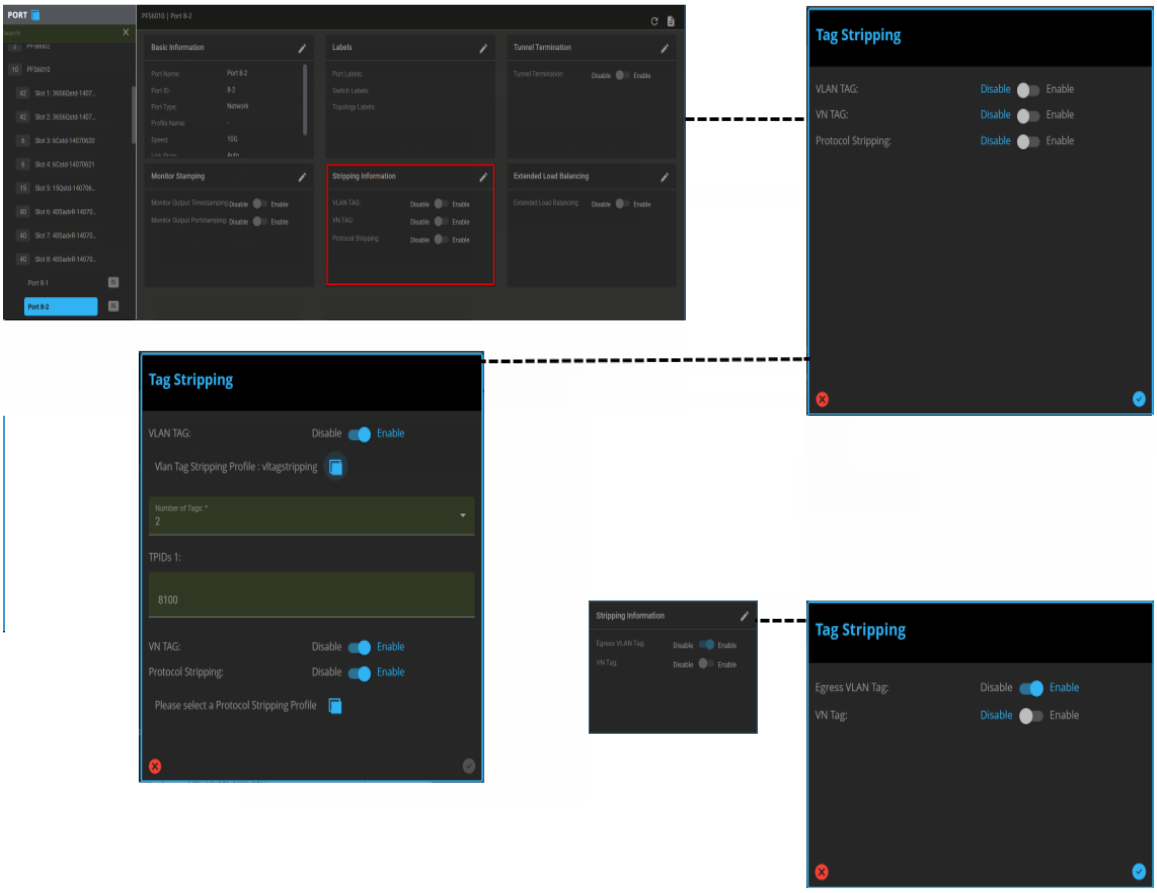
A user can configure VN, VLAN, MPLS L3 Label (after clicking on this, the user can see L2 MPLS stripping feature as well), and VXLAN for a selected 5xxx series device by navigating to the Switch Configure lifecycle, selecting a Switch and clicking on the Configuration tab. Click the edit icon to make any changes to the settings. Click on the blue circled check mark to save the changes or click the red **X** to cancel the changes.



Note: Egress VLAN Tag Stripping is supported only in 5k devices and in Monitor/Duplex/Service port types.

VLAN Tag Stripping Port Feature Profile	
VN Tag Stripping	Enable / Disable VN Tag Stripping on this port.
VLAN Tag Stripping	Enable / Disable VLAN Tag Stripping on this port.
Number of Tags to Strip	User-selectable number (i.e., 1, 2, or all) of tags to be removed.
VXLAN Tag Stripping	Enable / Disable VXLAN Tag Stripping on this port.
MPLS L3 Label Stripping	Enable / Disable MPLS L3 Label Stripping on this port.
Egress VLAN Tag Stripping	Enable / Disable Egress VLAN Tag Stripping on this port. (5000 series devices only, not supported in PFS-503x and PFS-504x devices)

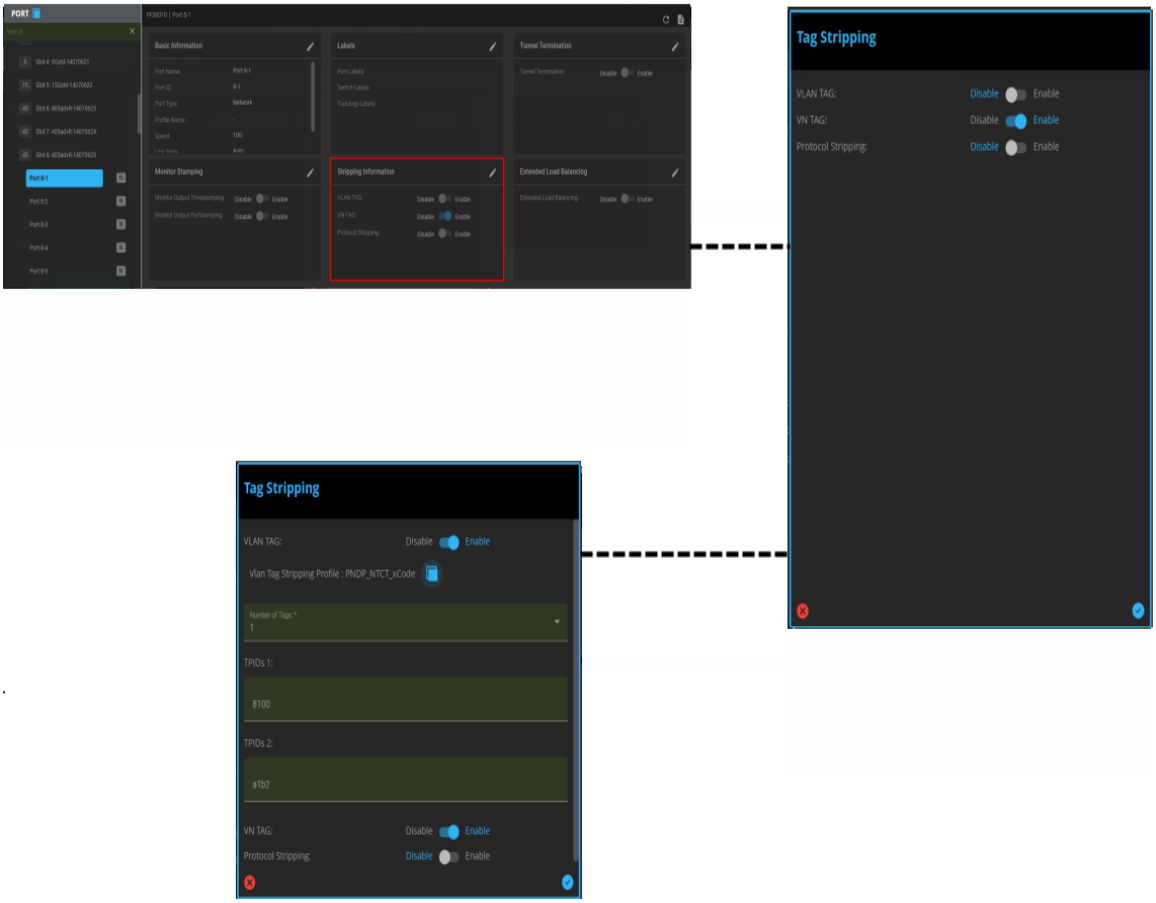
A user can configure VXLAN for a selected 5000/7000 series device by navigating to the Switch Configure lifecycle, selecting a Switch and clicking on the Configuration tab. Click the edit icon to make any changes to the settings. Click on the blue circled check mark to save the changes or click the red **X** to cancel the changes.



VLAN Tag Stripping Port Feature Profile	
VLXAN Tag Stripping	Enable / Disable VXLAN Tag Stripping on this port.
VTEP	IP address for VXLANTunnel End Point.
UDP Port	Port number for UDP.
VNID	24-bit segment ID number for VXLAN.

VN, VLAN Tag Stripping Port Feature Profile (UI for 6000 Series Platforms)

A user can configure VN and VLAN for a selected 6000 series device by navigating to the Switch Configure lifecycle, selecting a Switch and clicking on the Configuration tab. Click the edit icon to make any changes to the settings. Click on the blue circled check mark to save the changes or click the red **X** to cancel the changes.

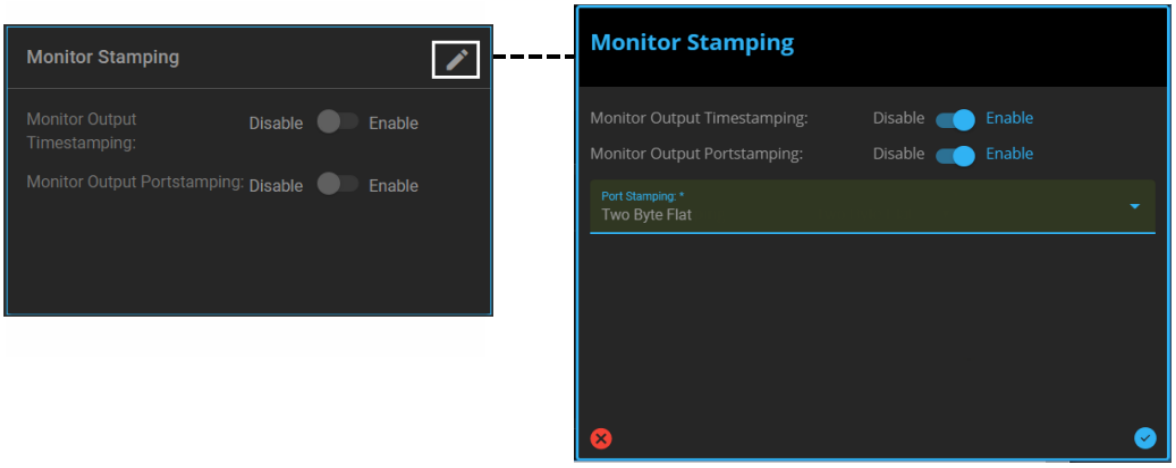


VLAN Tag Stripping Port Feature Profile	
VN Tag Stripping	Enable / Disable VN Tag Stripping on this port.
VLAN Tag Stripping	Enable / Disable VLAN Tag Stripping on this port.
Number of Tags to Strip	User-selectable number (i.e., 1, 2, or all) of tags to be removed.
TPID	Tag Protocol Identifier (TPID) with standard value of 0x8100.

Monitor_Stamping (PFS 6000 Series Only)

Packet Port Stamping can be used only on ports of a 40SadvR line card (on a 6000-series PFS) whose firmware image supports port stamping on that port.

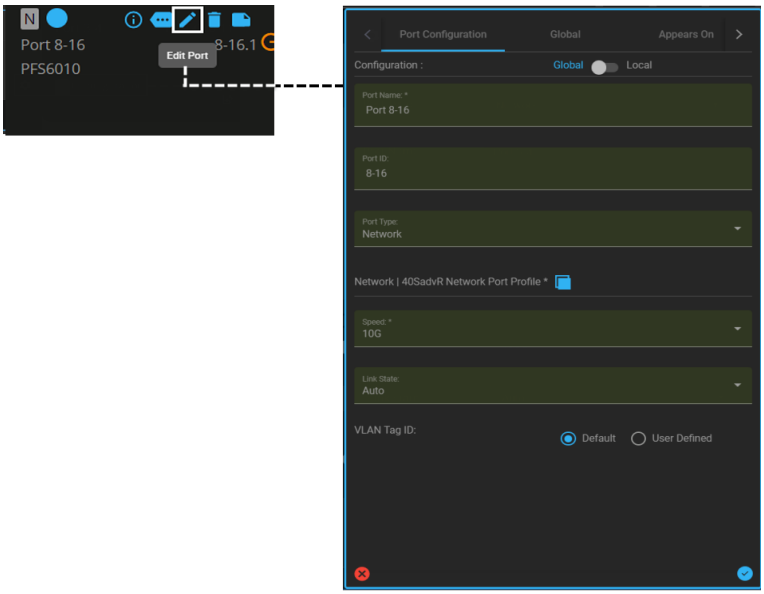
Click the edit icon to make any changes to the settings. Click on the blue circled check mark to save the changes or click the red **X** to cancel the changes.



Monitor_Stamping	
Monitor Output Portstamping	Enable / Disable Monitor Stamping on this port. Assigns a port stamp when traffic leaves a monitor port.
Port Stamping	Select One Byte Flat or Two Byte Flat as the portstamping option (Two Byte Flat is the default).
Monitor Output Timestamping	Enable / Disable Monitor Time Stamping on this port. Assigns a time stamp when traffic leaves a monitor port.

Port Properties from Deploy Lifecycle

When in Deploy Lifecycle, individual port properties / configurations can be displayed / edited by selecting Port Configuration on an individual node object.



Note: Port configurations cannot be changed from the Configure Lifecycle while a port is on a published topology.

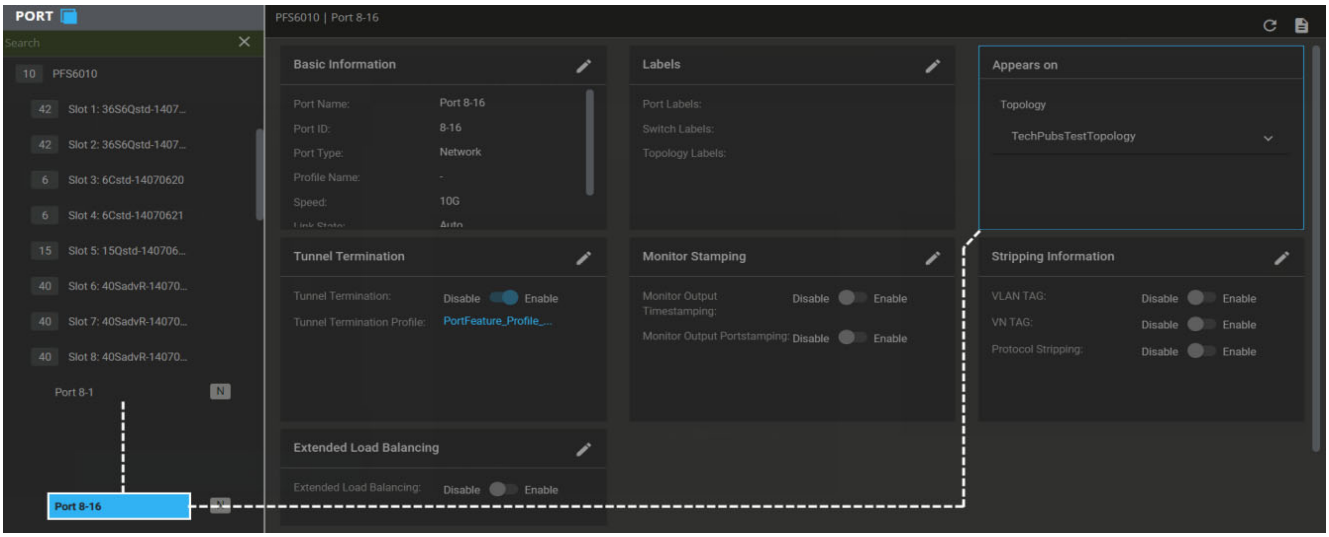
After unpublishing the topology, the port configuration can be changed from the Configure Lifecycle with the configuration changes taking affect immediately.

However, when the topology is republished, it will use the port profile that was assigned to the port when it was originally placed on the topology. This port profile was from the time prior to the configuration being changed (i.e., no stamping or tunnel termination). The topology publication remembers the initial port topology, ignoring any port configuration changes made after the initial publication.

To resolve this situation, unpublish the topology, remove the existing port from the topology, then select and drag the updated port from the port list into the topology screen. You can now connect the updated port as required and republish the topology.

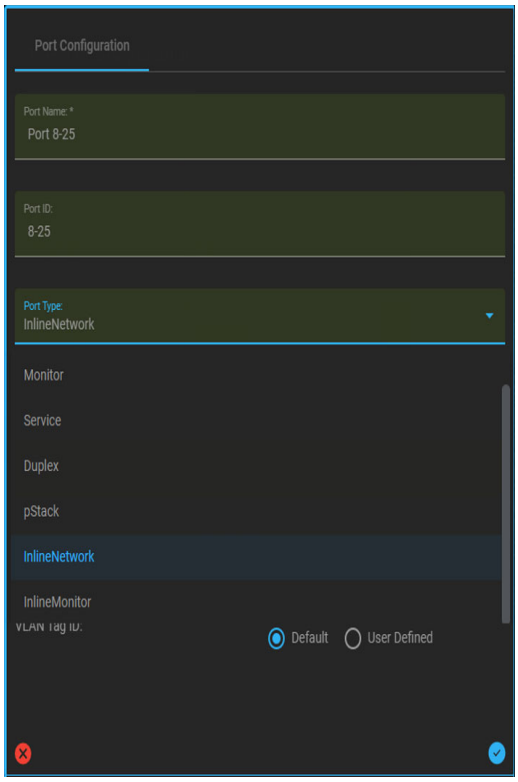
Configure > Port on Topology Association

Clicking on a port (if associated with a topology) from Configure > Perspective > Port displays an **Appears on Topology** card containing a list of all topologies (published / unpublished) the selected port is associated. Clicking on a topology version will open the screen of the selected topology from the Deploy Lifecycle.



Configure > Inline Port

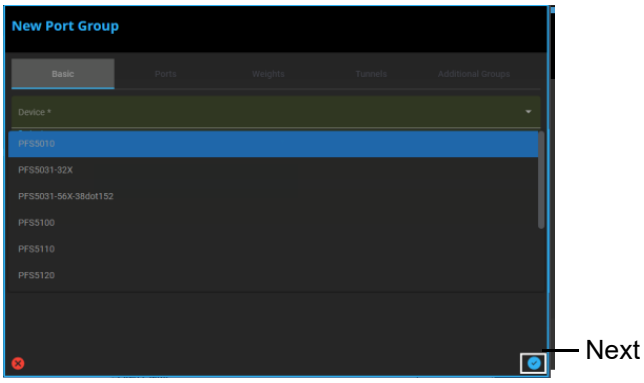
Inline port configuration from the Configure lifecycle behaves just like other port configurations. Changes are published immediately when submitted after validation is complete. Validation depends on group membership and published maps or topologies. Inline port types include **Inline Network** and **Inline Monitor**.



Perspective > Group

Selecting Group from the Perspective menu allows creating a new port group. Select Group, then click on **+ Group**. The New Port Group window displays.

Select a Device the group will reside on from the drop down menu. Click **Next** (**>**).



Basic

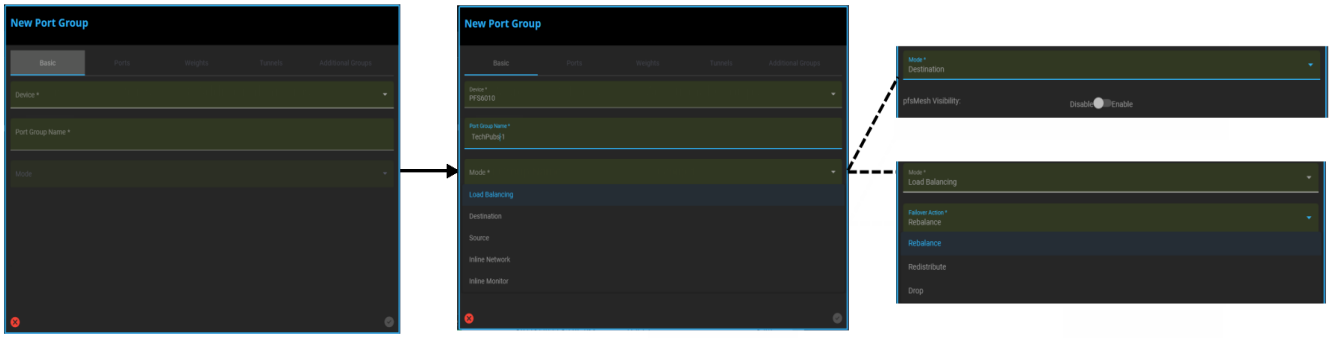
Enter a name for the new port group (56 characters maximum, no spaces allowed in the name) and select an operating mode (Load Balancing, Destination, Source, Inline Network, and Inline Monitor).

- If Destination is selected, a pfsMesh Visibility option displays, allowing destination port groups to be made visible to pStack; select either Disable (default) or Enable.
  When creating a local destination group, leave pfsMesh Visibility set to Disable.
- If Load Balancing is used, select the required failover action (i.e., select the action for the system to take if a member of the group is unavailable):
  - **Rebalance** - consolidate the load among the remaining active group members.
  - **Redistribute** - organize the offline port traffic to the remaining group members without disturbing the traffic on the remaining active ports.
  - **Drop** - stop traffic for the offline port member – traffic is not rebalanced or redistribute.
  - **Weighted Redistribute** - redistribute the traffic to remaining load balance weighted ports, without disturbing the traffic

> **Note:** The Weighted Redistribute failover action is only available for load-balanced ports, it is not supported for load-balanced tunnels. It is not applicable for PFS 6000s.

  - **Round Robin** - allows each active configured member of the group to forward traffic in turn

> **Note:** The Round Robin failover action supports the following platforms: 5100, 5120, 5121, 5110, 5030-32x, 5031-32X and 5031-56X.

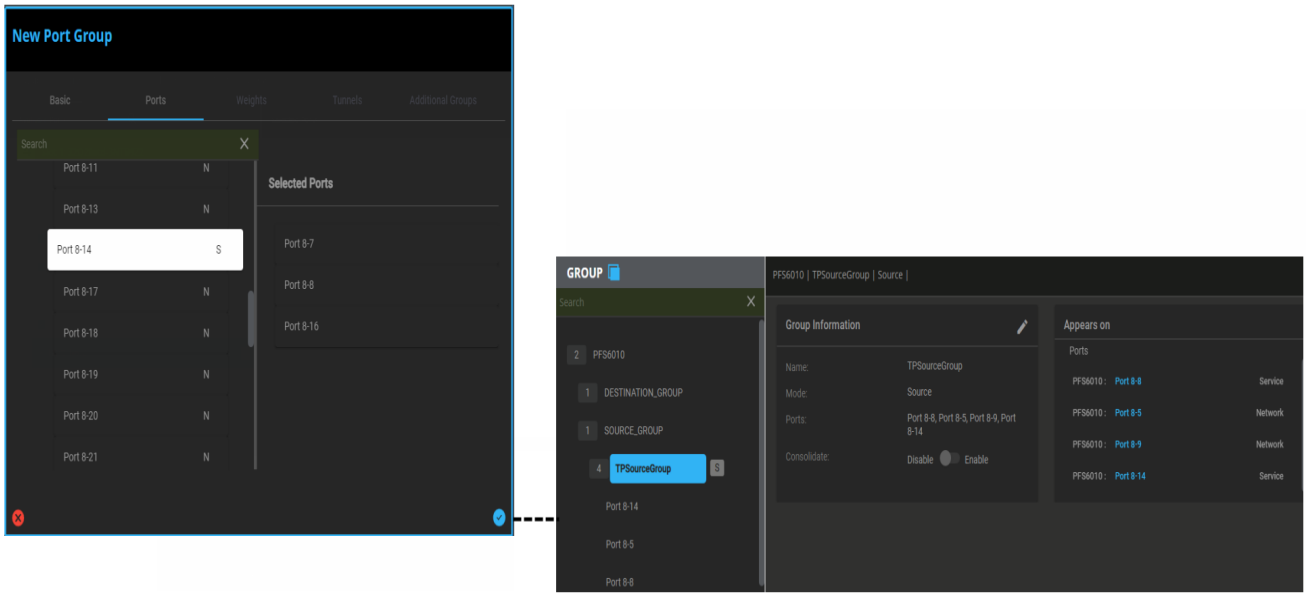


Ports

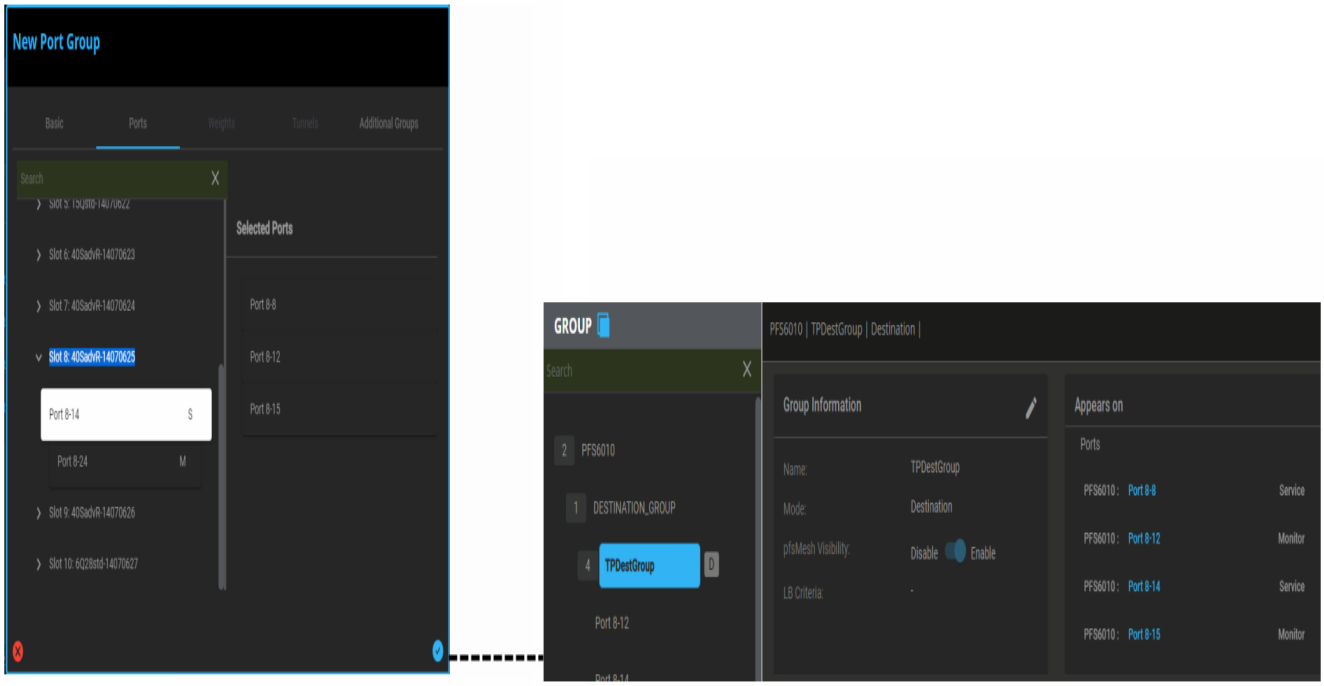
Select the ports to be included in the new port group by clicking on each applicable port name and dragging the port to the Selected Ports column.

Once required ports are selected, click on the Accept (check mark) icon to save the group.

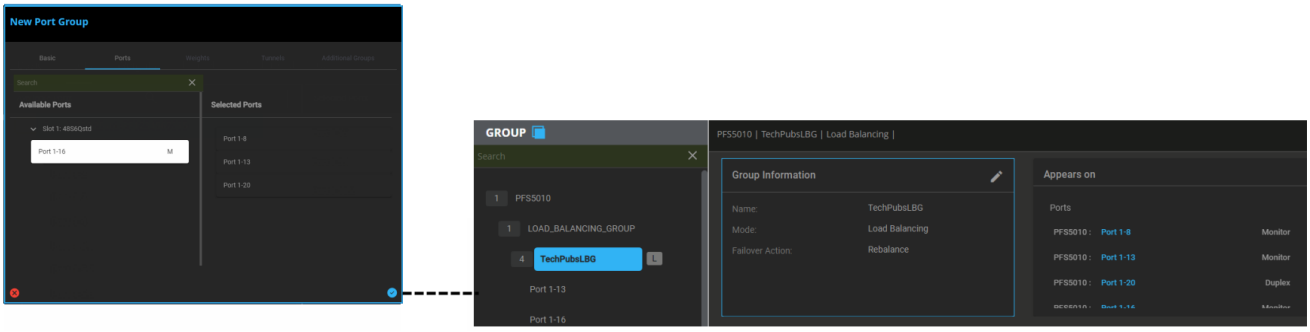
- **Source Groups:** Select Network / Service / Duplex ports.



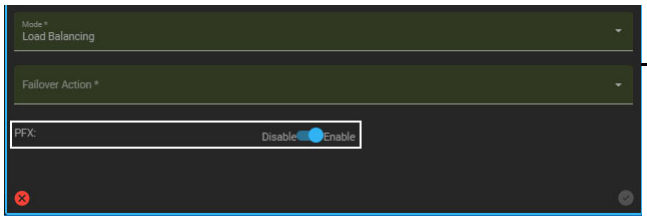
- **Destination Groups:** Select Service / Duplex / Monitor ports. Selected ports must already be configured as Monitor.



- **Load Balance Groups:** Select Service / Duplex / Monitor ports.

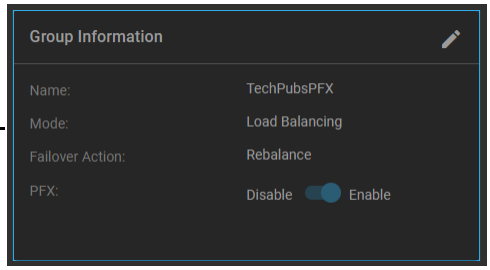


– Enabling PFX mode:



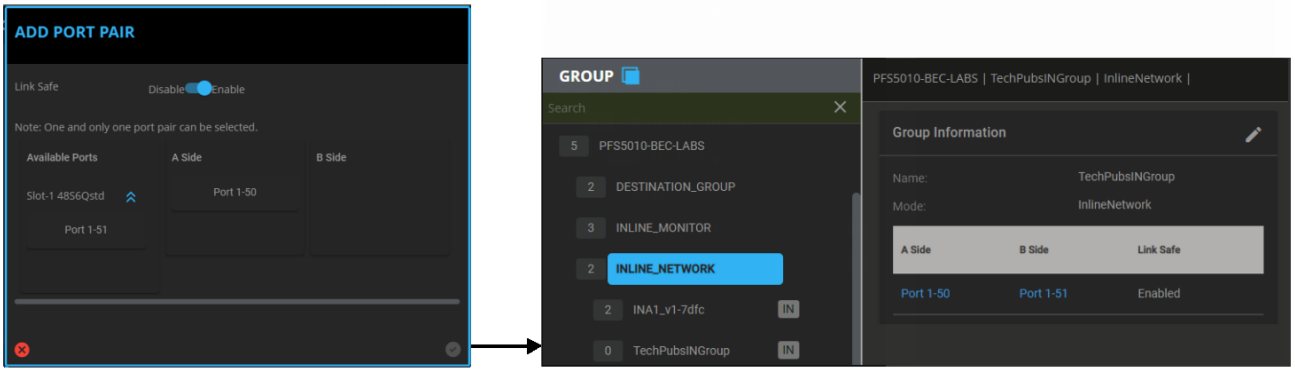
Adding new Port Group

Editing Group Information



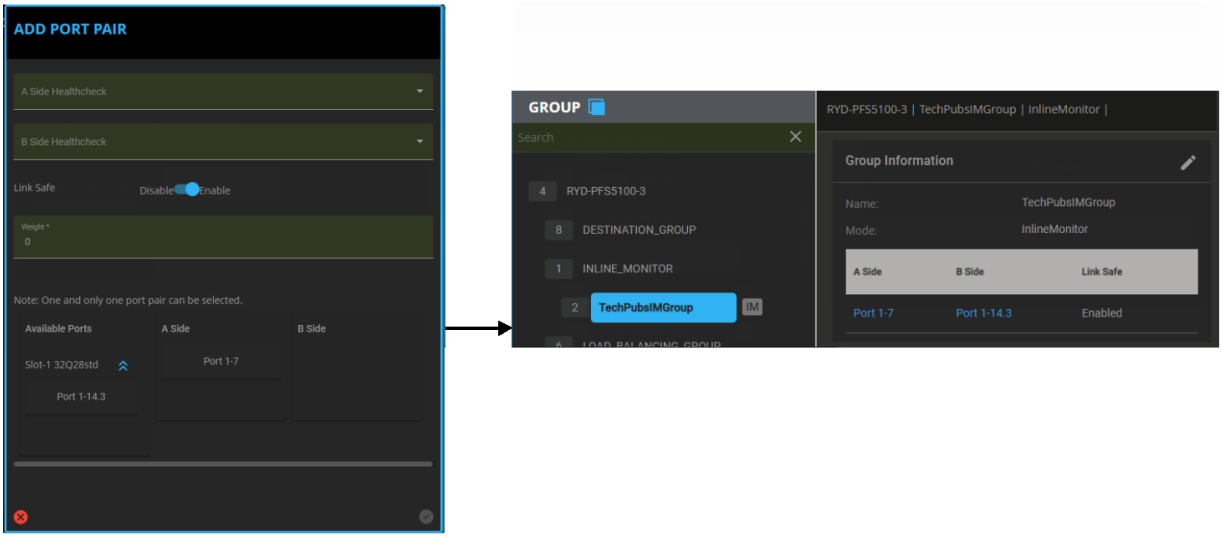
Inline Network Group Ports

Inline network groups have a set of port pairs, each with a link safe and weight setting. VLAN tagging can also be configured for the group. For each pair, an "A Side" and "B Side" port is required. When an "A Side" port is added, the "B Side" port will default to the next port.



Inline Monitor Group Ports

Inline monitor groups also have a set of port pairs, each with a link safe setting. Either an "A Side" or a "B Side" port must be configured. For each port in the pair, a health check library can be assigned.



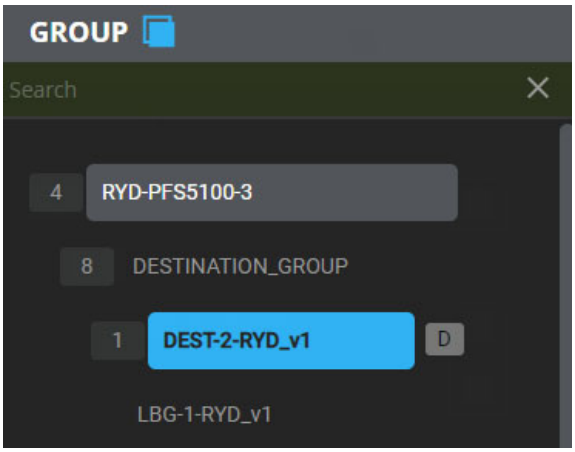
Additional Groups

A port group using Destination Mode must also have a Load Balancing Criteria assigned to the group. Port groups using Destination Mode with pfsMesh Visibility set to Disabled will have their Load Balance Criteria assigned when the traffic map/connection is created.

Destination Groups configured as available / visible to pfsMesh are displayed with a pStack Group (**PG**) icon next to them, whether the group is on an unmanaged or managed switch.

Switches that are discovered through pfsMesh and are not managed by this PFS Fabric Manager are marked with a Remote Switch (**RS**) icon.

Note: Groups discovered from unmanaged switches are not modifiable, and have no context aware menu.

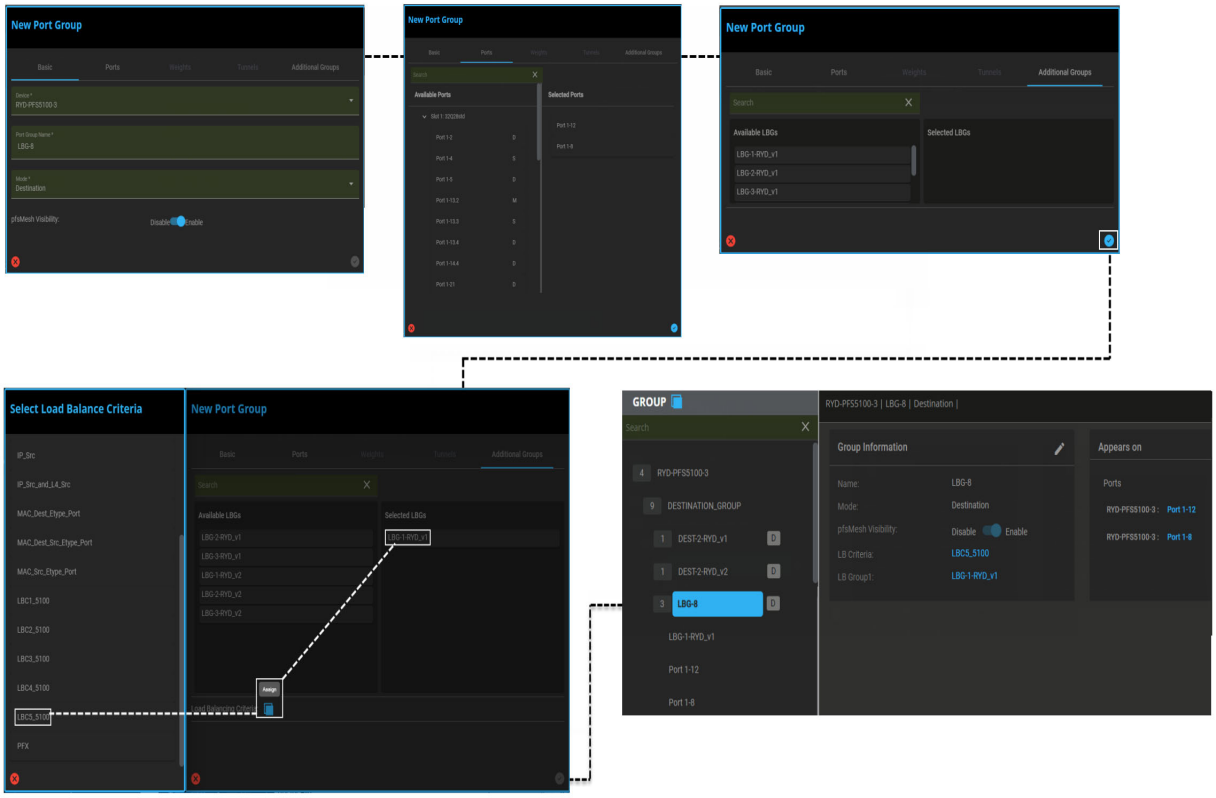


Configuring a Destination Group as a Remote Monitor Group for pfsMesh

After completing the Basic (Basic on page 3-47) and Ports (Ports on page 3-48) sections (selecting Destination mode and setting pfsMesh Visibility option to Enable), click on **Additional Groups**.

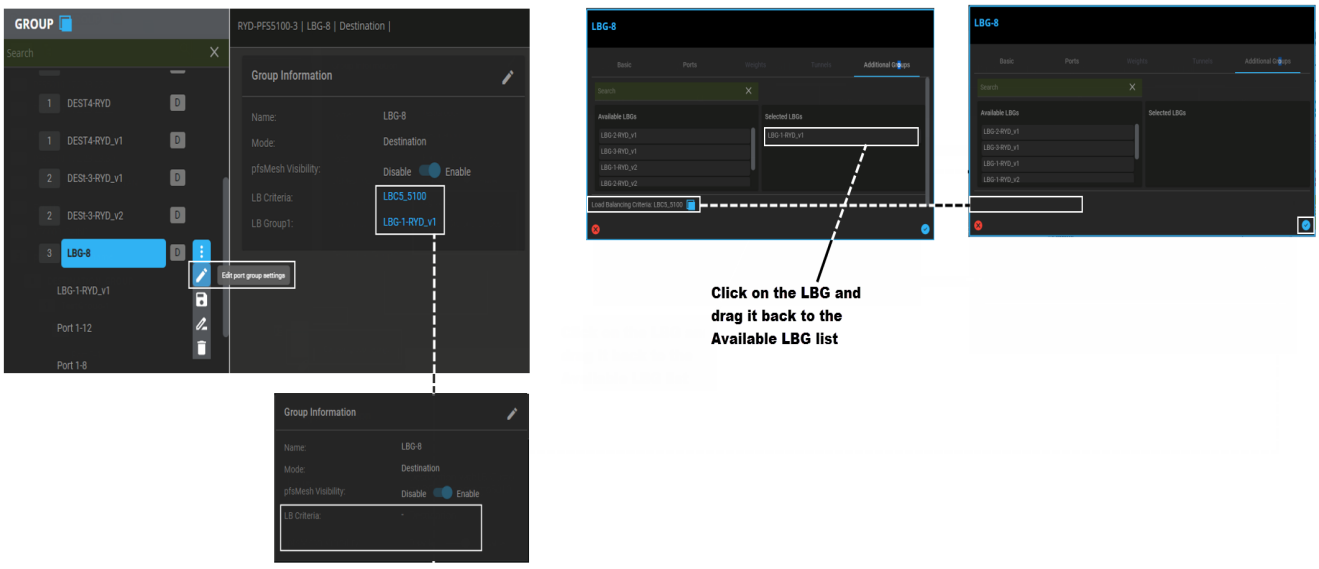
Double-click on the default (displayed) Load Balancing Group name, then on the Load Balancing Criteria **Accept** checkbox. Select the required Load Balancing Criteria name from the list, then click the blue **Accept** icon.

Note:
To multi-select groups, hold down the Ctrl key and select two or more Load Balancing Group groups.
To deselect a group, click on a listed group or for multiple groups, hold down the Ctrl key and select two or more Load Balancing Group groups.



Removing a Load Balancing Group from a Remote Monitor Group

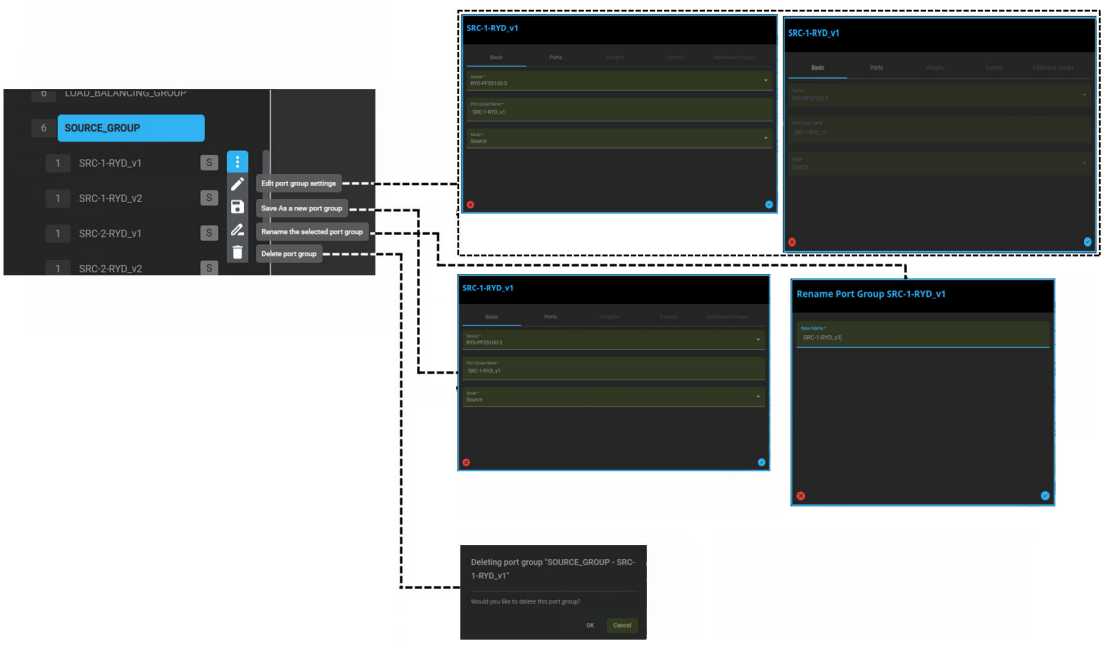
To remove an assigned Load Balancing Group after adding it to a Remote Monitor Group, from the Additional Groups page, click on the Load Balancing Group name and drag it back to the Available LBG list. The assigned Load Balancing Criteria is removed from the page. Click on the Accept check mark to keep the changes. The LB Groups and LB Criteria fields are now cleared.



Port Group Sub-Menu

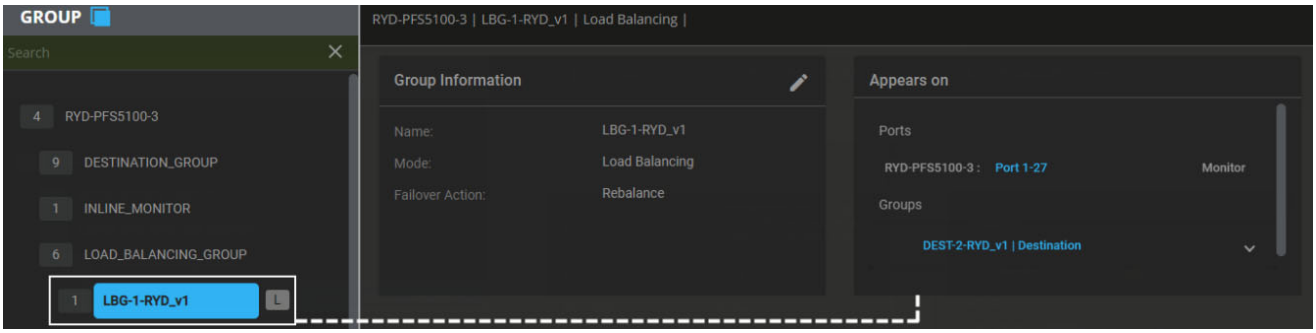
Each port group has a sub-menu with the following tasks:

- Edit port group settings
- Save-As a new port group
- Rename the selected port group
- Delete port group



Configure > Group on Topology Association

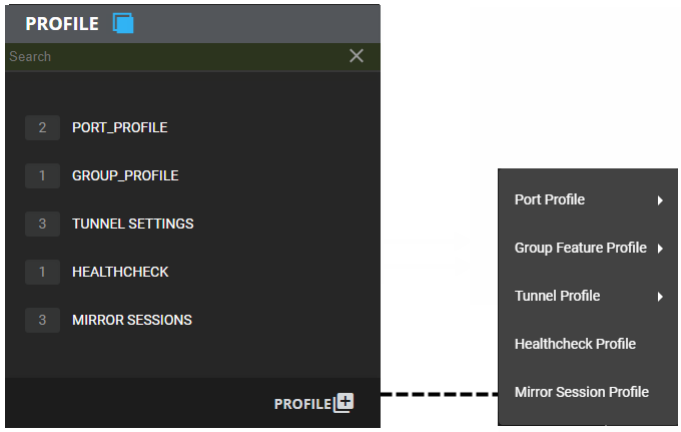
Clicking on a group (if associated with a topology) from Configure > Perspective > Group displays an **Appears on Topology** card containing a list of all topologies (published / unpublished) the selected group is associated. Clicking on a topology version will open the screen of the selected topology from the Deploy Lifecycle.



Perspective > Profile

Selecting Profile from the Perspective menu allows viewing the properties of the ports in the installed line cards in a switch, switch groups, and configuration features of installed switches.

From the Profile menu, click on **+ Profile** and select the profile type (Port, Group or Tunnel) to create.

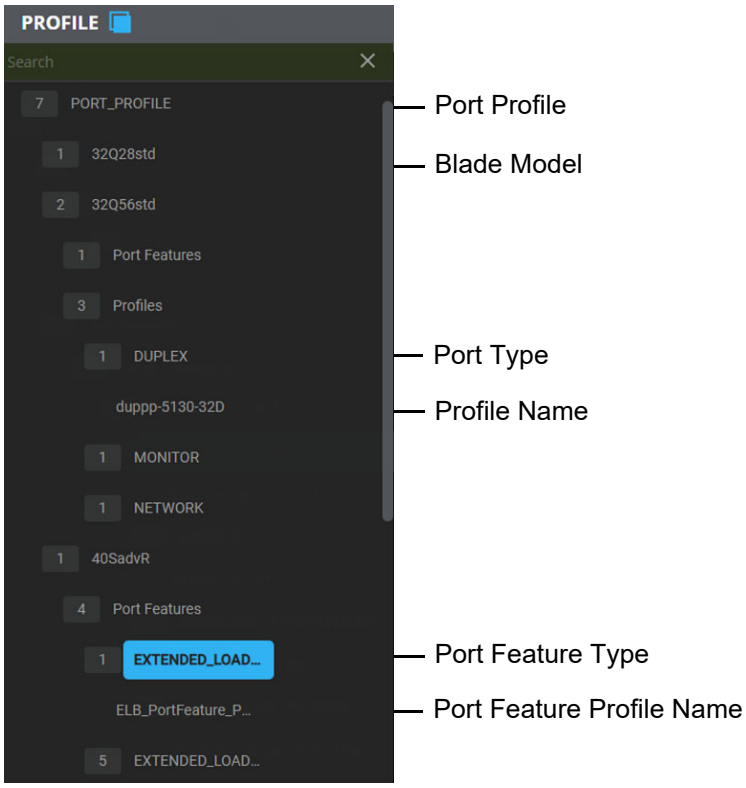


Port Profile

Clicking on Port Profile displays a list of port types (Duplex, Network, Monitor, Service, pStack) associated with a line card; clicking on a port type allows viewing / editing the properties associated with the port type.

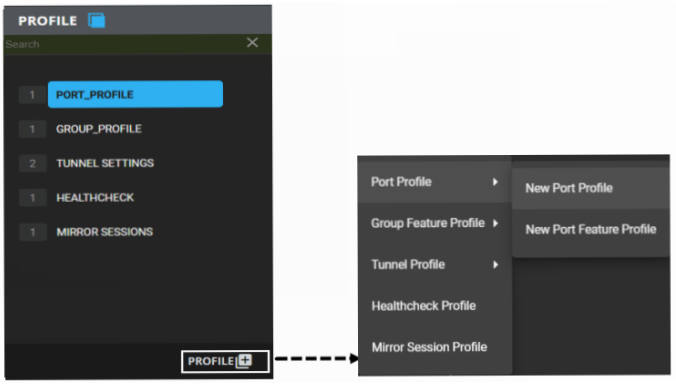
Port Features displays the features associated with the port; clicking on a port feature allows editing the properties associated with each feature.

Note: Profile creation in software versions prior to 6.0 are no longer supported.

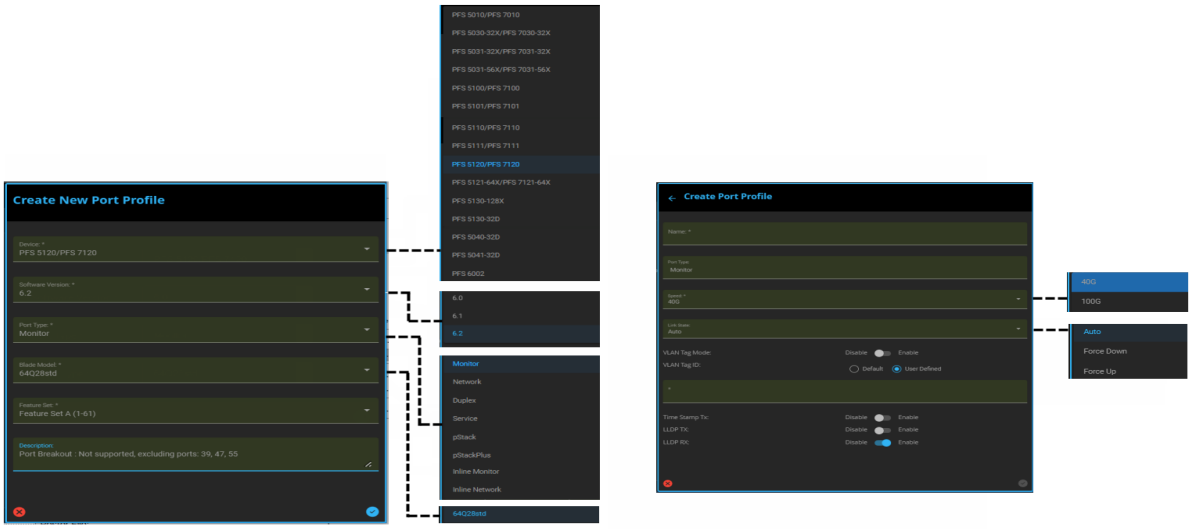


Creating a Port Profile

1 From Perspective > Profile, click on **+ Profile**. Select **Port Profile** and **New Port Profile** from the profile menu.



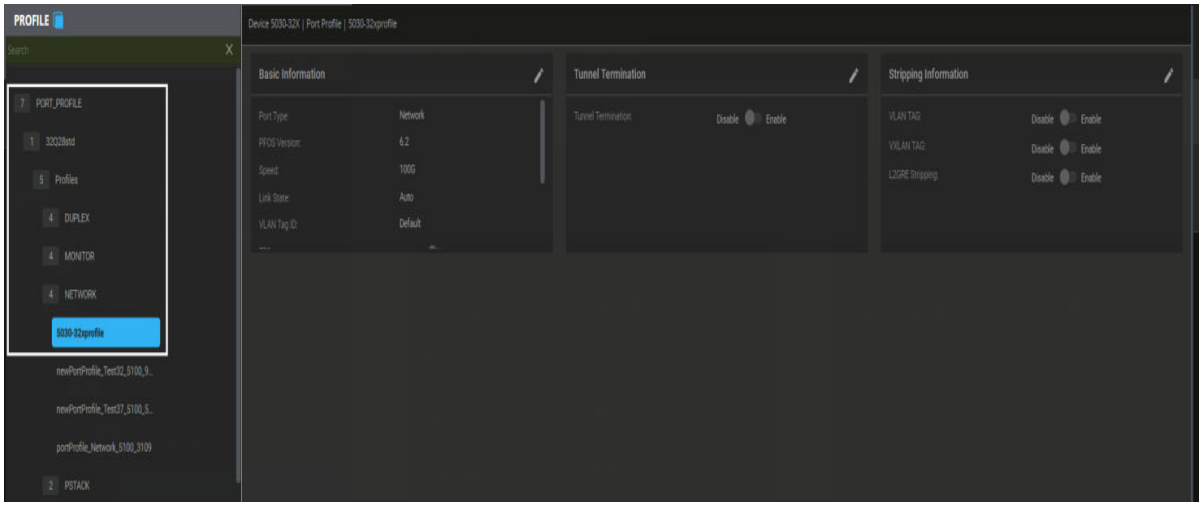
2 From the Create New Profile screen, define the properties of the port profile.



Profile Property		Description
Device		Select the required switch.
Blade Model		Select the required line card for the selected switch.
Port Type		Select the required port for the selected line card.
Basic	Name	Profile Name (56 characters maximum)
Properties	Speed	Select the transceiver port speed, if the inserted transceiver supports more than one speed.
	Link State	Select the link state for the port (options vary depending on port type): • Auto – Normal operation • Force Down – Force the link down • Force Up – Force the link up
	VLAN Tagging	Enable / Disable VLAN Tagging in this port (this option is dependent on port type).
	VLAN ID	Use the default VLAN ID (if VLAN Tagging is set to Enable), or to specify the starting VLAN ID, select User Defined and enter a starting VLAN ID.

3 Click on the Accept icon to save the new port profile.

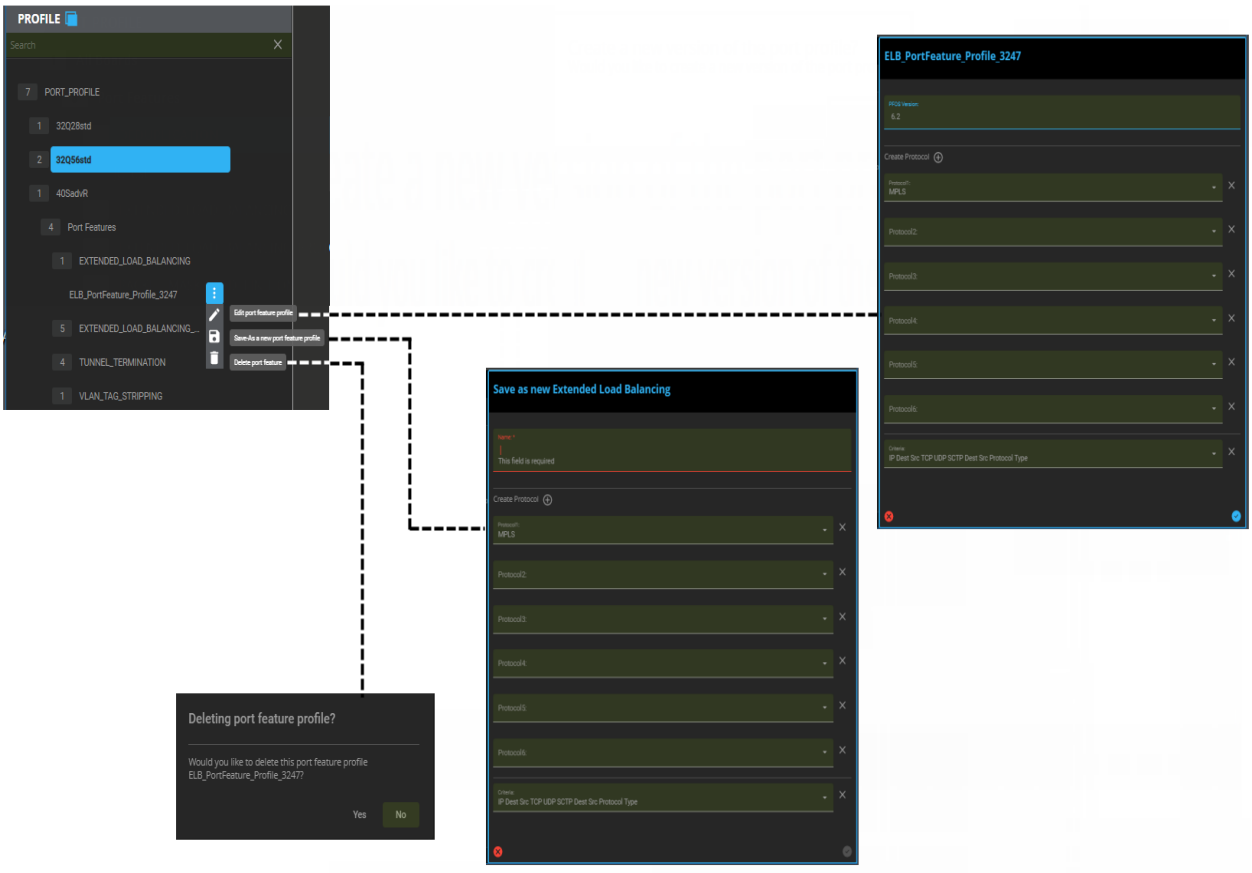
4 From the Port Profile menu, you can view the properties of the new port profile.



Port Profile Sub-Menu

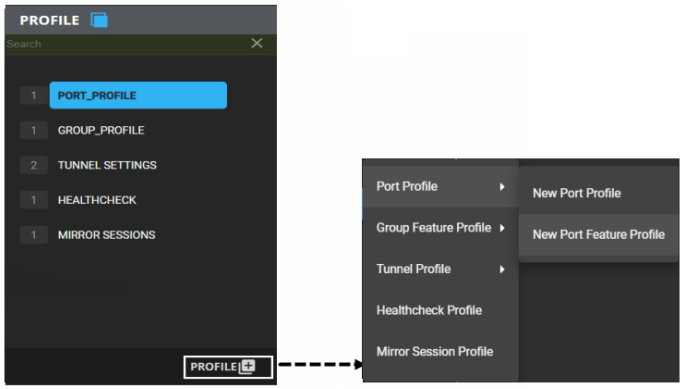
Each port profile has a sub-menu with the following tasks:

- Edit port feature profile
- Save-As a new port feature profile
- Delete port feature profile

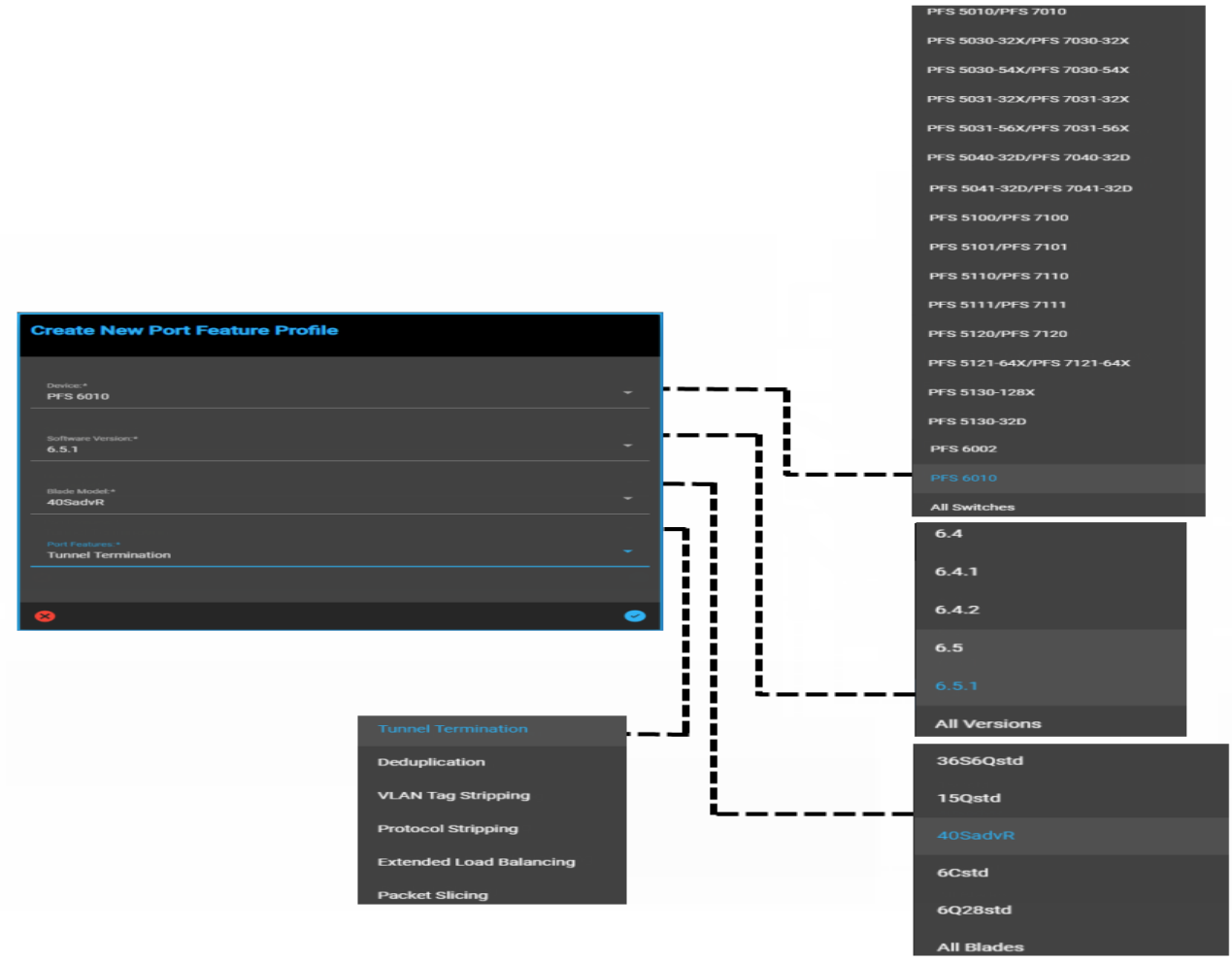


Creating a Port Feature Profile

1 From Perspective > Profile, click on **+ Profile**. Select **Port Profile** and **New Port Feature Profile** from the profile menu.



2 From the Create Port Feature Profile screen, select the Device, Blade Model, and Port Feature type. Click on the arrow to open the second window, then enter a name for the profile (56 characters maximum) and fill out the remaining fields required by the Port Feature Profile type (see subsequent sections for details).



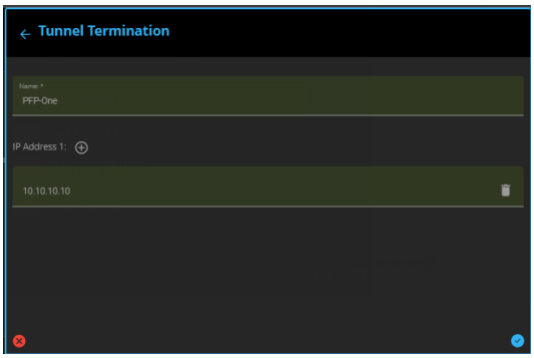
3 Click on the Accept icon to save the new port feature profile.

4 From the Port Profile menu, you can view the properties of the new port feature profile.

Tunnel Termination Profile

When creating a Tunnel Termination Profile, add the IP address to be used for terminating the IP tunnel.

Note: Clicking on the **+** next to the initial IP Address field allows adding additional IP addresses as required.



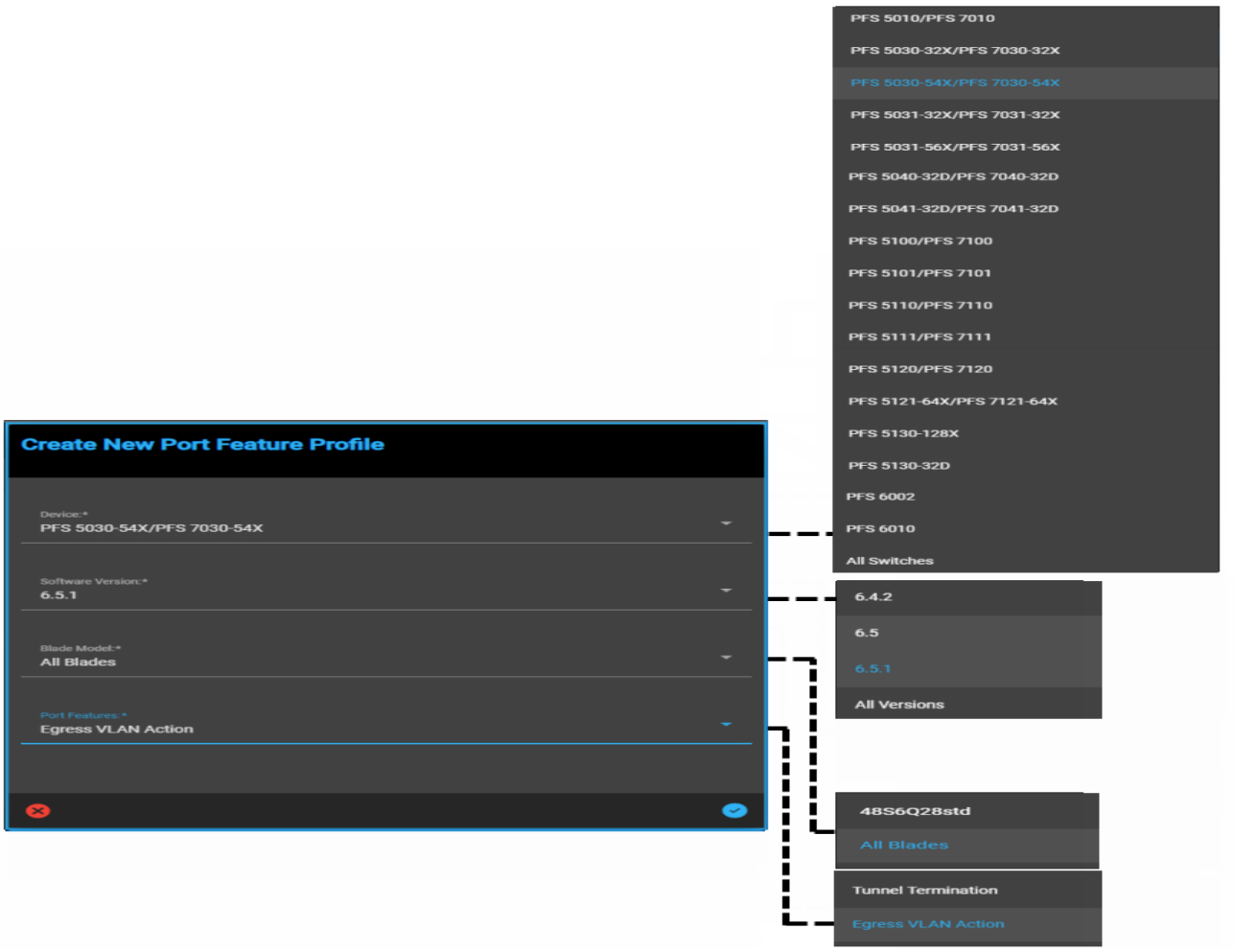
Egress VLAN Action Profile

Egress VLAN Action profiles can be used only on a 5k/7k-series PFS. Only one egress-vlan-action profile is allowed per Inline Monitor port, a PFS device can support a total of 8 egres-vlan-action profiles, and each egress-vlan-action profile can support a maximum of 16 VLAN IDs.

Creating an Egress VLAN Action Profile

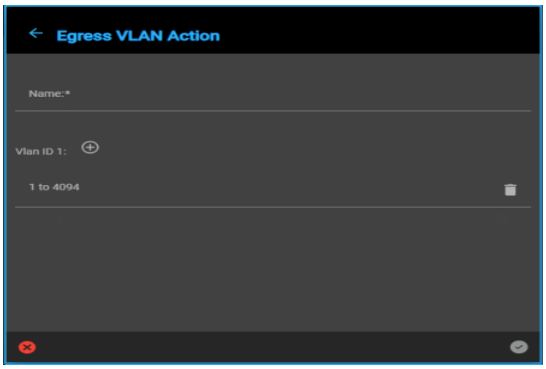
1 From Perspective > Profile, click on **+ Profile**. Select **Port Profile** and **New Port Feature Profile** from the profile menu.

2 From the Create Port Feature Profile screen, select the Device, Software Version, Blade Model, and Port Feature type. Click on the accept icon.



3 The Egress VLAN Action screen is displayed, enter a name for the profile and the VLAN ID.

Note: Clicking on the **+** next to the initial VLAN ID field allows adding additional VLAN IDs as required.



4 Click on the Accept icon to save the new Egress VLAN Action profile.

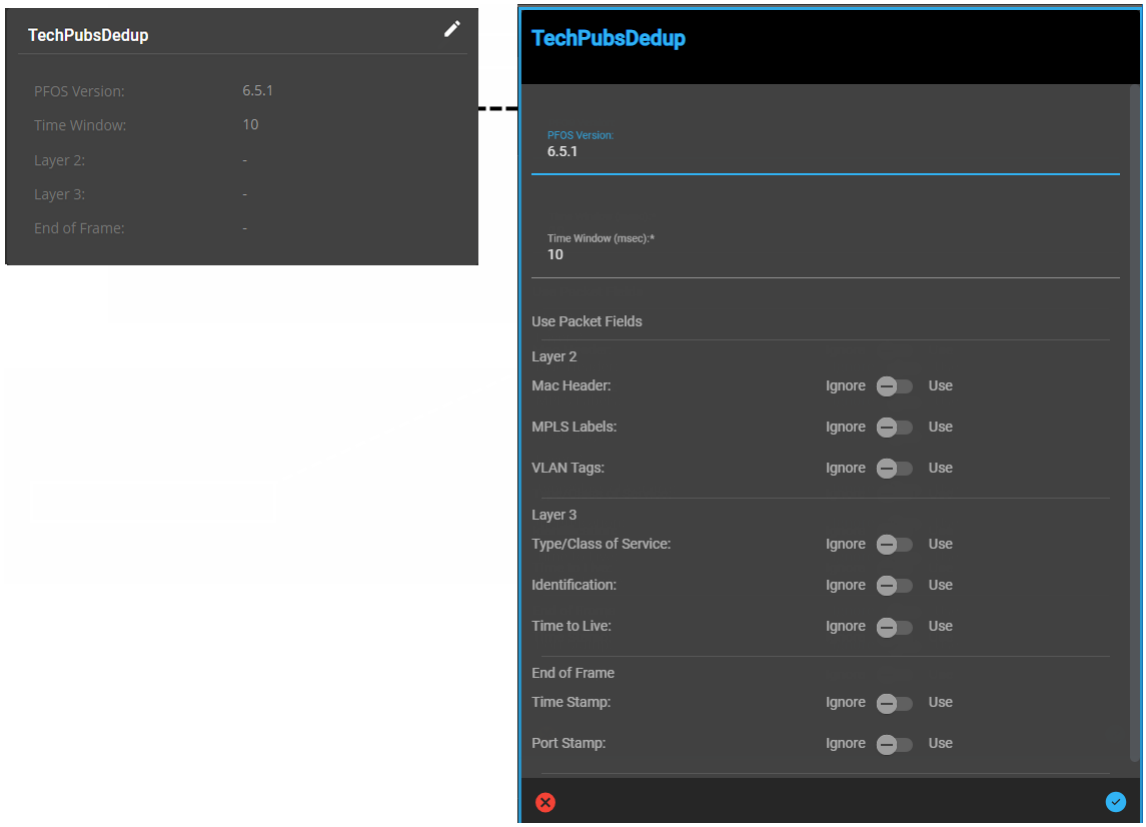
5 From the Port Profile menu, you can view the properties of the new Egress VLAN Action profile.

Deduplication Profile (PFS 6000 Series Only)

Deduplication Port Feature Profiles can be used only on ports of a 40SadvR line card (on a 6000-series PFS) whose firmware image supports deduplication on that port.

Creating a new Deduplication Port Profile:

Click the edit icon to make any changes to the settings. Click on the blue circled check mark to save the changes or click the red **X** to cancel the changes.



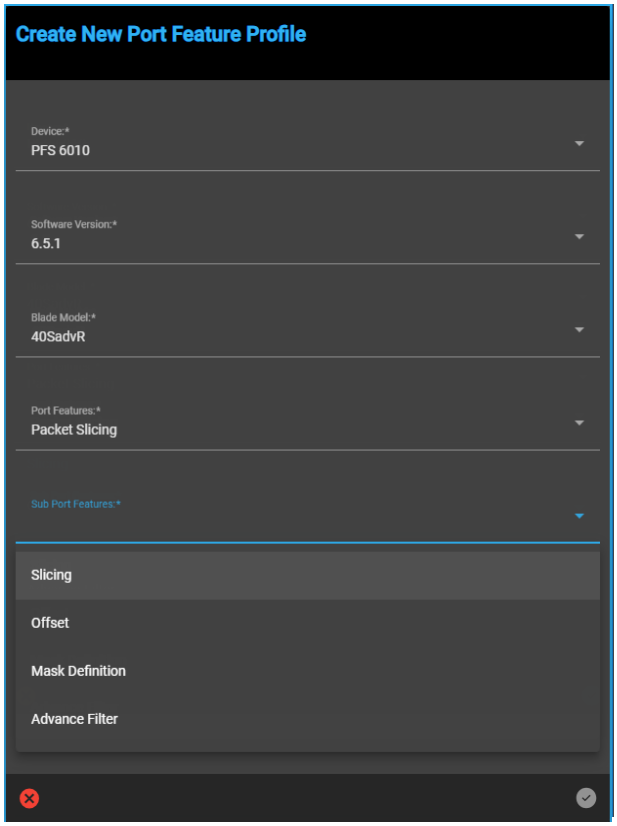
Deduplication Port Feature Profile			
Deduplication	Enable / Disable Deduplication on this port.		
Deduplication Port Feature Profile	(Optional) Select a profile name.		
Time Window	Specify a time window of between 1 and 4,000 milliseconds (default = 10) for tracking and comparison for each unique packet.		
Use Packet Fields	Layer 2	MAC Header	Ignore / Use on this port.
		VLAN Tags	Ignore / Use on this port.
		MPLS Labels	Ignore / Use on this port.
	Layer 3	Type / Class of Service	Ignore / Use on this port.
		Identification	Ignore / Use on this port.
		Time to Live	Ignore / Use on this port.
	End of Frame	Time Stamp	Ignore / Use on this port.
		Port Stamp	Ignore / Use on this port.

Packet Slicing Profile (PFS 6000 Series Only)

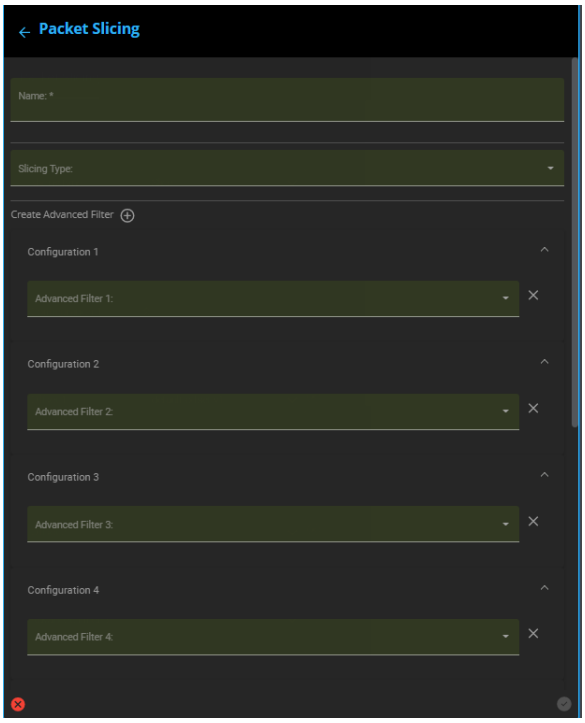
Packet Slicing Port Feature Profiles can be used only on ports of a 40SadvR line card (on a 6000-series PFS) whose firmware image supports packet slicing on that port.

The Packet Slicing profile has the following sub-port features:

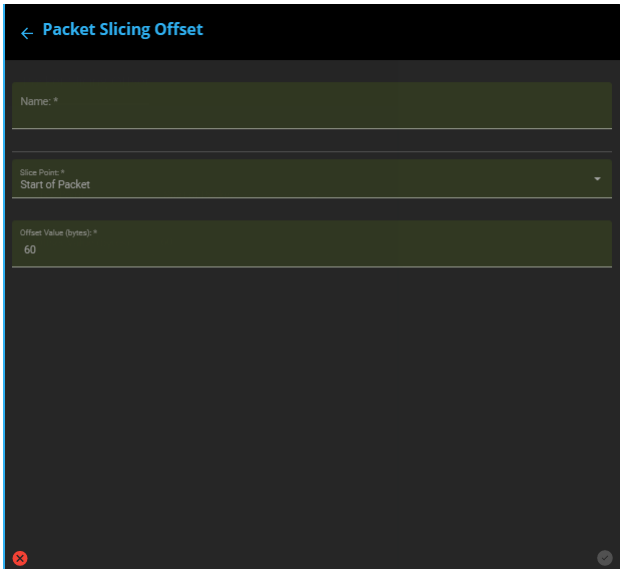
- Slicing
- Offset
- Masking Definition
- Filter



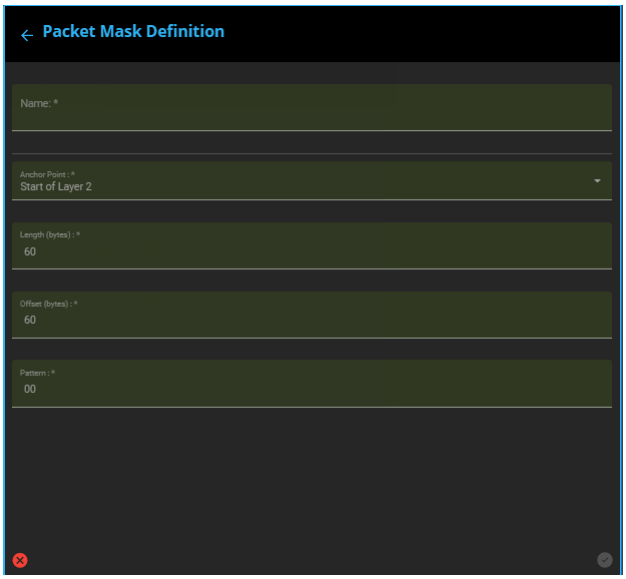
Packet Slicing port feature with Slicing type set to Slice.



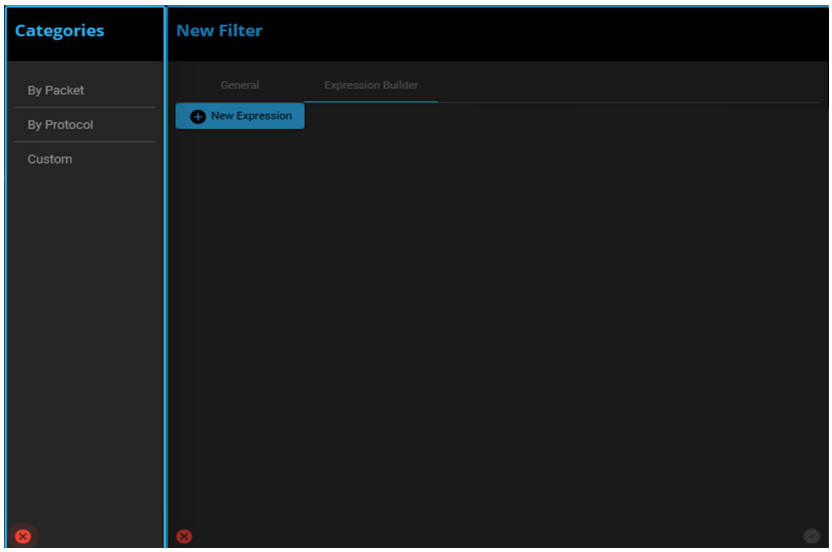
Packet Slicing Offset profile:



Packet Slicing Mask Definition profile:

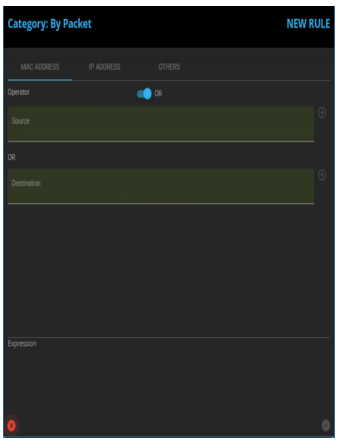

Packet Mask Definition
Name: *
Anchor Point : *
Start of Layer 2
Length (bytes) : *
60
Offset (bytes) : *
60
Pattern : *
00

Filter profile:

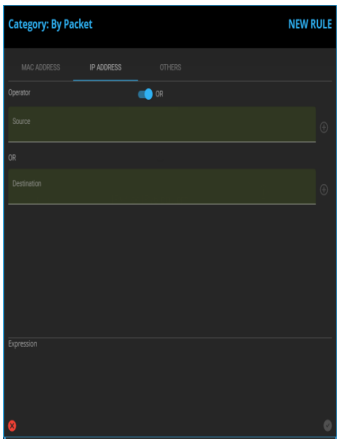


Filter by Packet:

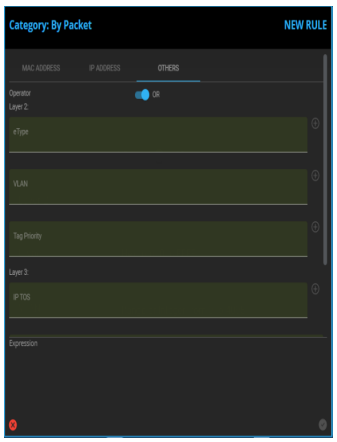
MAC Address



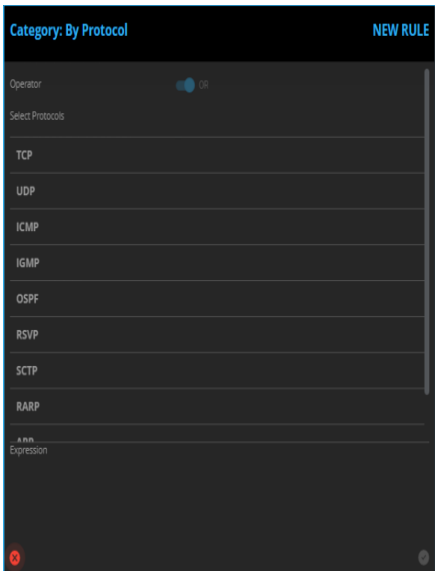
IP Address



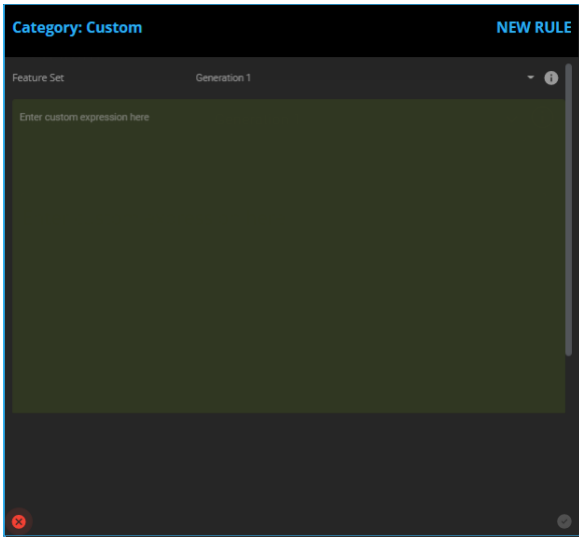
Other



Filter by Protocol:



Custom Filter:



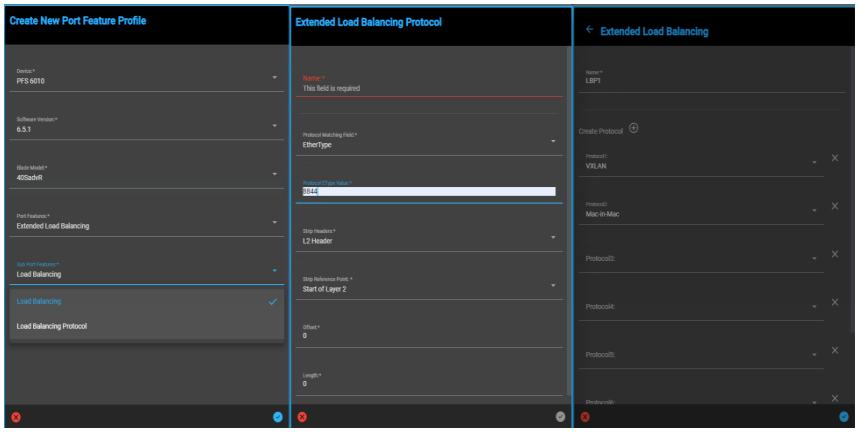
Extended Load Balancing Profile (PFS 6000 Series Only)

Extended Load Balancing Port Feature Profiles can be used only on ports of a 40SadvR line card (on a 6000-series PFS) whose firmware image supports extended load balancing on that port.

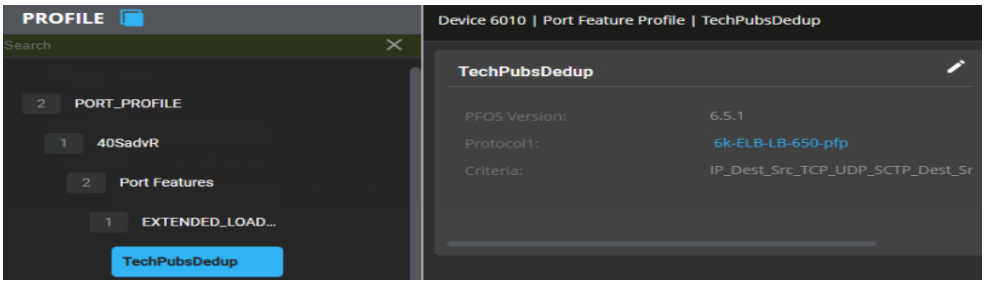
The Extended Load Balancing profile has the following sub-port features:

- Load Balancing
- Load Balancing Protocol

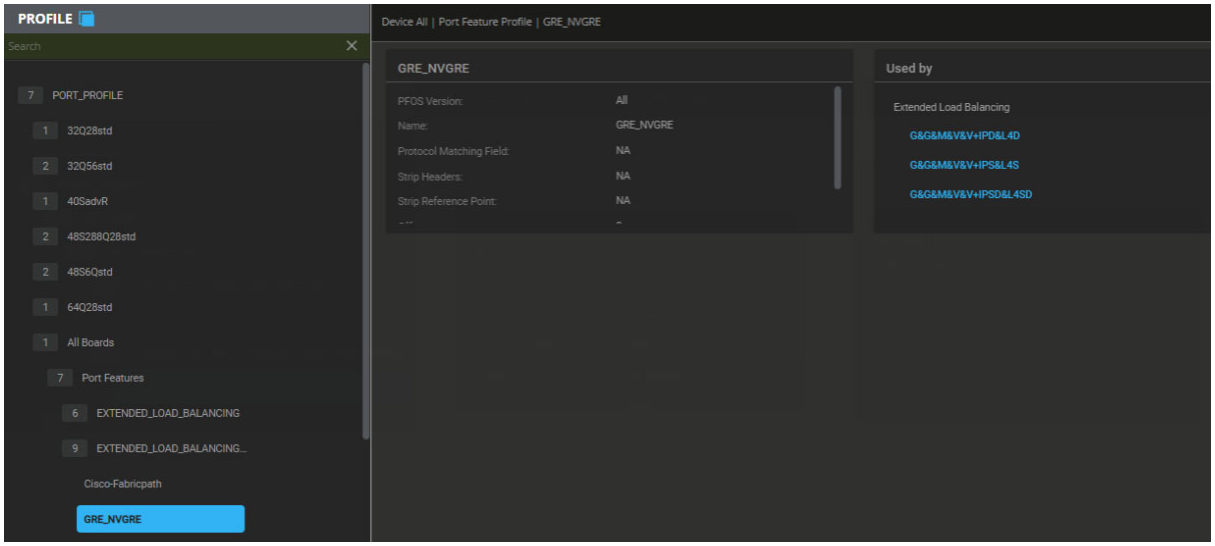
Creating a new Extended Load Balancing Profile.



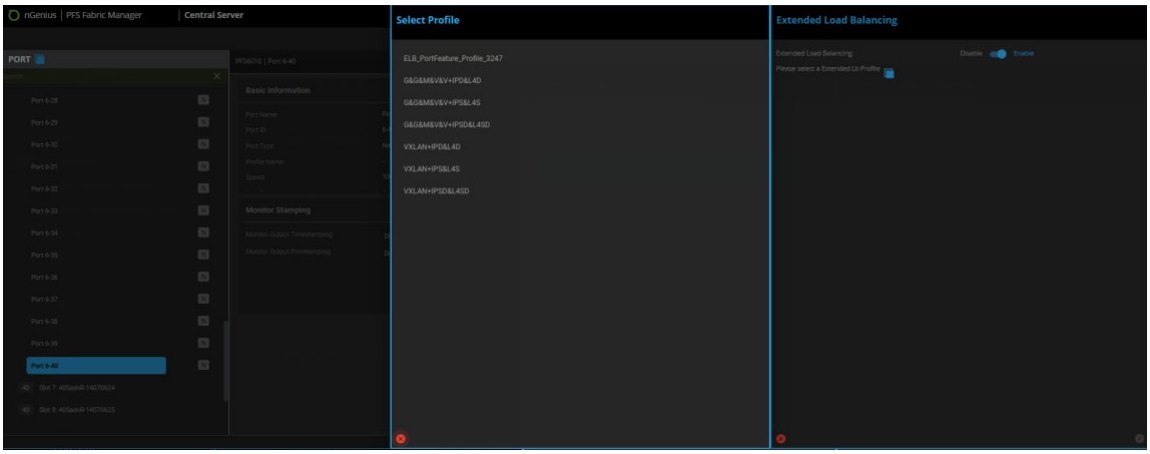
Viewing/Editing an Extended Load Balancing Profile.



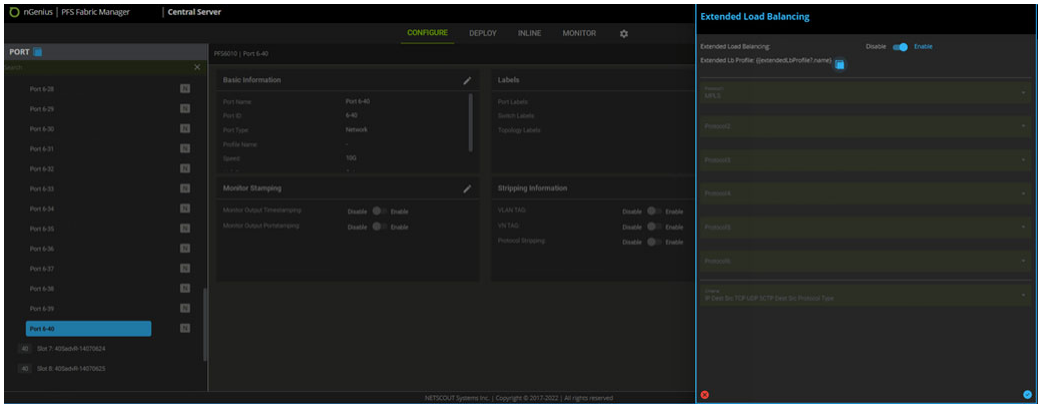
Viewing/Editing Extended Load Balancing Protocol Profiles.



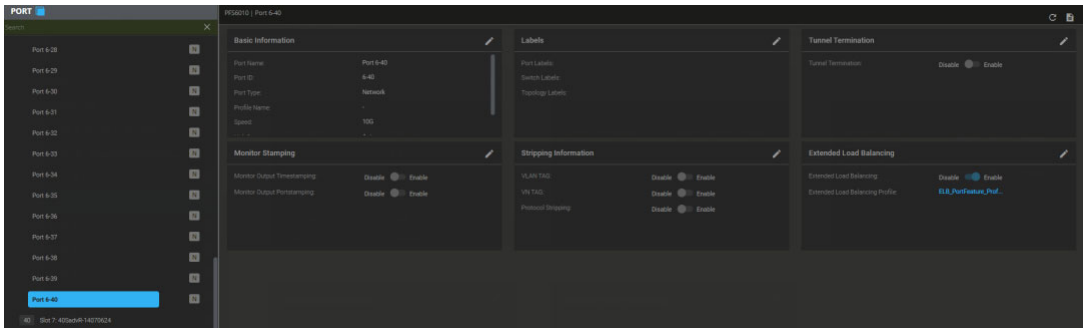
Assigning Extended Load Balancing to a supported Port.



Viewing/Editing of profile selection from the selected port.



Published profile on the selected port.

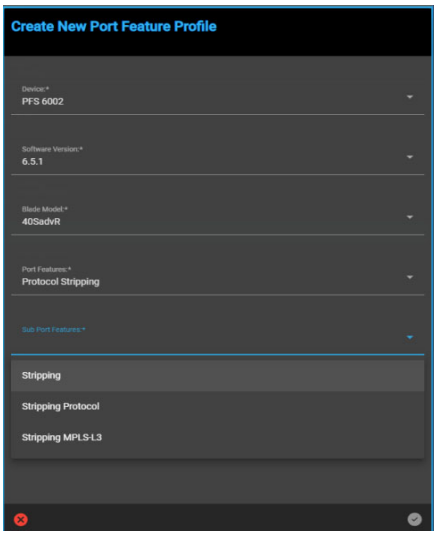


Protocol Stripping Profile (PFS 6000 Series Only)

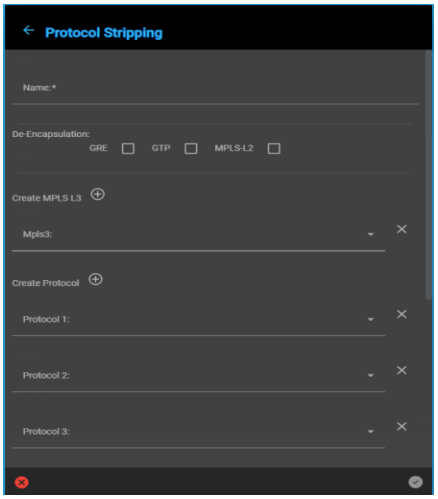
Protocol Stripping Port Feature Profiles can be used only on ports of a 40SadvR line card (on a 6000-series PFS) whose firmware image supports protocol stripping on that port.

The Protocol Stripping profile has the following sub-port features:

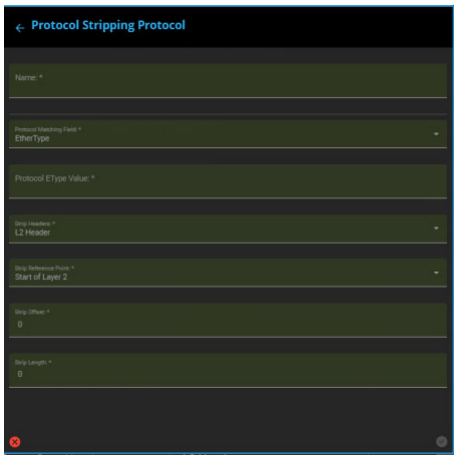
- Protocol
- Stripping
- MPLS-L3



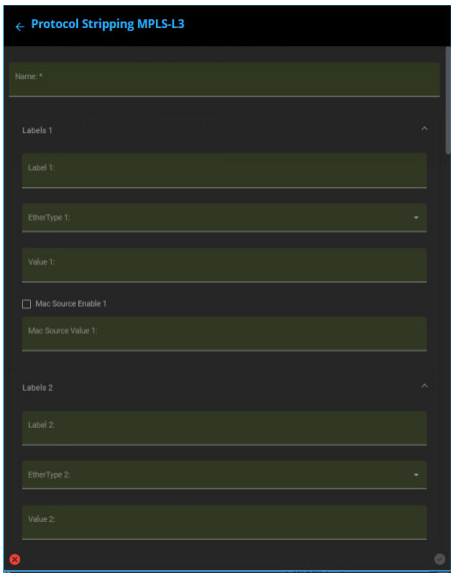
Protocol Stripping port feature set to Stripping.



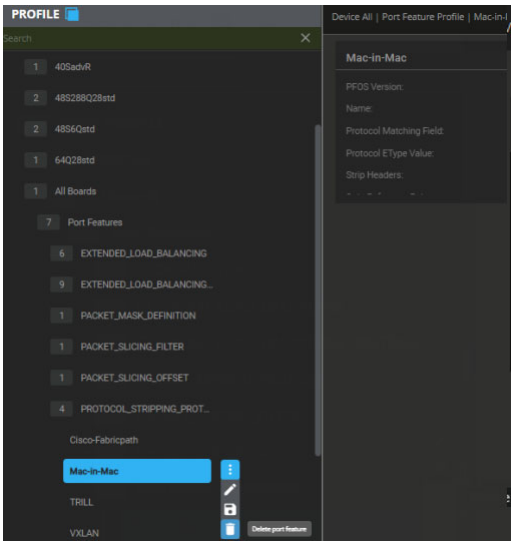
Protocol Stripping port feature with set to Protocol.



Protocol Stripping port feature with set to MPLS-L3.

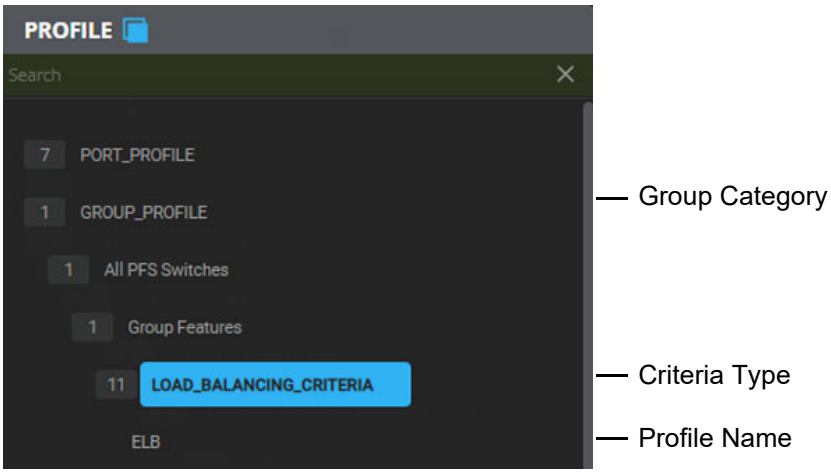


Deleting the Protocol Stripping port feature profile.



Group Profile

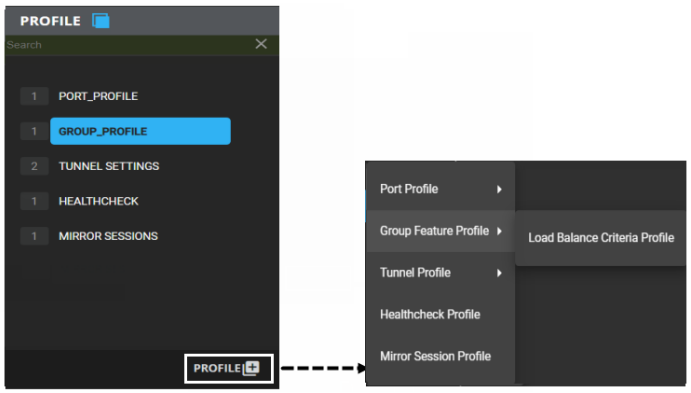
Clicking on Group Profile expands the list of accepted switches by type of switch with associated feature profiles.



Creating a Group Profile

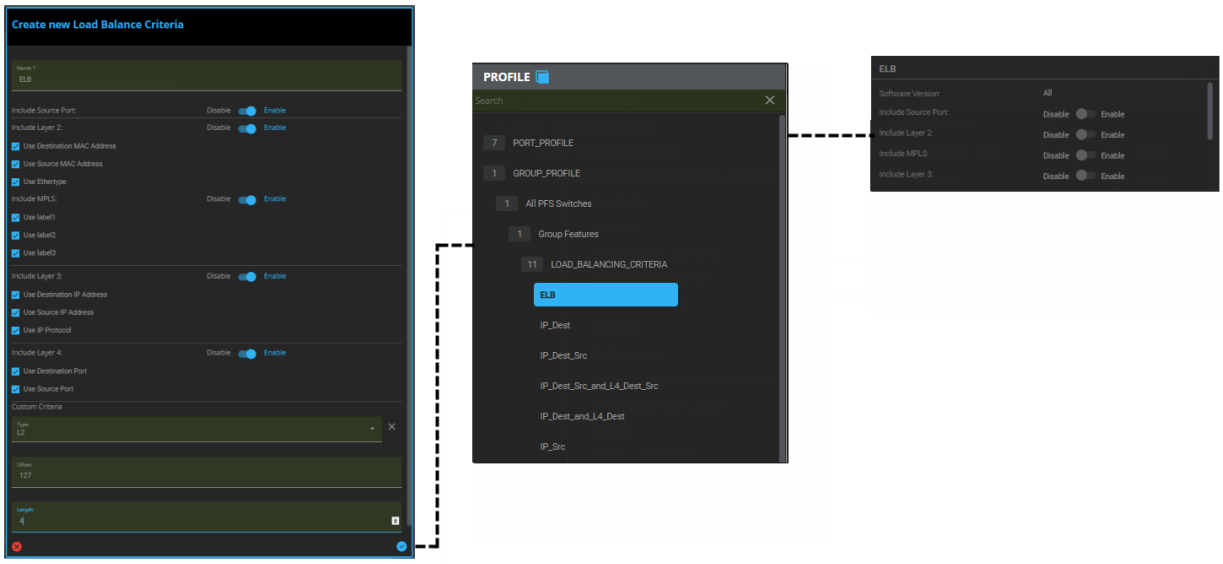
1 From Perspective > Profile, click on **+ Profile**. Select **Group Profile** and **Load Balance Criteria Profile** from the profile menu. The New Load Balance Criteria window displays.

> **Note:** Load Balance Criteria (LBC) Group Profiles are associated to Load Balance Groups on a topology. The default LBC is used unless it is overridden.



2 Enter a name for the profile (56 characters maximum) then select the feature options for the profile; selecting enable for feature selections displays additional options for the feature.

3 Click on the Accept icon to save the new group profile.

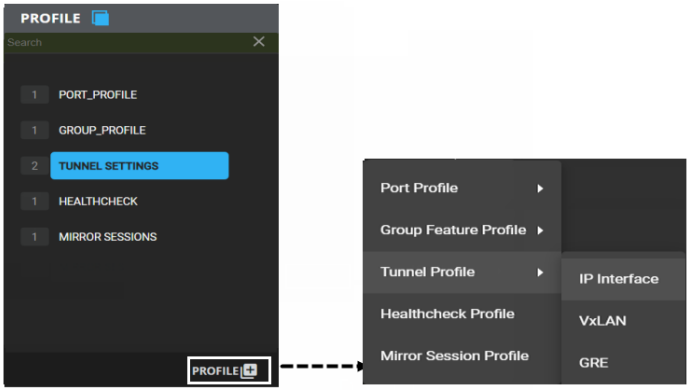


Tunnel Profile

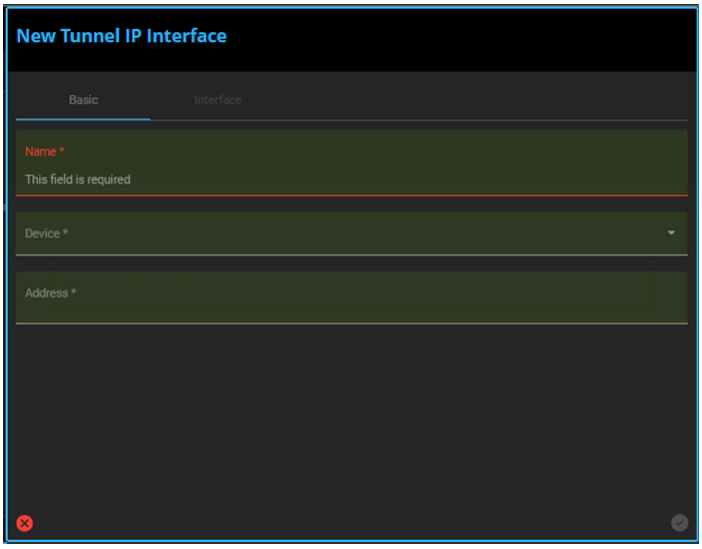
Clicking on Tunnel Profile expands the list of devices/ports with associated feature profiles.

Creating a Tunnel IP Interface Profile

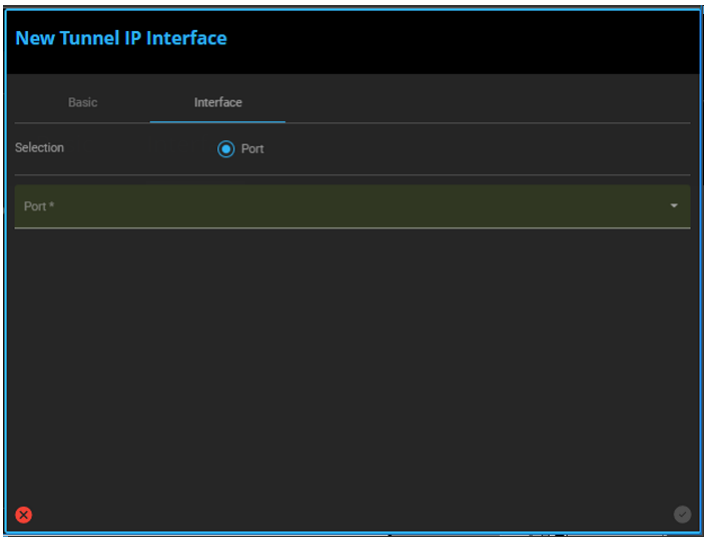
1 From Perspective > Profile, click on **+ Profile**. Select **Tunnel Profile** and **IP Interface** from the profile menu. The New Tunnel IP Interface window displays.



2 In the Basic section, enter a name for the profile (56 characters maximum) then select/enter the feature options for the profile.



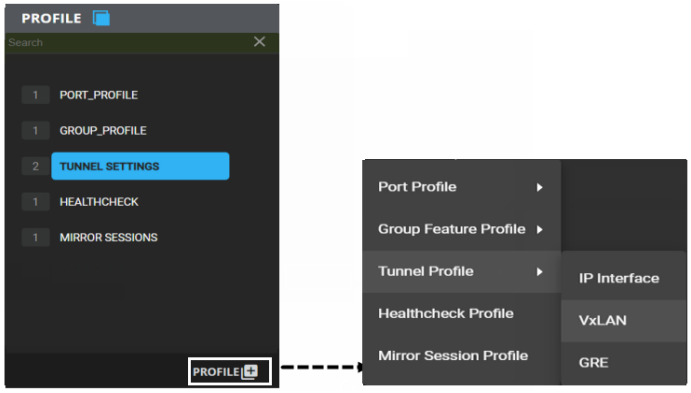
3 In the Interface section, select the port for the profile.



4 Click on the Accept icon to save the new IP Interface profile.

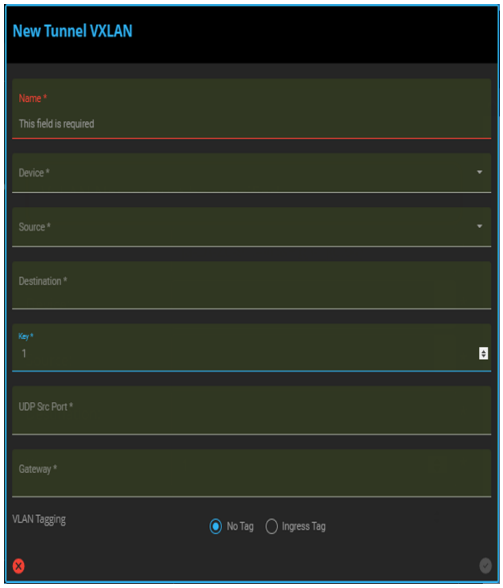
Creating a Tunnel VxLAN Profile

1 From Perspective > Profile, click on **+ Profile**. Select **Tunnel Profile** and **VxLAN** from the profile menu. The New Tunnel VxLAN window displays.



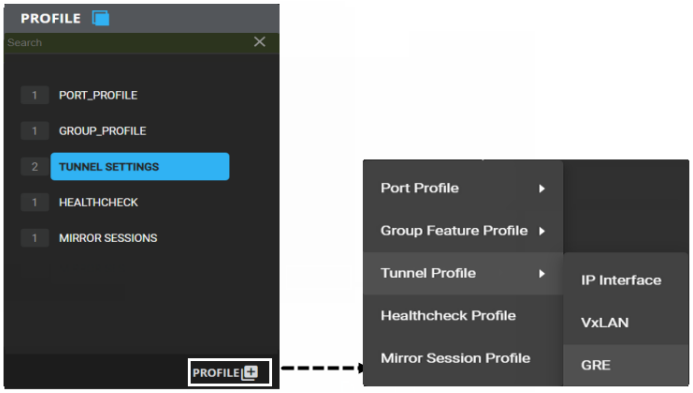
2 Enter a name for the profile then select/enter the feature options for the profile.

3 Click on the Accept icon to save the new VxLAN profile.



Creating a Tunnel GRE Profile

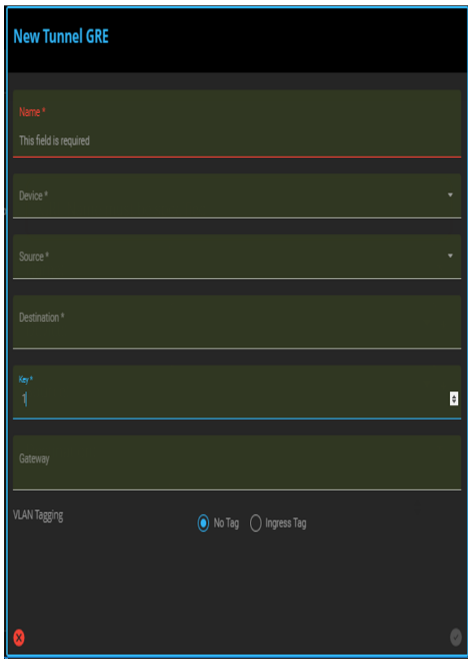
1 From Perspective > Profile, click on **+ Profile**. Select **Tunnel Profile** and **GRE** from the profile menu. The New Tunnel GRE window displays.



2 Enter a name for the profile then select/enter the feature options for the profile.

3 Click on the Accept icon to save the new GRE profile.

Note: On 703x-* switches, the value for the Key Range parameter starts at 0 and other switch models the parameter starts at 1.



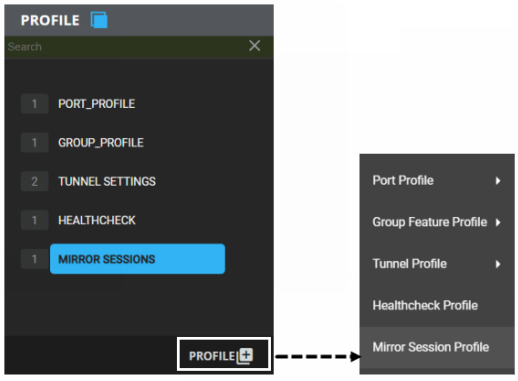
Mirror Session Profile

Clicking on Mirror Sessions expands the list of accepted switches by type of switch with associated feature profiles.

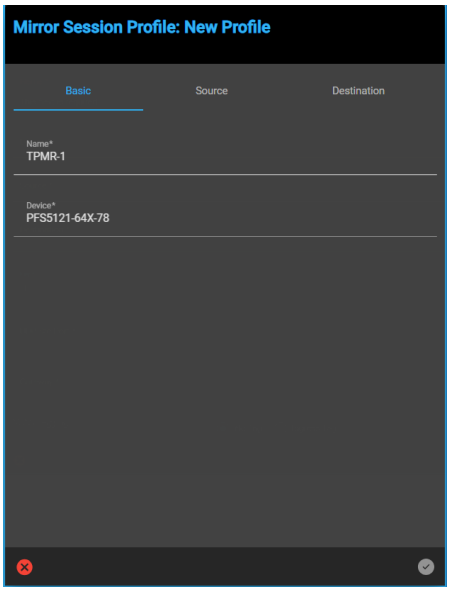
Note: Only a maximum of four (4) mirror sessions are allowed per device.

Creating a Mirror Session Profile

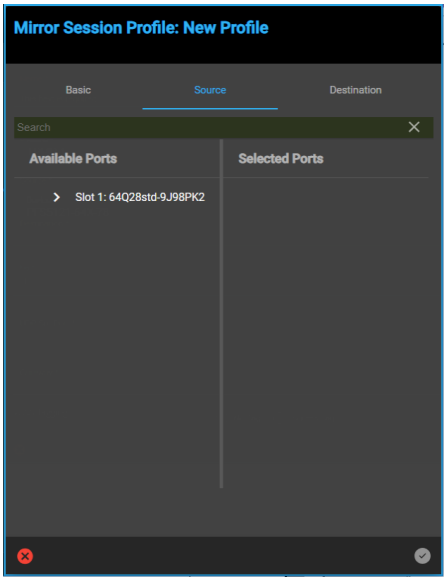
1 From Perspective > Profile, click on **+ Profile**, then select **Mirror Session Profile** from the profile menu. The Mirror Session Profile: New Profile window displays.



2 From the **Basic** tab, enter a name for the profile and select a device.



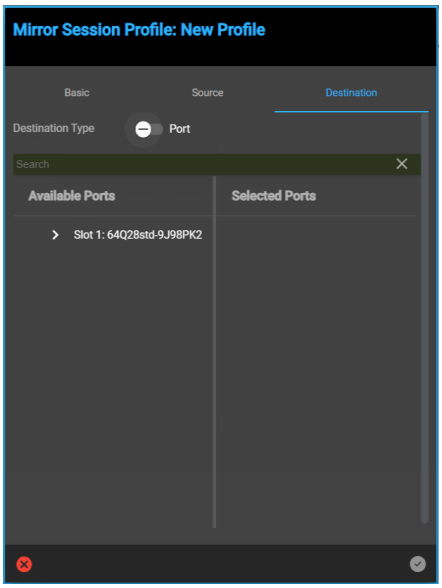
3 From the **Source** tab, select a port from the Available Ports column and drag it to the Selected Ports column.



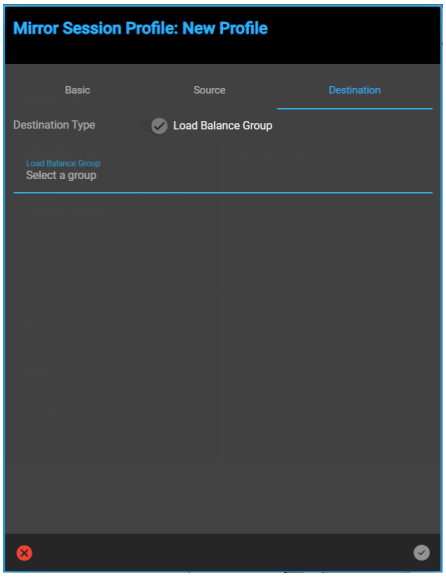
4 From the **Destination** tab, select the destination type: Port or Load Balance Group.

Note: Only one (1) destination port is allowed per mirror session.

If you select a port destination, select a port from the Available Ports column and drag it to the Selected Ports column.



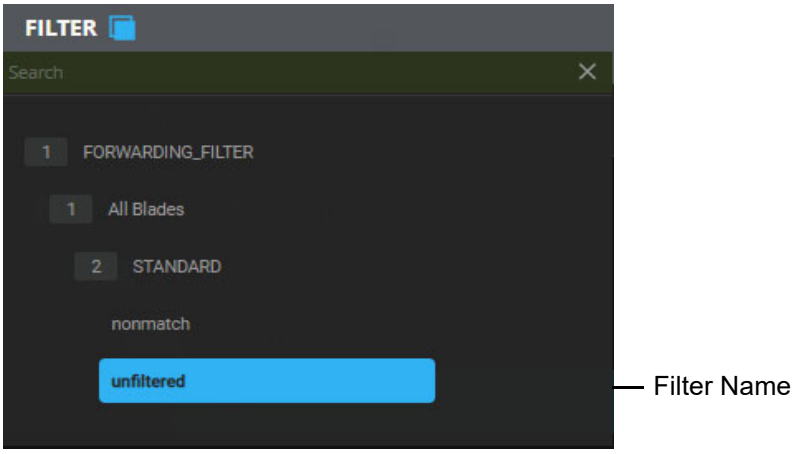
If you select a load balance group, select a group



5 Click on the Accept icon to save the new mirror session profile.

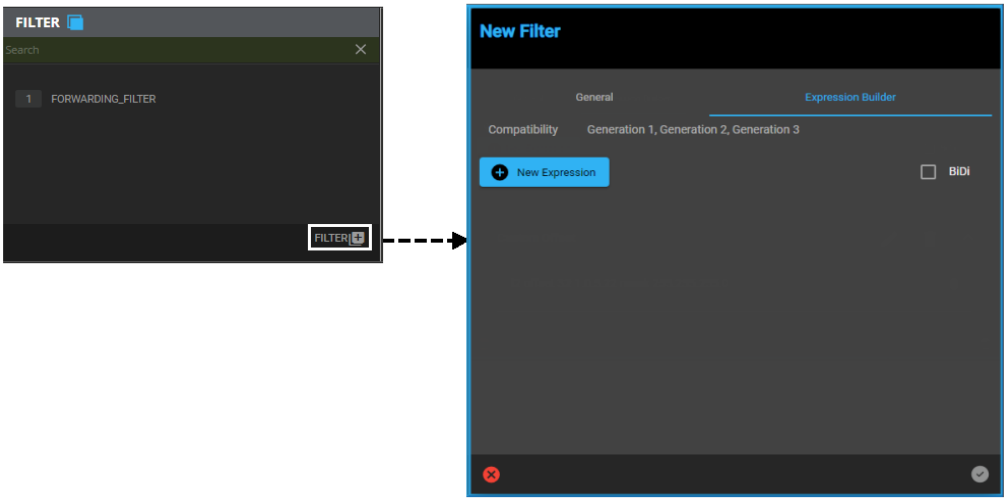
Perspective > Filter

Selecting Filter from the Perspective menu allows creating, editing, and viewing the properties of defined filters available for use when creating network topologies.



Creating a Filter

1 From Perspective > Profile, click on **+ Filter**. On the New Filter > General screen, enter a name for the new filter (56 characters maximum) then click on Expression Builder to continue.



Define the Filter Requirements

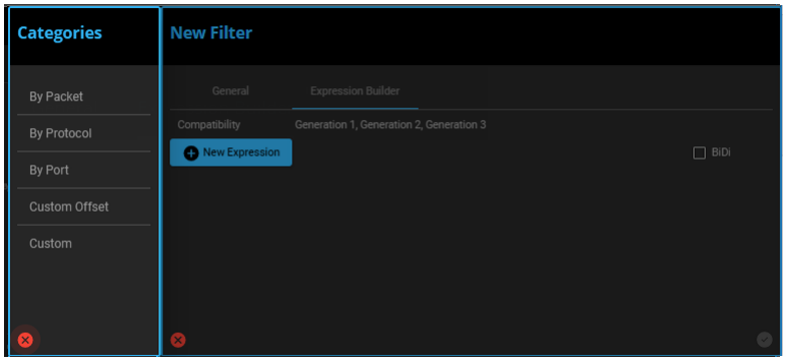
From Expression Builder, click on **+ Expression**. Select from the categories:

- Packet on page 3-79
- Protocol on page 3-81
- Port on page 3-82
- Custom Offset on page 3-82
- Custom on page 3-83

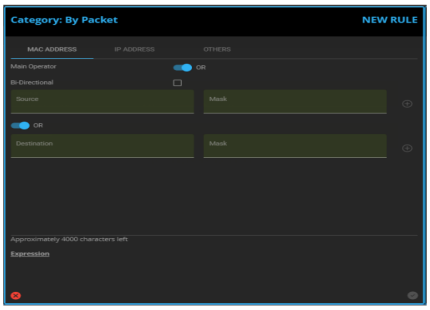
to define the requirements of the filter.

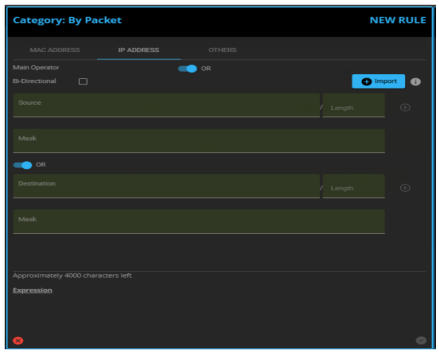
Important: Filter expressions must not exceed a total of 4000 characters.

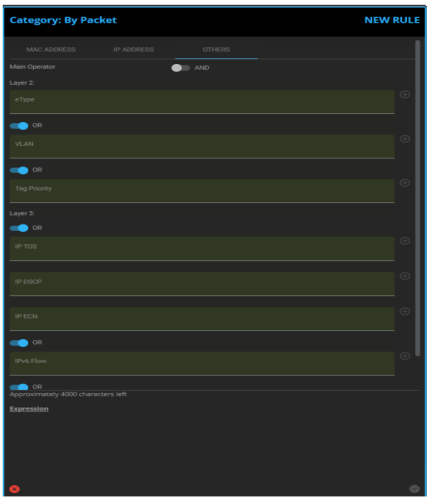
Click on the accept check mark to save the new filter.



Packet



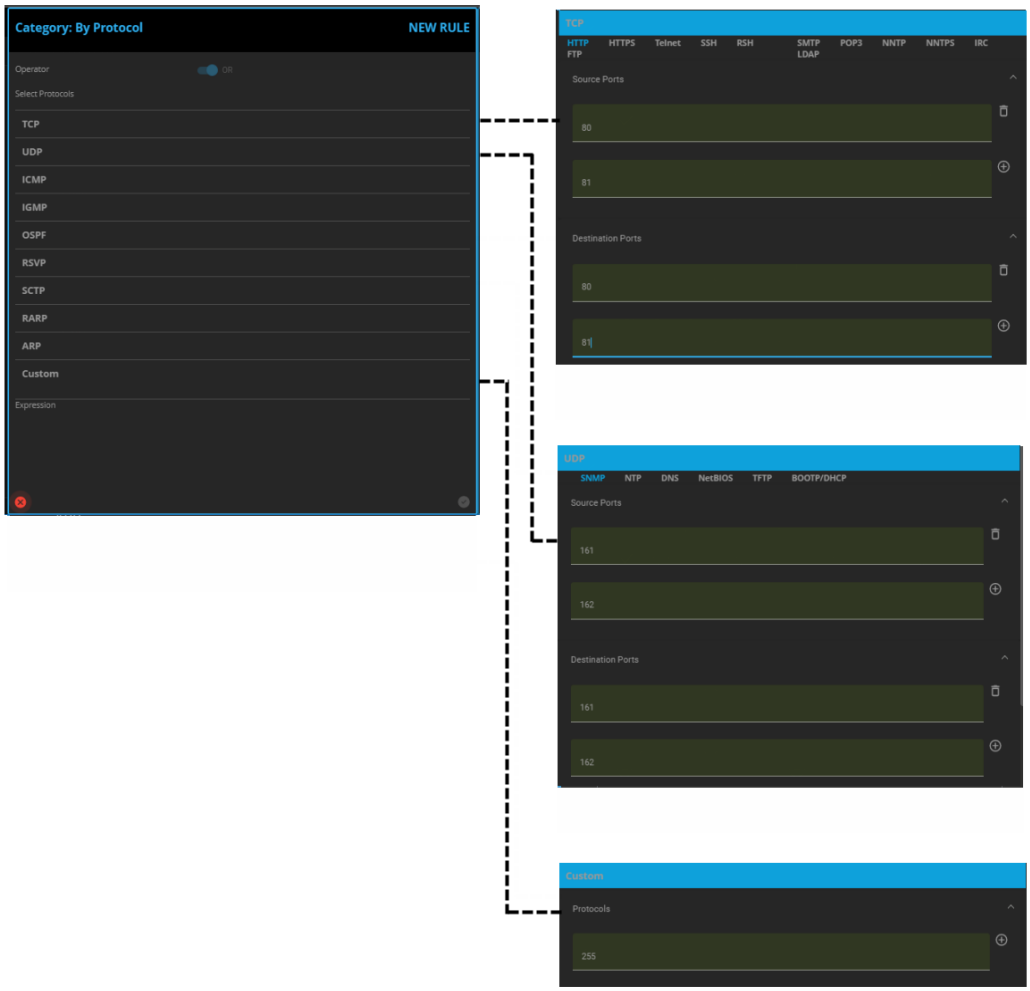




MAC Address		
Operator		Select how to combine source and destination (logical and / or) of MAC address.
Bi-Directional		Enable/disable bi-directional functionality
Source		Ethernet (IEEE 802.3 - Layer 2) source address. Additional addresses can be added as required.
Destination		Ethernet (IEEE 802.3 - Layer 2) destination address. Additional addresses can be added as required.
IP Address		
Operator		Select how to combine source and destination (logical and / or) of IP address.
Bi-Directional		Enable/disable bi-directional functionality
Source / Mask		IP (Layer 3) source address (if an IP packet). Additional masks can be added as required.
Destination / Mask		IP (Layer 3) destination address (if an IP packet). Additional masks can be added as required.
Others		
Operator		Select how to combine the Layer 2 / Layer 3 values (logical and / or).
Layer 2	Etype	Ethernet Type. Refer to the Protocol list to restrict the EType settings to a particular protocol. Additional ranges can be added as required.
	VLAN ID	Enter the IEEE 802.1q VLAN ID (if a tagged packet). Additional ranges can be added as required.
	Tag Priority	Enter the IEEE 802.1p/q priority (if a tagged packet). Additional ranges can be added as required.
Layer 3	IP TOS	Enter the type of service (TOS) class for the filter. Additional ranges can be added as required.
	IP DSCP	Enter the differentiated services code point (DSCP) for the filter. Additional ranges can be added as required.
	IP ECN	Enter the explicit congestion notification (ECN) for the filter. Additional ranges can be added as required.
	IPv6 Flow	Enter the IP Flow field (if an IPv6 packet). Additional ranges can be added as required.

Protocol

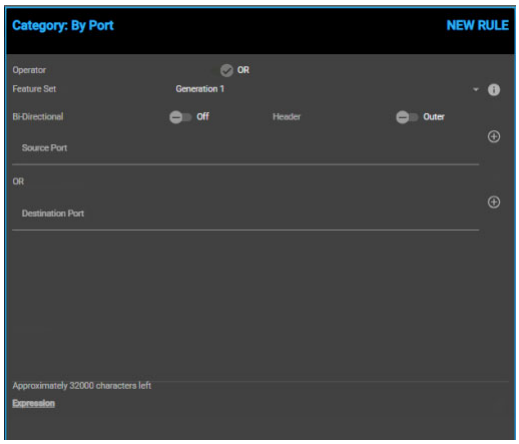
Select the required protocol. Selecting TCP, UDP, or Custom opens an additional option section.



Protocol	Additional Options	
ICMP	IP Protocol 1	
IGMP	IP Protocol 2	
TCP	Shortcut	HTTP, HTTPS, Telnet, SSH, RSH, FTP, SMNP, POP3, NNTP, NNTPS, IRC, LDAP
	Source Ports	Range: 0-65535 Enter port values as required; add (+) or remove (-) port fields as required.
	Destination Ports	
UDP	Shortcut	SMTP, NTP, DNS, NetBIOS, TFTP, BOOT/DHCP
	Source Ports	Range: 0-65535 Enter port values as required; add (+) or remove (-) port fields as required.
	Destination Ports	
RSVP	IP Protocol 46	
OSFP	IP Protocol 89	
SCTP	IP Protocol 132	
RARP	IP Protocol 8035	
ARP	IP Protocol 0806	
Custom	Enter an IP Protocol number between 2 - 255.	

Port

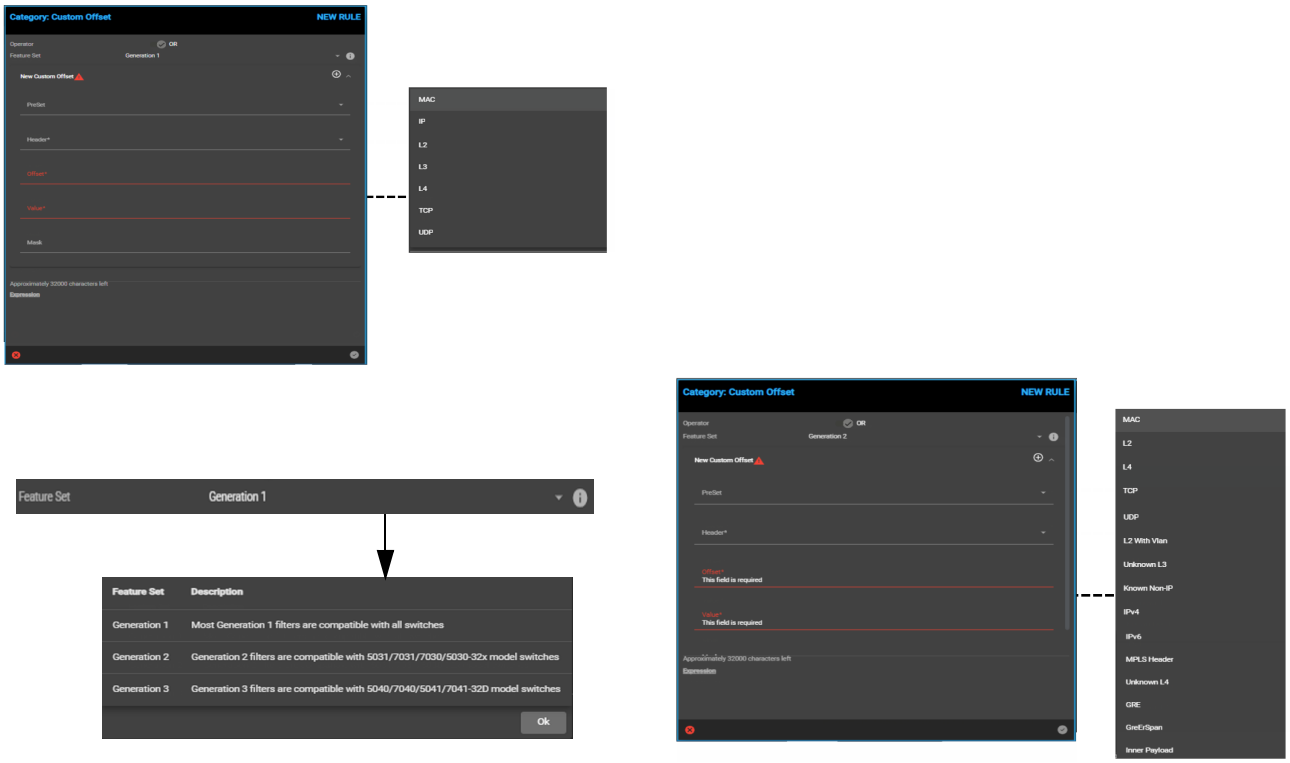
Specify the port settings for the selected protocol. The protocol options vary according to the selected protocol.



Port Settings	
Operator	Select how to combine source and destination (logical and / or) of TCP address
Feature Set	Select Generation 1, Generation 2, or Generation 3
Bi-Directional	Enable/disable bi-directional functionality
Source Port/Destination Port	Range: 0-65535 Enter port values as required; add (+) port fields as required

Custom Offset

Custom offset filtering (often referred to as user-defined filtering) allows you to create a byte filter window beginning at the selected header for comparison with all packets that pass through the filter.

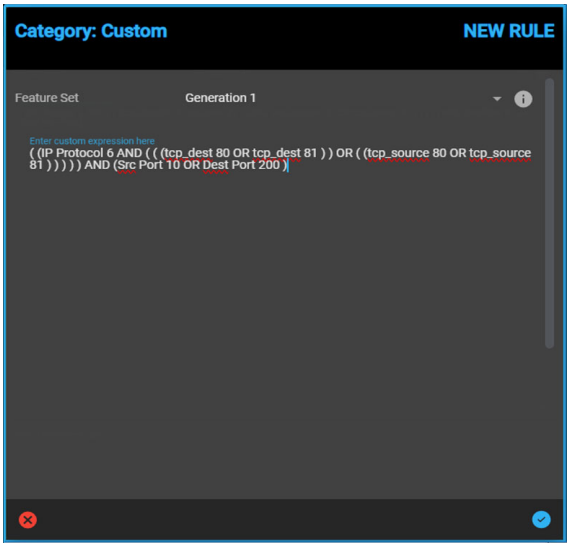


Custom Offset Settings	
Operator	Select how to combine (logical and / or) of TCP address.
Feature Set	Specify with which PFS the Custom Offset filter should be compatible. Generation 1 - Most Generation 1 filter are compatible with all switches. Generation 2 - Generation 2 filters are compatible with 503x/703x model switches. Generation 3 - Generation 3 filters are compatible with 504x/704x model switches.
Presets	GTP Flags, GTP Length, GTP Message Type, GTP Destination IP Address, GTP Source IP Address, GTP TEID, GTP-U Destination IPv4, GTP-U Source IPv4, VN TAG Destination IP, VN Tag Source IP, VxLAN VNID
Header	Gen1 - MAC, IP, L2, L3, L4, TCP, UDP Gen 2 - MAC, L2, L4, TCP, UDP, L2 with VLAN, Unknown L3, Known Non-IP, IPv4, IPv6, MPLS Header, Unknown L4, GRE Gen 3 - MAC, L2, L4, TCP, UDP, L2 with VLAN, Unknown L3, IPv4, IPv6, MPLS Header, Unknown L4, GRE
Offset	Specify an offset from the beginning of the header window with the desired hexadecimal data pattern to be compared to receive packets (range: 0-63).
Value	Valid IPv4/IPv6 address or a value from 0 to 8 hexadecimal digits.
Mask	(Optional) Valid IPv4/IPv6 mask or a value from 0 to 8 hexadecimal digits.

Custom

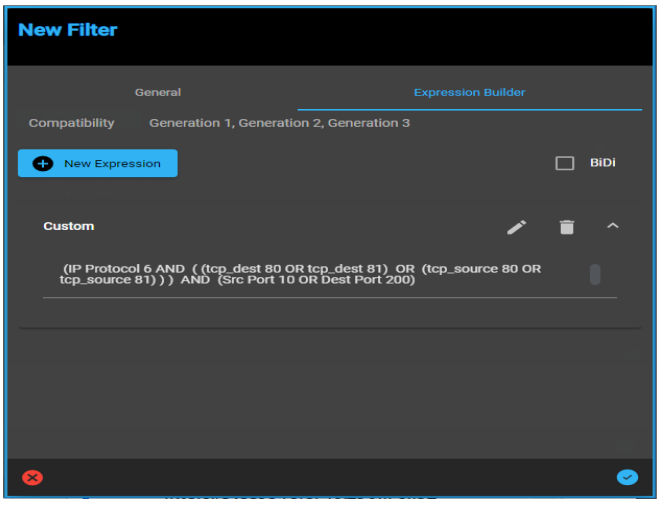
Selecting Custom allows creating more complicated expressions and copying / pasting of pre-defined expressions from other filters.

Important: Filter expressions must not exceed a total of 4000 characters.

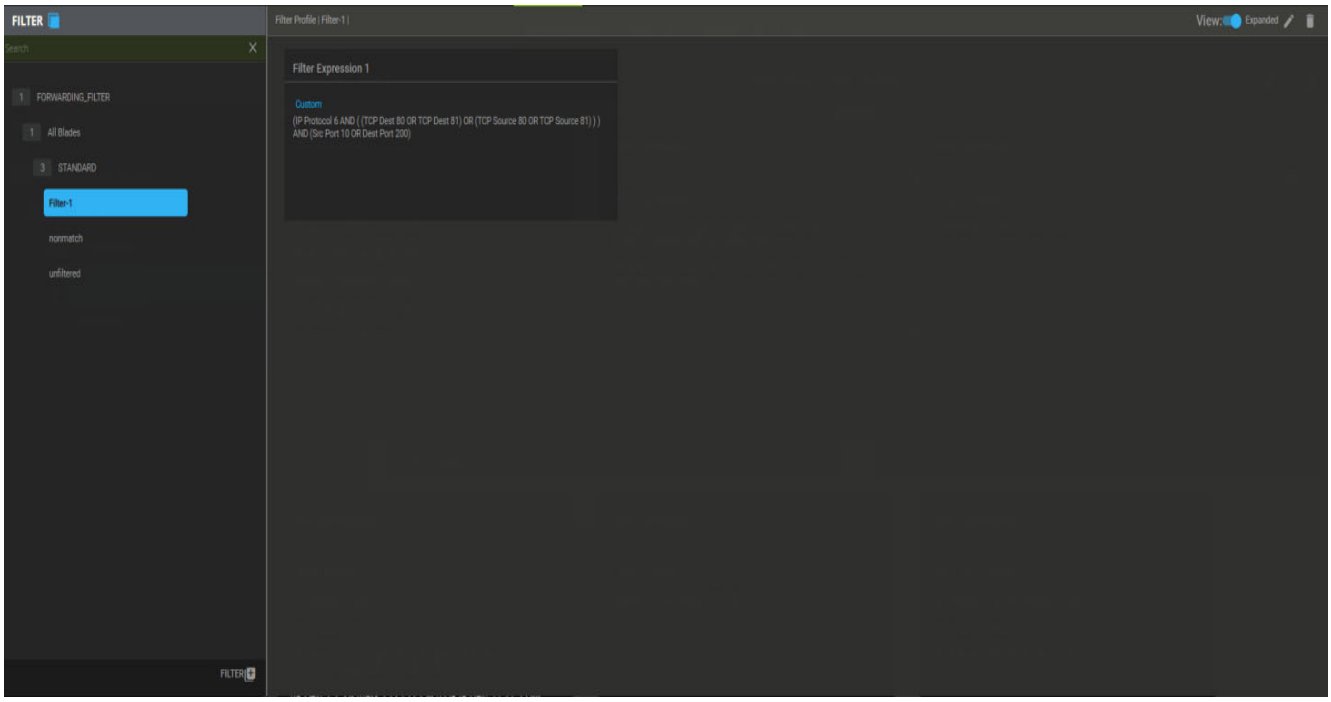


Saving the New Filter

Once the filter values are defined, you can review the defined filter expression from the General > Filter Expression display. Save the new filter by clicking on the Accept icon.

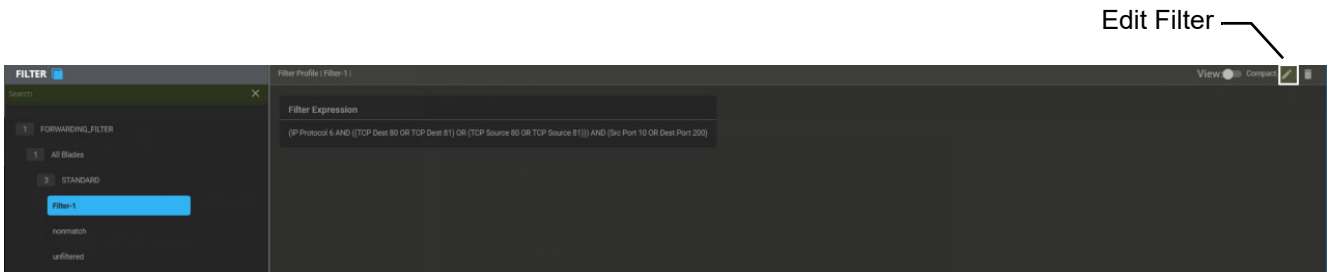


The saved filter is now available in the Perspective > Filter menu. Clicking on the filter version allows viewing the filter properties.There are two views: Expanded and Compact. The Expanded view displays each filter expression separately and the Compact view displays the filter expression as a single expression.



Editing Filter Properties

To edit the properties of a defined filter, first select the filter version then click the edit filter icon on the filter profile screen.



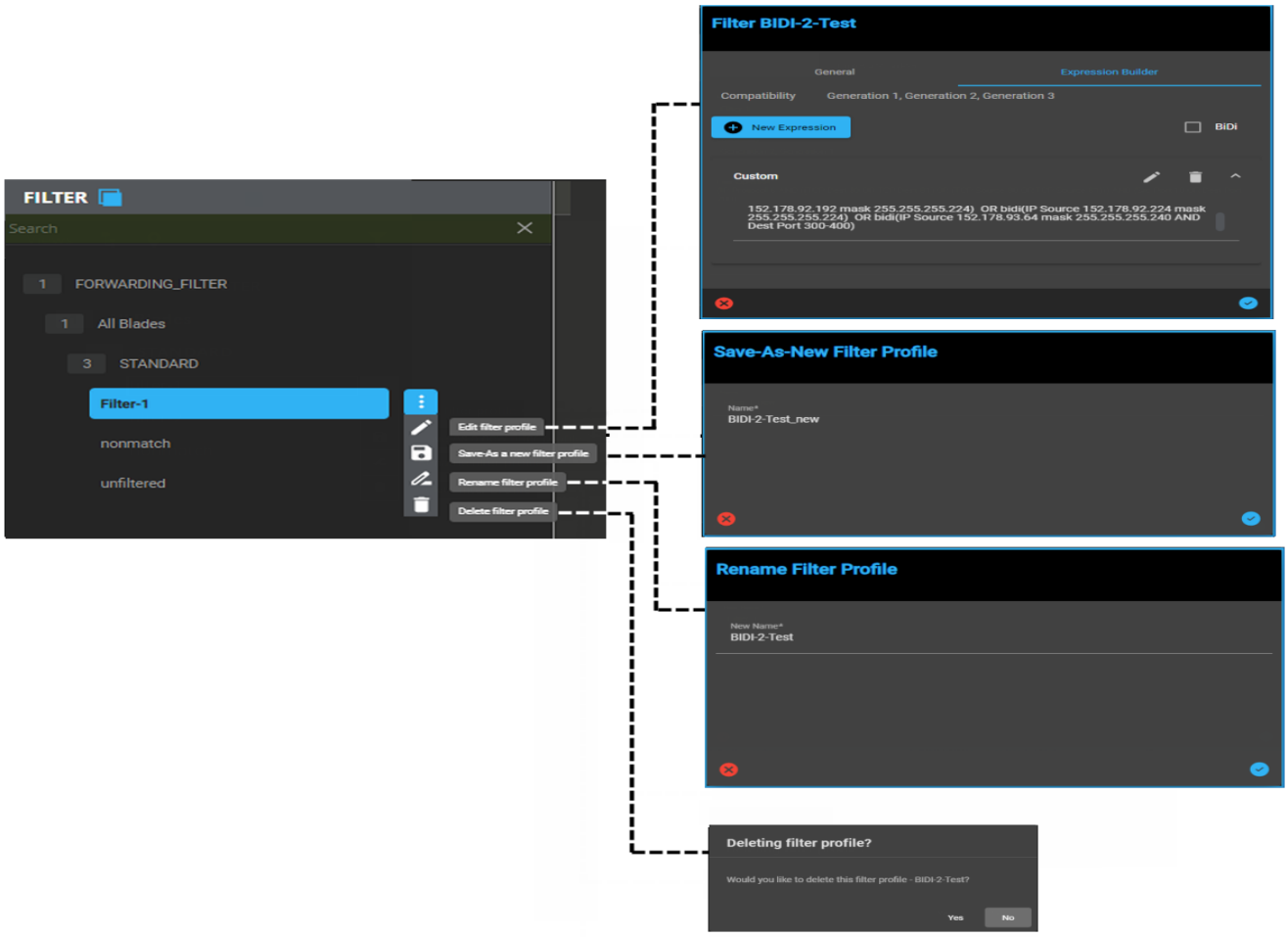
Filter Sub-Menu

Each created filter has a sub-menu with the following tasks:

- Edit Filter Profile
- Rename Filter Profile
- Save-As a new Filter Profile

> **Note:** Save-as can be used to replicate complicated filters, to make a new, similar filter.

- Rename the selected Filter Profile
- Delete Filter Profile



Perspective > Trigger

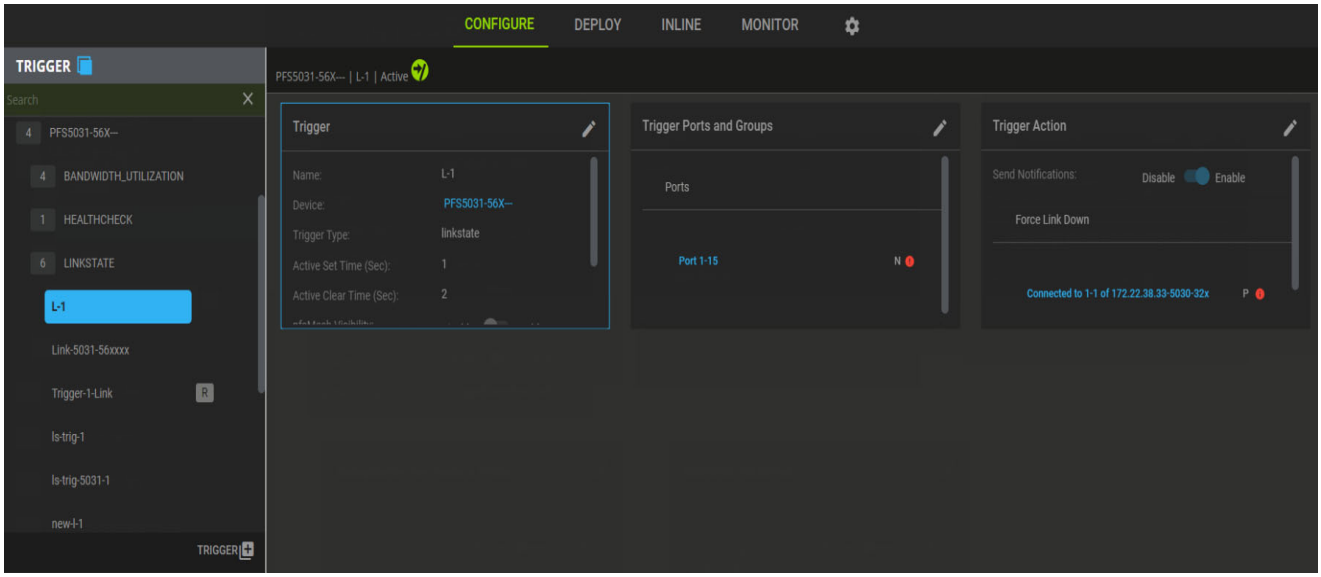
Selecting Trigger from the Perspective menu allows viewing and editing the configuration of trigger policies. Trigger policies allow the user to monitor a set of conditions and take specified actions based on the outcome of the events automatically. This is key for providing robust and highly available packet flow switching fabrics, whether for passive or active monitoring.

The user can monitor the following conditions in order to take some action:

- Link status of one or more ports
- Bandwidth utilization of one or more ports
- Overflow drops of one or more ports
- Health check status of one or more Inline monitor groups
- PPS trigger policy
- Combination of other trigger policies

As a result of one of these conditions, the user can take one or more of the following actions:

- Modify the Traffic Mapping (as defined and configured in Topology)
- Send a notification, which includes sending Syslog messages, SNMP traps, and NETCONF notifications
- Force link down on one or more ports



Timer Settings

Each policy has one of two kinds of timer settings:

Active set time

This option allows the user to identify if the condition is occurring intermittently. When this timer is set, the policy will not become active until the condition has occurred for the user specified interval.

Active clear time

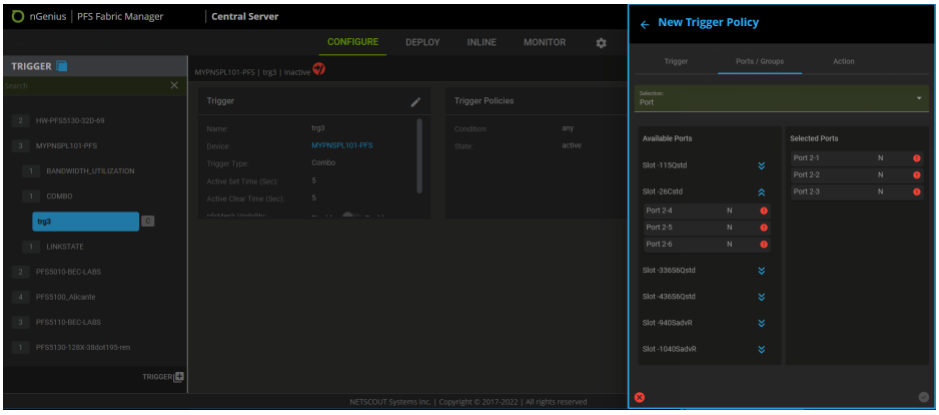
This option complements active set time by allowing the user to identify if the condition is not occurring intermittently. When this timer is set, the policy will become inactive only after the condition has not occurred for the user specified interval.

Select Ports or Groups

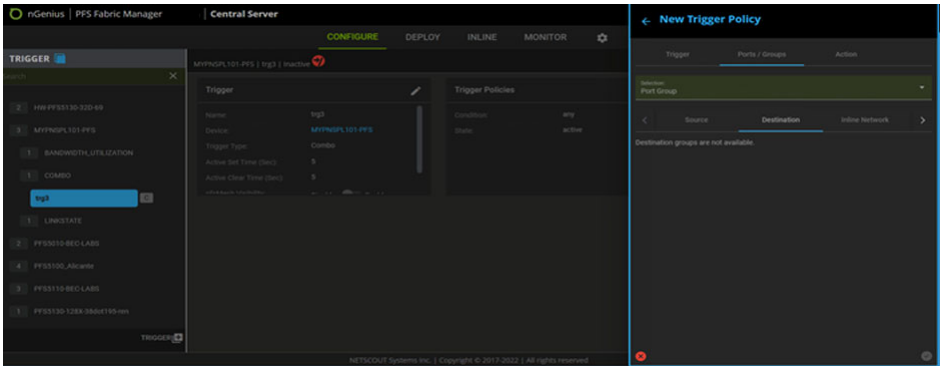
Users can select a list of ports or port groups to monitor for the trigger condition.

- For **Linkstate**, **Bandwidth utilization** or **Overflow** triggers, either ports or port groups can be selected but not both.
- For **HealthCheck** triggers, only Inline Monitor Groups can be selected.
- This option is not relevant to **Combo** triggers.

Select Ports



Select Groups

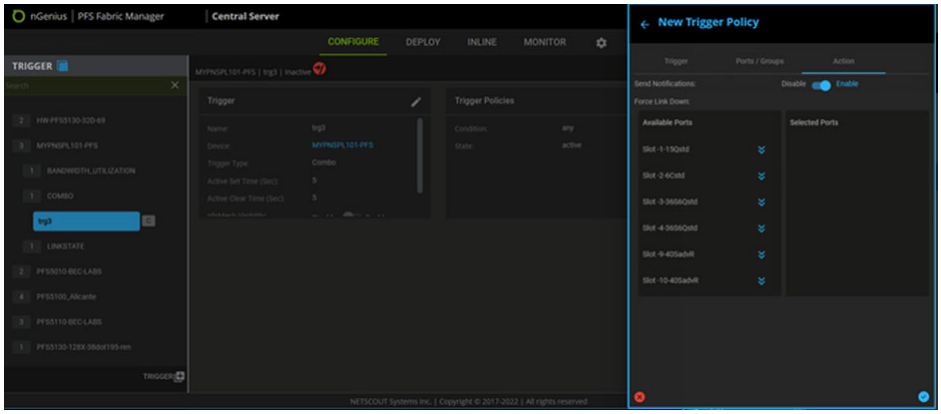


Trigger Actions

Actions can be configured for each trigger policy. When the policy becomes active, any configured actions will be taken. All trigger types support the following options.

Send Notifications

If this option is enabled, a notification will be sent when the policy becomes active. The notification will be sent via any enabled notification channels (Syslog, SNMP, NETCONF).



Force Port Link Down

Users can select a list of ports to force link down when the policy becomes active.

Trigger Types

Each trigger type has it’s own configuration options as described in the following sections.

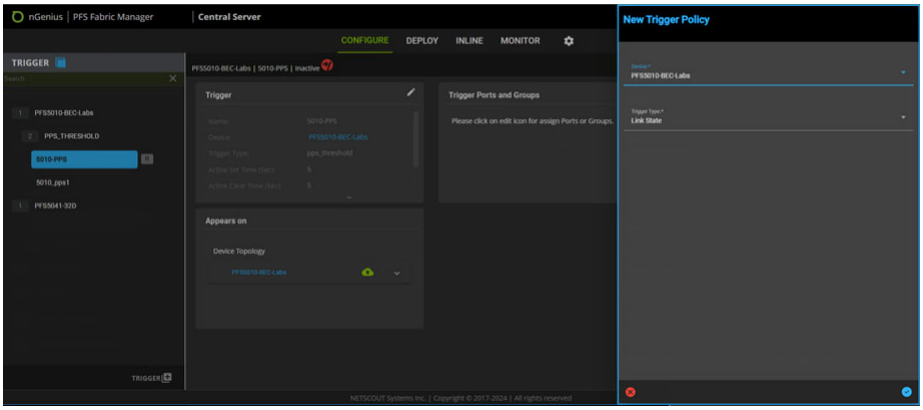
Linkstate Trigger Type

This policy type tests for the port link status of ‘up’ or ‘down’ for selected ports for the specified time (Active set time) to make the trigger active.

Specific Options

Trigger Link - select which link state condition activates the trigger policy

- Any Online - Any of the selected links are up
- Any Offline - Any of the selected links are down
- All Online - All selected links are up
- All Offline - All selected links are down

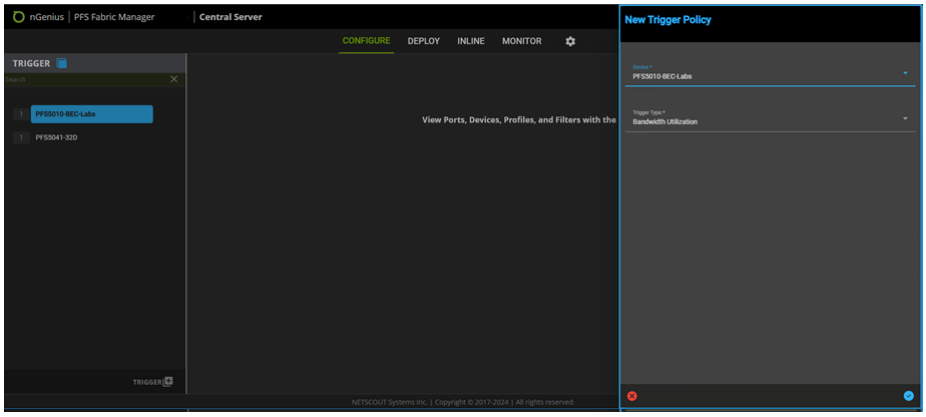


BandwidthUtilization Trigger Type

This policy type tests for utilization of at least one selected port outside of the defined range for the specified time (Active set time) to make the trigger active. Once it is active, the trigger will only go inactive when all ports are in the normal range for the specified time (Active clear time).

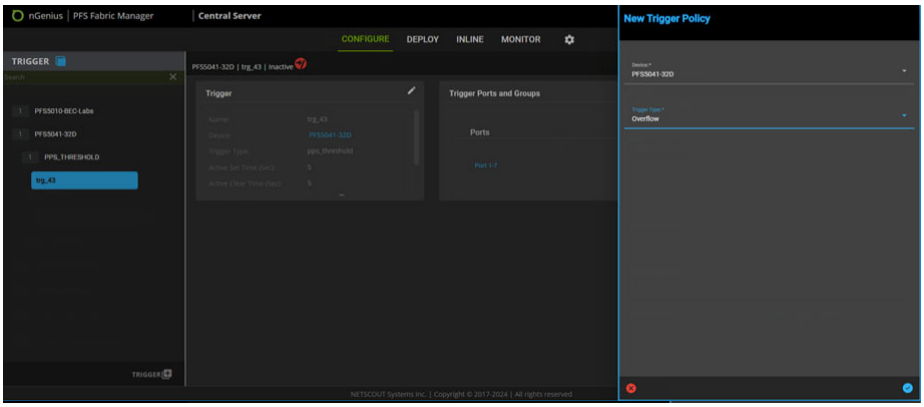
Specific Options

- Direction - only the specified direction will be monitored
  - RX
  - TX
- Min - The minimum level threshold below which the trigger gets activated
- Max - The maximum level threshold above which the trigger gets activated



Overflow Trigger Type

This policy type tests for port overflow by monitoring the port overflow counters. Whenever a port overflow is detected for any selected port for the specified time (Active set time), the trigger becomes active. This trigger type has no specific options.

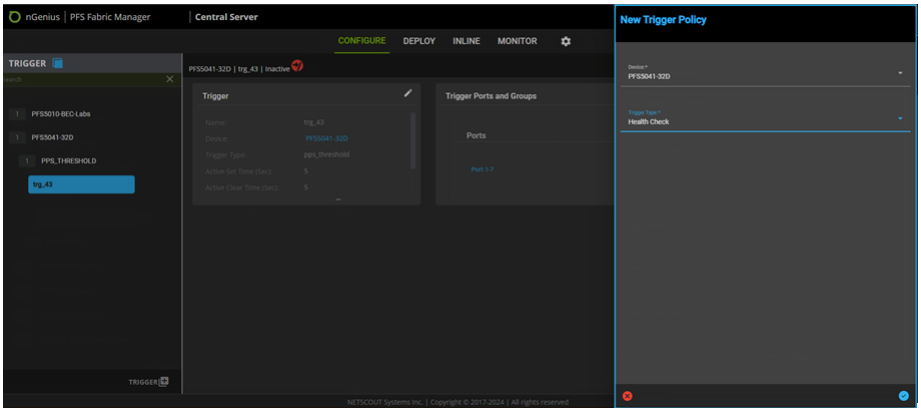


HealthCheck Trigger Type

This policy type tests for the health-check status of selected Inline-monitor port groups. HealthCheck trigger policies allow logical link down of the port pairs in an inline monitor port group when health check fails.

Specific Options:

- Trigger Link - select which health check condition activates the trigger policy
  - Any - Any of the selected port pairs have a failed health check
  - All – All selected port pairs have a failed health check



Combo Trigger Type

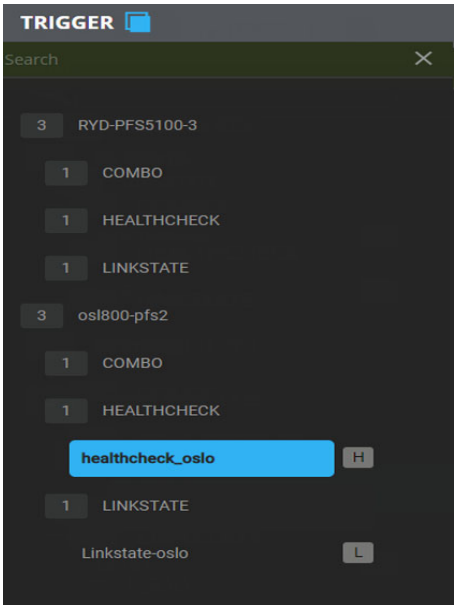
This policy type monitors the state of other selected trigger policies.

Specific Options:

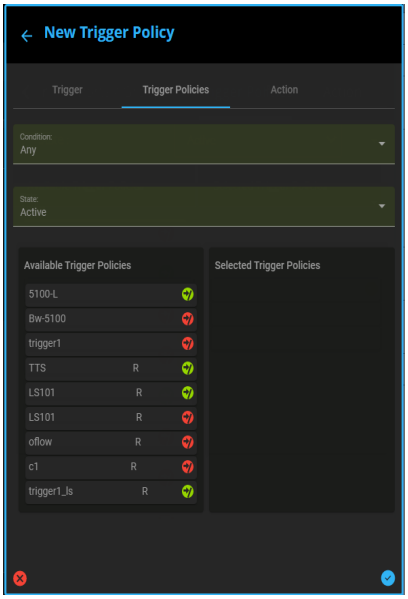
- Condition – select which trigger policy condition activates the parent trigger policy
  - Any – any selected trigger policy is in the below state
  - All – all selected trigger policies are in the below state
- State – select which trigger policy state activates the parent trigger policy
  - Active – selected trigger policy is active
  - Inactive - selected trigger policy is inactive
- Remote Trigger Policies
  - Lists the triggers learned via pStack and pfsMesh-enabled triggers defined on other managed switches.

Note: The listed pfsMesh-enabled triggers are not necessarily currently visible/accessible via pStack.

  - pfsMesh visible triggers are designated with an "R" to the right of their name in the perspective window.

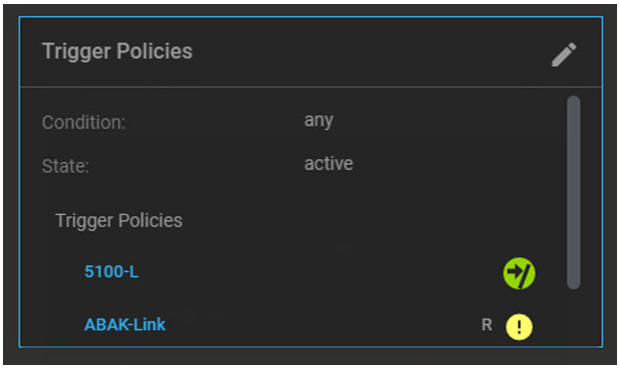


- The “Available Trigger Policies” tab will list the local and remote triggers. Only remote triggers will display the “R” designator.

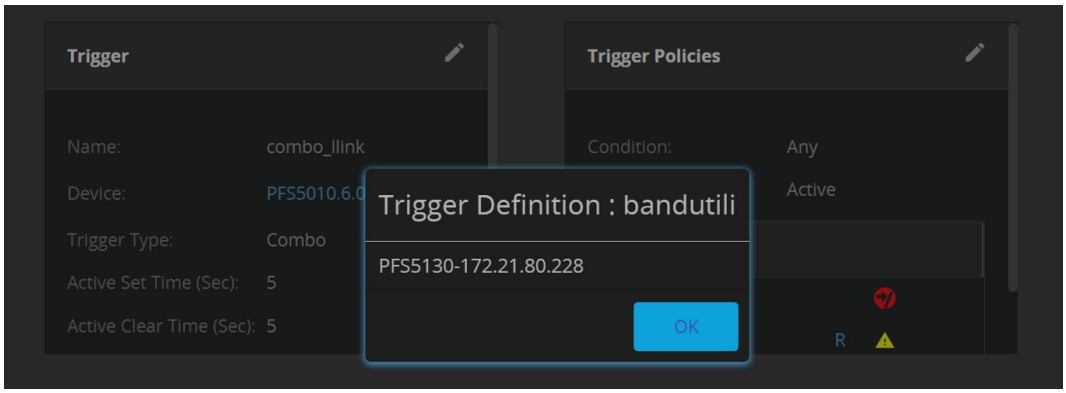


– View Combo Trigger

- Displays additional details of the remote trigger.
- If the servers are not connected via pStack, the remote trigger will be marked as “Not visible via pfsMesh”, when you hover over the trigger name (with the warning icon), and the trigger status will be hidden.

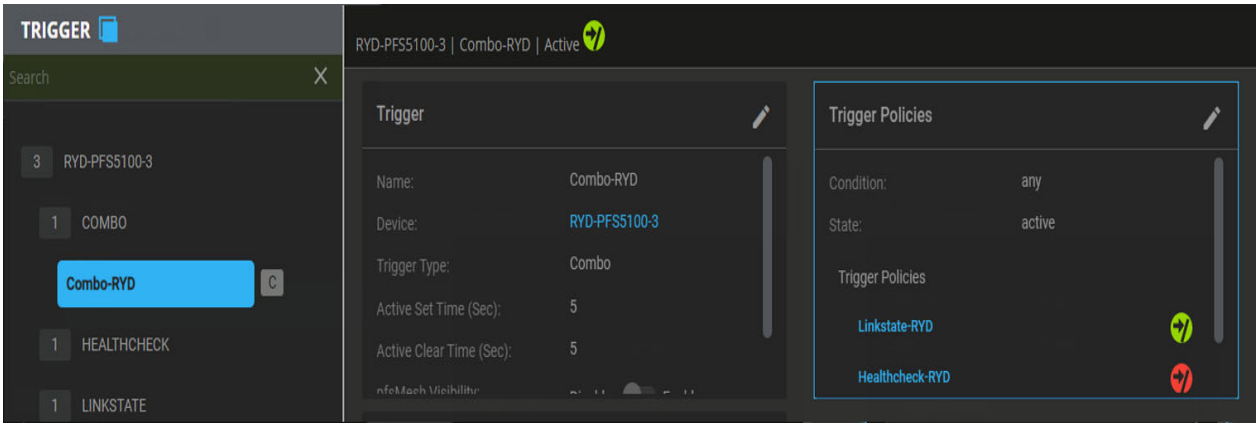


- Clicking on the missing remote trigger name will display the possible trigger reference from the managed switches. From the pop-up dialog box, you can navigate to the respective trigger's view page.



- If there is no possible reference, the message "This remote trigger policy not found on any managed device" will be displayed.

- If the pStack connection is stable, the remote trigger will be displayed with the trigger status.



- Clicking on the trigger name will display the view page of the respective trigger policy.

pfsMesh Option

The user can configure whether the trigger is visible to all nodes in pfsMesh (remote node).

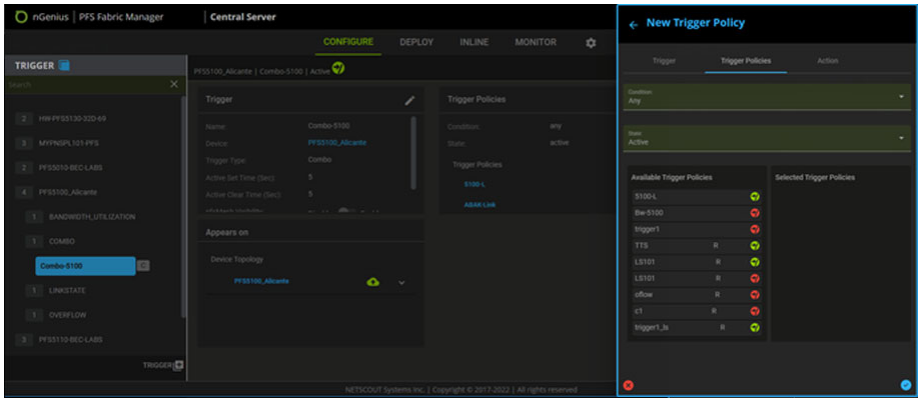
- Disable: the trigger is visible only to the node on which it was created.
- Enable: the trigger is visible to all nodes in pfsMesh.

Notes:

- Only 16 triggers per PFS can be configured as pfsMesh enabled.
- A combo trigger can be configured as "pfsMesh enabled" only if its profile does not contain any remote trigger profiles.

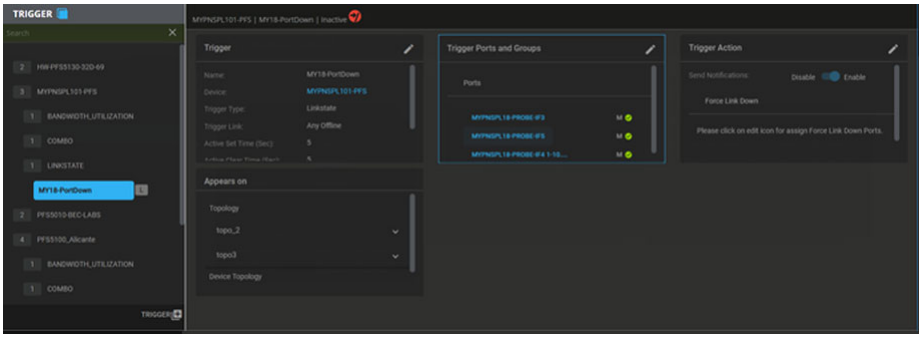
Select Trigger Policies

Users can select one or more trigger policies to be monitored for the defined condition.



Configuration

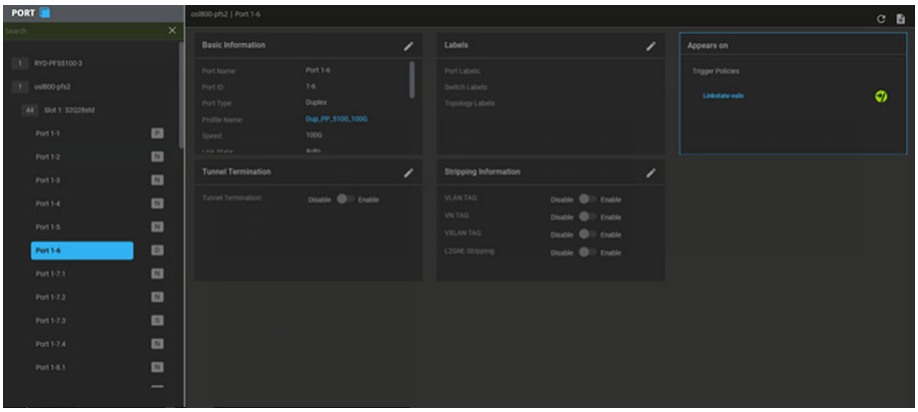
Users can manage Trigger policies from the Configure LifeCycle perspective.



Note: When a user deletes a policy which is used on topology, a warning is displayed. If none of the topologies is published, the user can confirm and proceed. However, if the policy is used in published connections, it cannot be deleted.

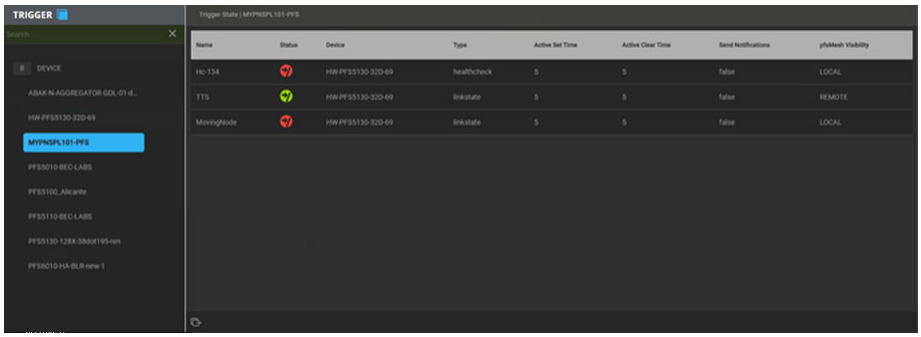
Port Link State

From the port view in the Configure Lifecycle perspective, any trigger policies that reference a selected port should be listed in order to help users understand the link state and navigate through related configuration screens.



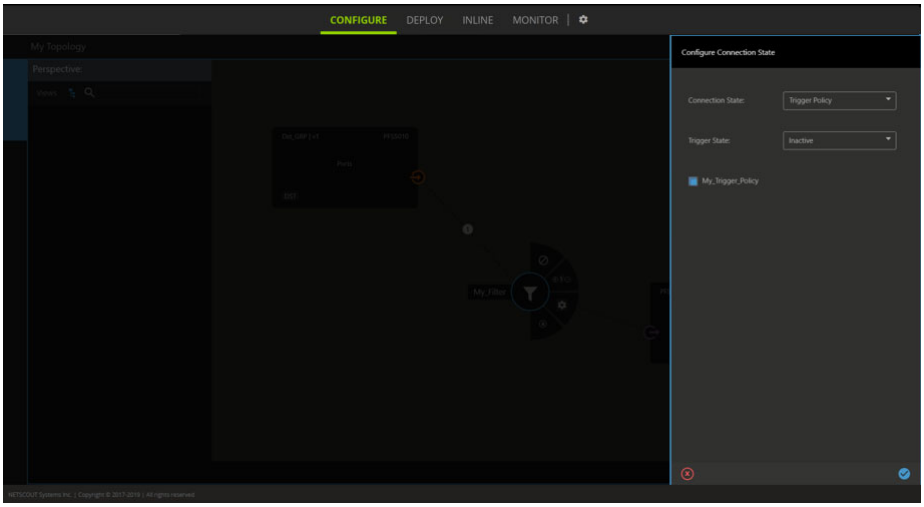
Monitoring

From the Monitor Lifecycle perspective, users can view a paginated table of all the trigger policies with common information and status.



Topology

For each connection on a topology, users can select a connection state. The configured connection state can be enabled, disabled or bound to a trigger policy. Changes to the connection state configuration on a topology will require a new publication, similar to filter assignment. The connection state configuration cannot be changed on a published topology.



After a trigger policy is assigned to a topology, the active connection state (enabled or disabled) will be driven by the trigger state (active or inactive). The active connection state is visualized on the topology for each edge.

Disabled connections will be dashed and when a trigger policy is assigned, an icon will decorate the filter node. If the policy is active, the icon will be green and if the policy is inactive, the icon will be gray. When a configured trigger policy is missing, the icon will be red.

Publication and Learning

Publication

With other configuration areas, for example port feature profiles (application libraries), the profile is not published until it is used. In addition, the profile will be unpublished when it is no longer used.

This behavior is driven by the portability of some profiles across devices. Filters, Port Features and Load Balance Criteria can be used on multiple devices. Even port groups behave in the same way, although they are device specific. This bypasses constraints on the number of port groups per device, while allowing for Fabric Manager features, like group versioning.

Trigger policies break this pattern and instead behave similarly to switch configuration. When a policy is saved, it is immediately published to the device. Trigger policies do not support versioning. When the policy is deleted, it will be unpublished as well. Changes to trigger policies are committed directly to the device.

If a device is disconnected from an NMS (Fabric Manager central server) than any trigger policies belonging to that device cannot be changed from the central server.

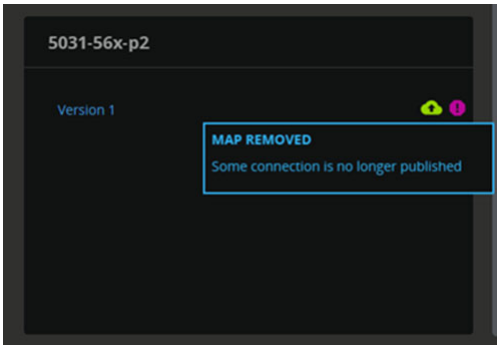
Learning

When trigger policy is added, removed or changed through some PFOS channel directly (Web UI, CLI, NETCONF) while Fabric Manager is running, than the changes are learned in near real time by the managed devices and pushed to any managing NMS.

Initial learning imports trigger policy configuration from PFOS. This process was designed to learn configuration after first install and has limitations. Configuration that is removed from PFOS while Fabric Manager is installed but not running is not be subsequently removed from Fabric Manager. For example, if a trigger policy is removed using the CLI while Fabric Manager is not running, the trigger policy is not deleted from Fabric Manager when it starts again.

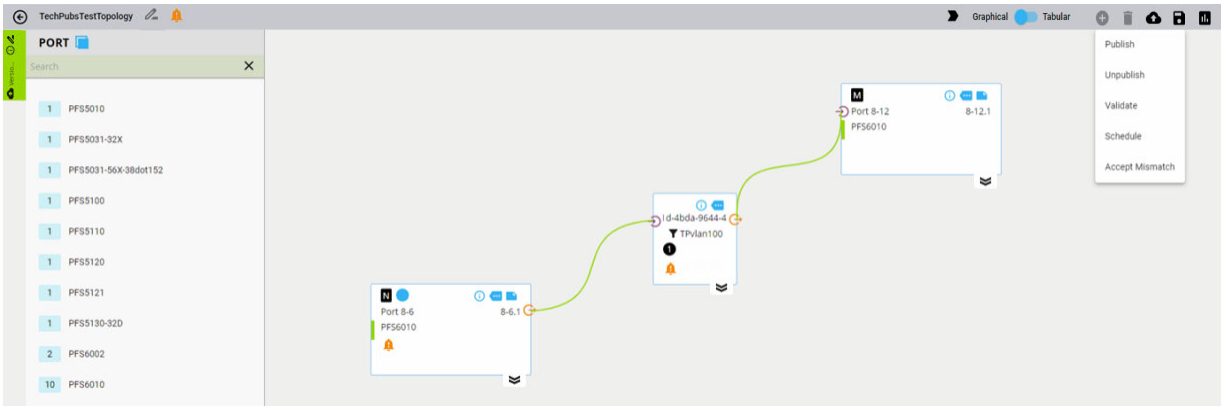
The same limitation applies to the NMS. When a device is centrally managed, then removed from management and not deleted from the central server and configuration is removed from the device in stand-alone mode, the changes are not properly learned to the NMS or when it is moved back to managed.

When a published topology’s flow maps are deleted from PFOS, the PFF Fabric Manager learns that the map or maps part of the user topology have been removed from PFOS (either manually from CLI or WebUI) and a decorator icon is displayed for the deleted map.



Topology Mismatch

When the current state of PFOS is out of sync with any published topologies, those topologies display an indicator of some mismatch. A new mismatch type is required to show when traffic map trigger policy configuration is out of sync with any published topology. For example, if a traffic map is referenced by a topology and the map is changed to disabled through the PFOS CLI, the topology must show a mismatch indicator.



In the case of this type of mismatch, a new workflow must be handled. In 6.0.5 when a topology is mismatched, it can be republished to resolve the issue. However, if the trigger policy is deleted from the CLI after the map is changed to disabled, the policy is immediately removed from Fabric Manager. In this case, it cannot be published and the user must version or unpublish the topology.

A Precedence Warning Indicator is displayed when the user precedence is not set correctly (such as if a Device topology is saved as a User topology in NMS), in this case by default all precedence would be set to 0 and needs to be corrected. It indicates that the topology is not published in the order defined by the precedence.

Accept Mismatch Workflow

When changes are made to PFOS configuration, from an out of band interface, and those changes conflict with a published topology, the topology is decorated with information about the mismatch.

In addition to the pre-existing option to re-publish the topology, users can now accept the changes. Accepting changes on a mismatched topology will create a new topology version with those changes. The new version is automatically published.

Chapter 4
Deploy Lifecycle

This chapter describes Device Topologies and how to create passive monitoring topologies, either from scratch or from imported PFS configuration (on Device Topologies), in PFS Fabric Manager.

Topology Types

There are two types of topologies in the Deploy Lifecycle of PFS Fabric Manager: User topologies and the special (read-only) Device topologies.

Users can now toggle between tabular and graphical views from the topology canvas.

For published topologies, including any device topology, both the tabular and graphical views are read only. On any unpublished topology, changes can be made from either the graphical or tabular view. Traffic map and port configuration can both be changed from the tabular view. When a user makes changes from the tabular view, layout values (node coordinates) will be auto-generated for the graphical view.

Connections or traffic maps can be exported from any user or device topology (published or unpublished) to a new or existing topology version. With the graphical topology, all connections are exported; the tabular topology also allows a subset of the connections to be exported.

User Topologies

User topologies are where users establish connections or traffic maps which move traffic from port to port (or from PFS to PFS) within the monitoring network.

User topologies may contain traffic maps from one or many PFS. Organizing traffic maps or connections into topologies depends on how the user wishes to organize the connections. Possibilities include creating topologies for all the connections in a datacenter, a floor in data center, or per user or per group.

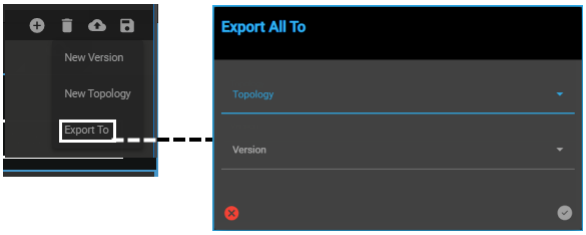
Device Topologies

Device topologies are special topologies which display all the published traffic maps or connections for specific device. Clicking on a device in the Active Devices window, located on the main Deploy screen, displays the device topology. The connections may have been published from PFS Fabric Manager or learned from the device. The topologies are auto-rendered and cannot be directly modified in the Device Topology.

Users normally do not use the Device Topology except when importing configuration from a PFS which was recently added to the Central Server.

Saving Imported Traffic Maps as User Topologies

You can save the current switch topology as another editable, published topology by selecting **Export To > New Topology**.



This new topology, can be modified and published just like any other user topology.

However, it is highly recommended that, unless the configuration has only a few traffic maps, a device's traffic maps should be split among multiple user topologies. See User Topologies on page 4-1for information on how to ideas on organizing traffic maps among user topologies.

The following procedure is the recommended way to import a PFS' existing configuration into multiple user topologies for normal day-to-day use in PFS Fabric Manager.

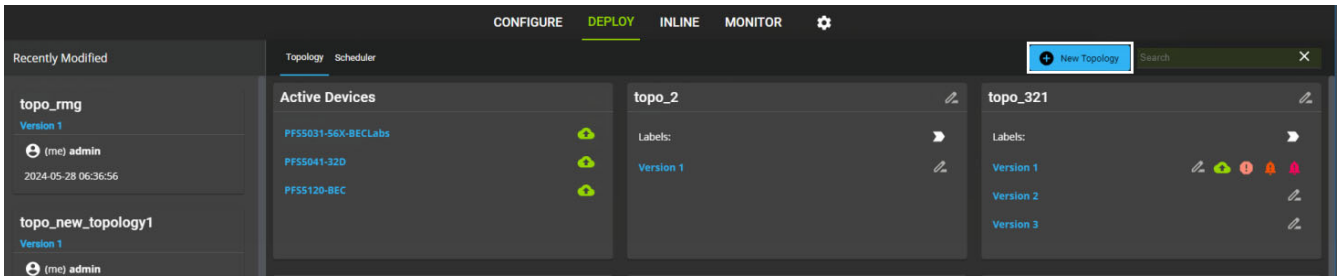
1. Open the Device Topology of the PFS whose configuration should be imported.
2. Switch to the tabular topology view (see Topology > Tabular View on page 4-30 for information on graphical vs tabular topologies).
3. Select one or more traffic maps to be exported to a user topology.
4. Perform an Export To operation to export the selected traffic maps to a new or existing user topology. Set the **Open Selected Topology** option to **No**, so that you will remain on the Device Topology.
5. Modify the traffic map selection to select the traffic maps to save to the next user topology, deselecting the maps already exported, selecting new traffic maps to export.

6 Repeat steps 4-5 until all traffic maps on the Device Topology have been exported to user topologies.

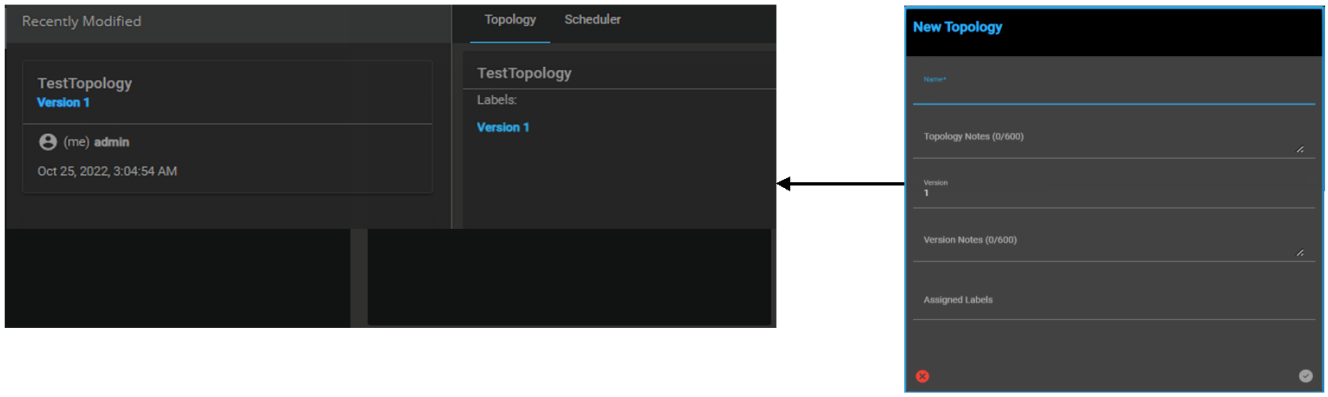
7 Publish any unpublished user topologies to which traffic maps were exported in the steps above. User topologies that were created in step 4 will already be published; existing user topologies that were selected in step 4 will not be published.

Create a New Topology

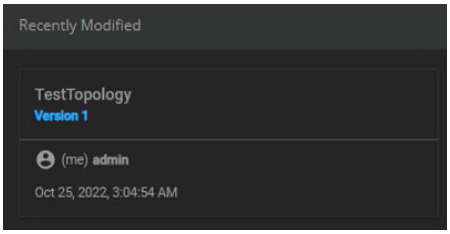
From the interface screen, select Deploy then click on New Topology - a New Topology screen displays.



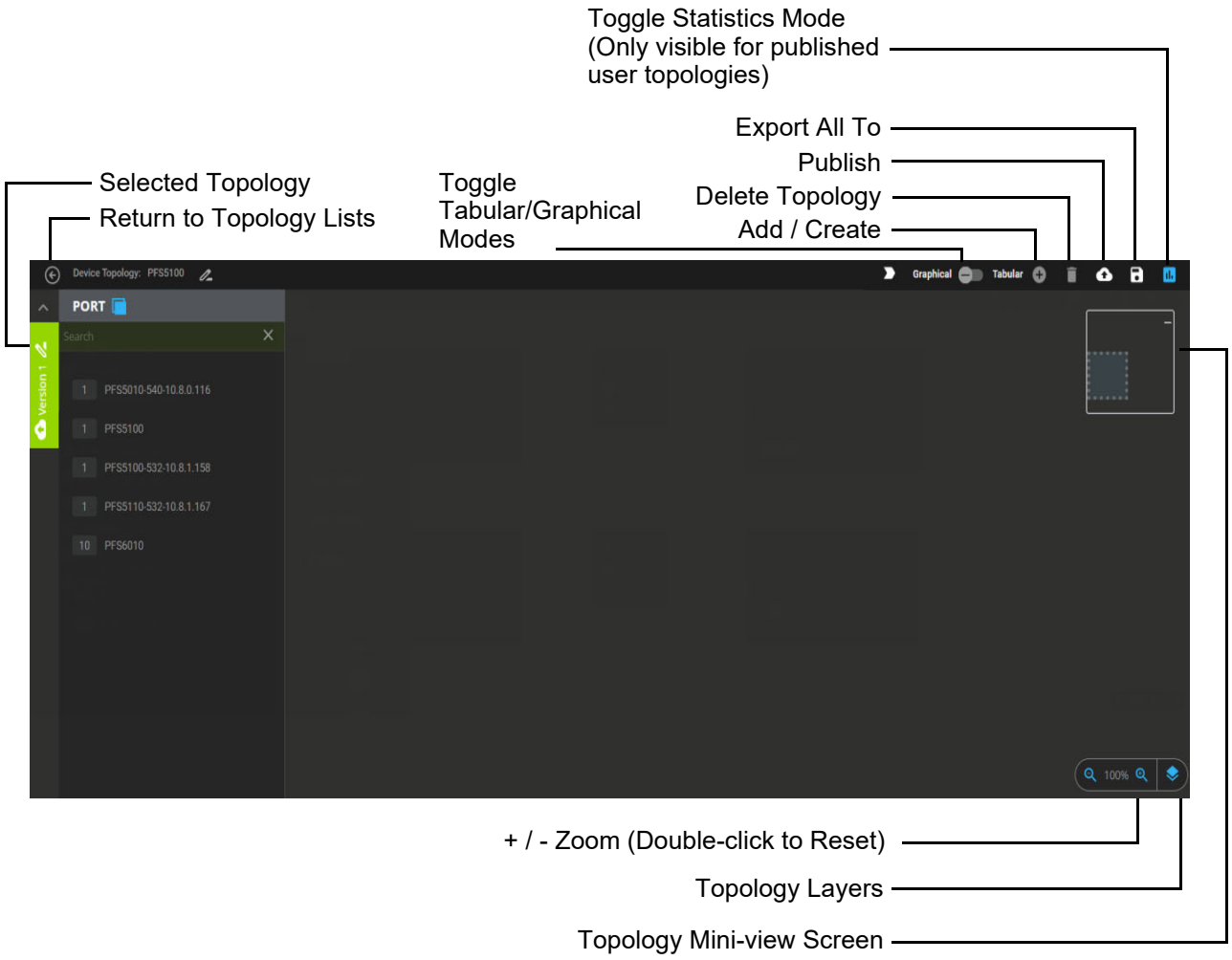
Enter a name for the new topology, you can also enter topology notes and version notes (specific to each topology version), then accept (check mark) the topology. The new topology is now listed.



Click on the topology title to open the main topology screen.



Topology Screen / Features

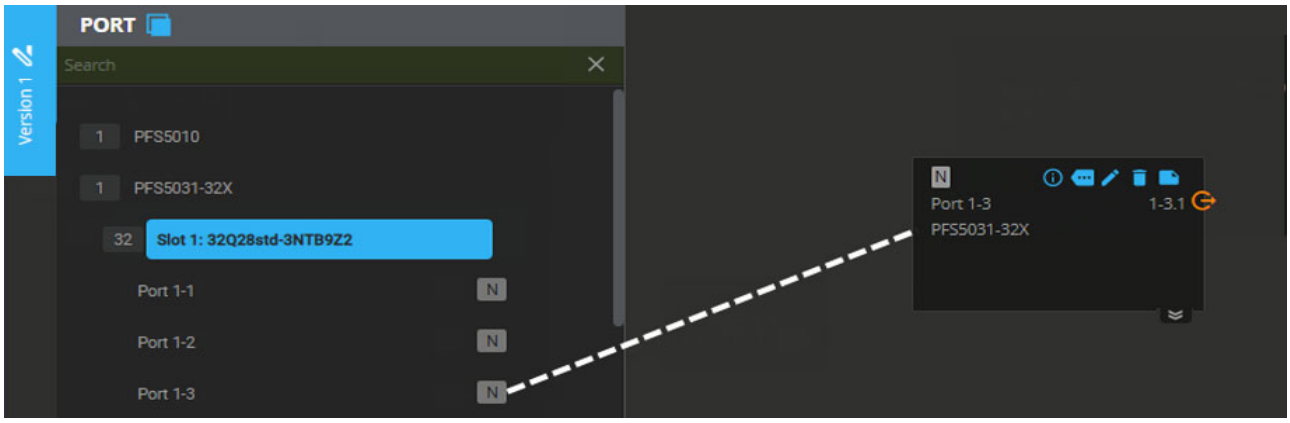


Populating a Topology

After you have created a new topology, you can begin populating the topology.

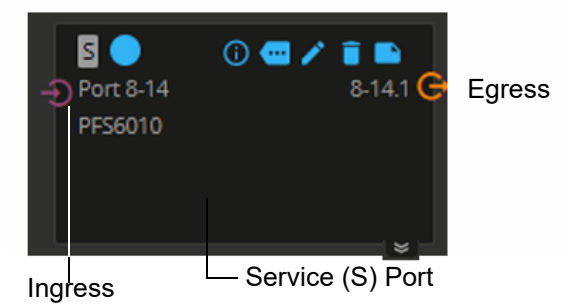
From the Perspective > Port menu, select a port and drag it to the topology canvas. For each port bought onto the screen, a separate port node is added.

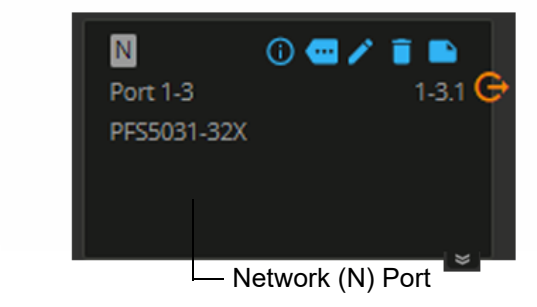
> **Note:** After the port has been dragged to the topology, the port's configuration on the topology is now local to that topology. Any further configuration changes to the port, in the Configuration lifecycle or other topologies, will not affect the port's configuration on the current topology. To refresh the port's configuration on a topology, remove it from the topology and then add it again.

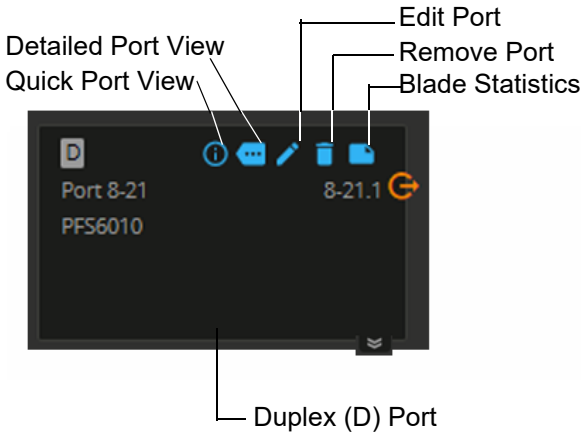


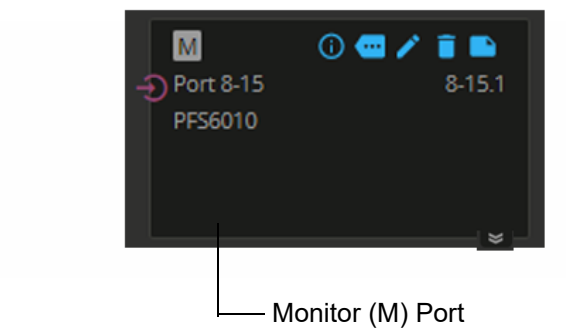
Port Nodes / Port Groups / Filter Details

Port Nodes

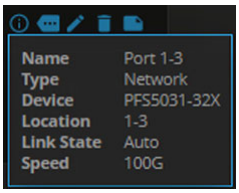




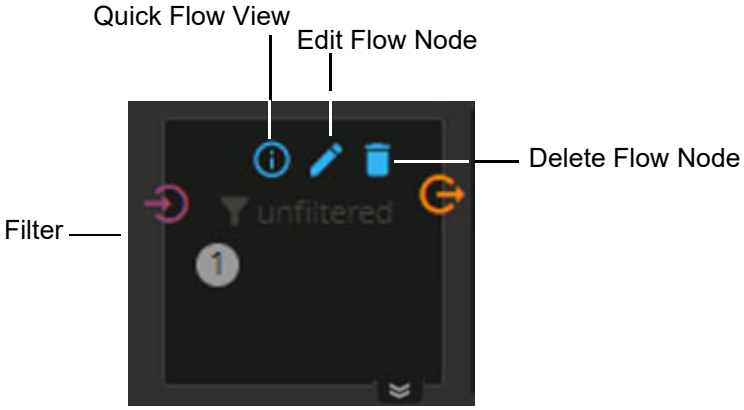




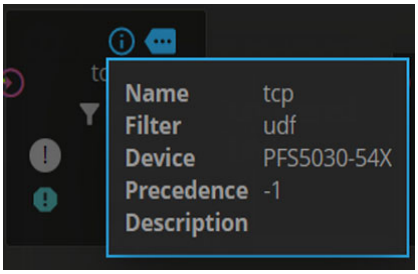
Port Node Quick Info



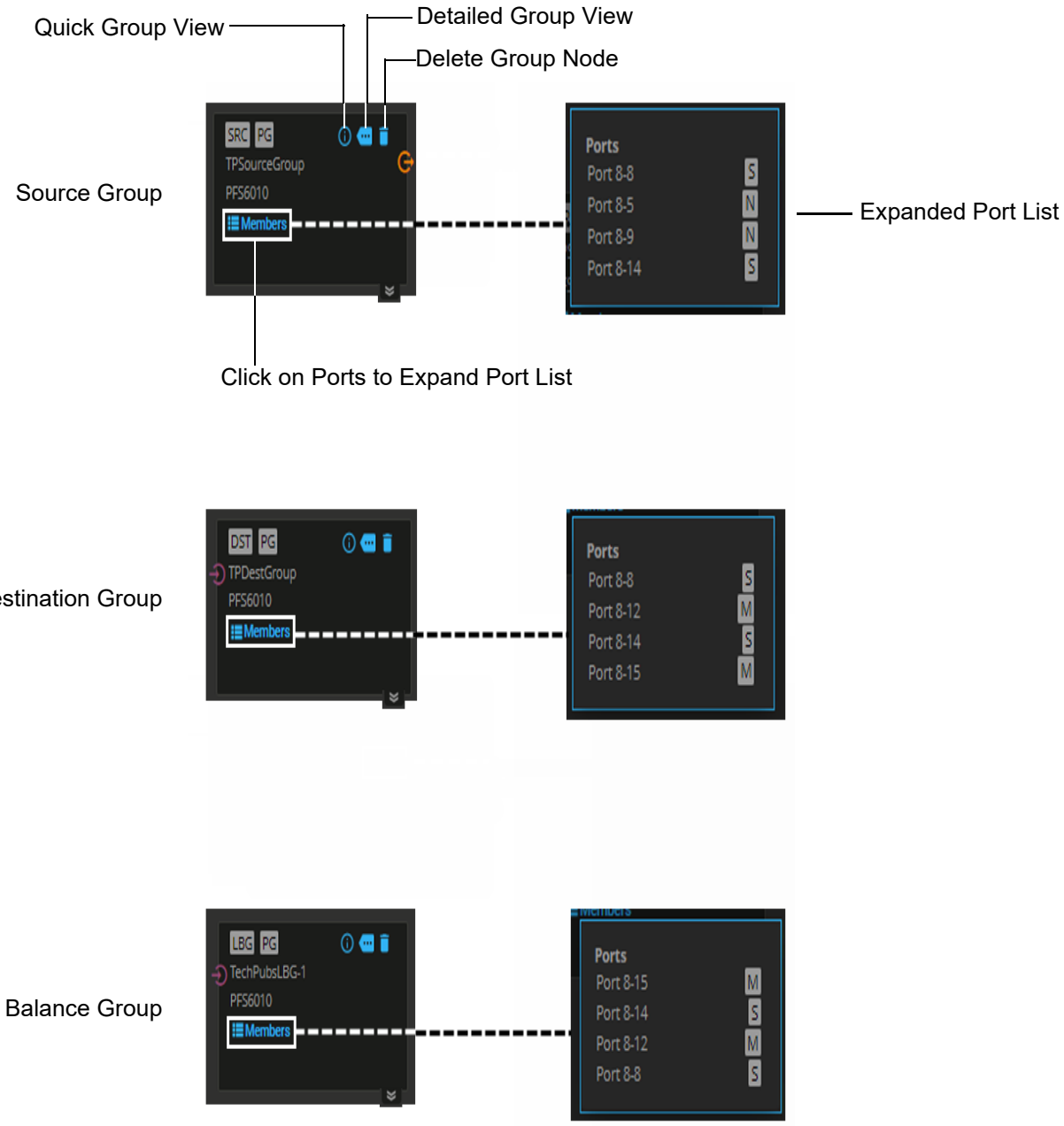
Flow Nodes



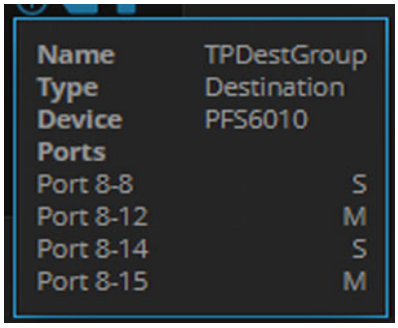
Flow Node Quick Info



Port Groups


Quick Group View
Detailed Group View
Delete Group Node
Source Group
SRC
PG
TPSourceGroup
PFS6010
Members
Ports
Port 8-8
Port 8-5
Port 8-9
Port 8-14
S
N
N
S
Expanded Port List
Click on Ports to Expand Port List
Destination Group
DST
PG
TPDestGroup
PFS6010
Members
Ports
Port 8-8
Port 8-12
Port 8-14
Port 8-15
S
M
S
M
Load Balance Group
LBG
PG
TechPubsLBG-1
PFS6010
Members
Ports
Port 8-15
Port 8-14
Port 8-12
Port 8-8
M
S
M
S

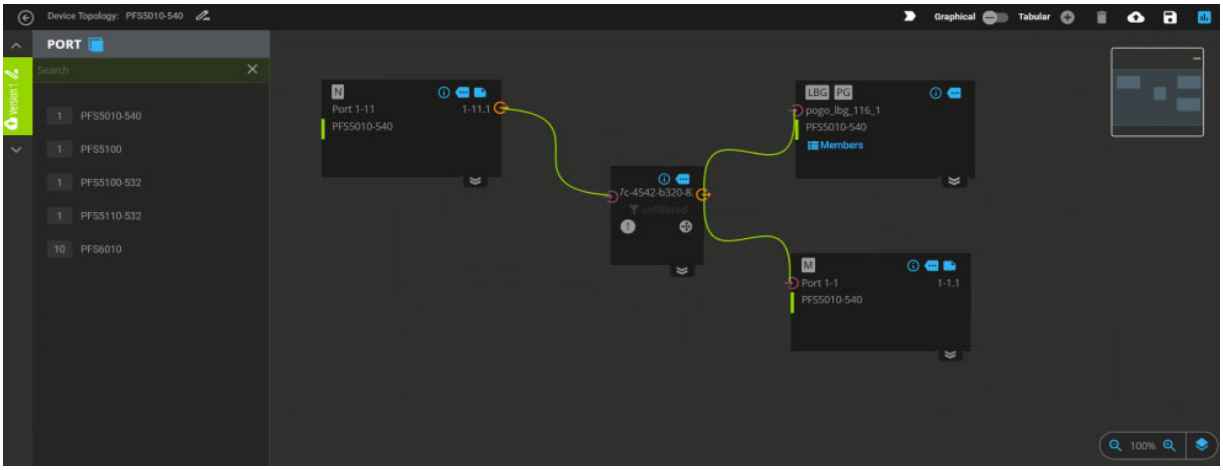
Port Group Quick Info



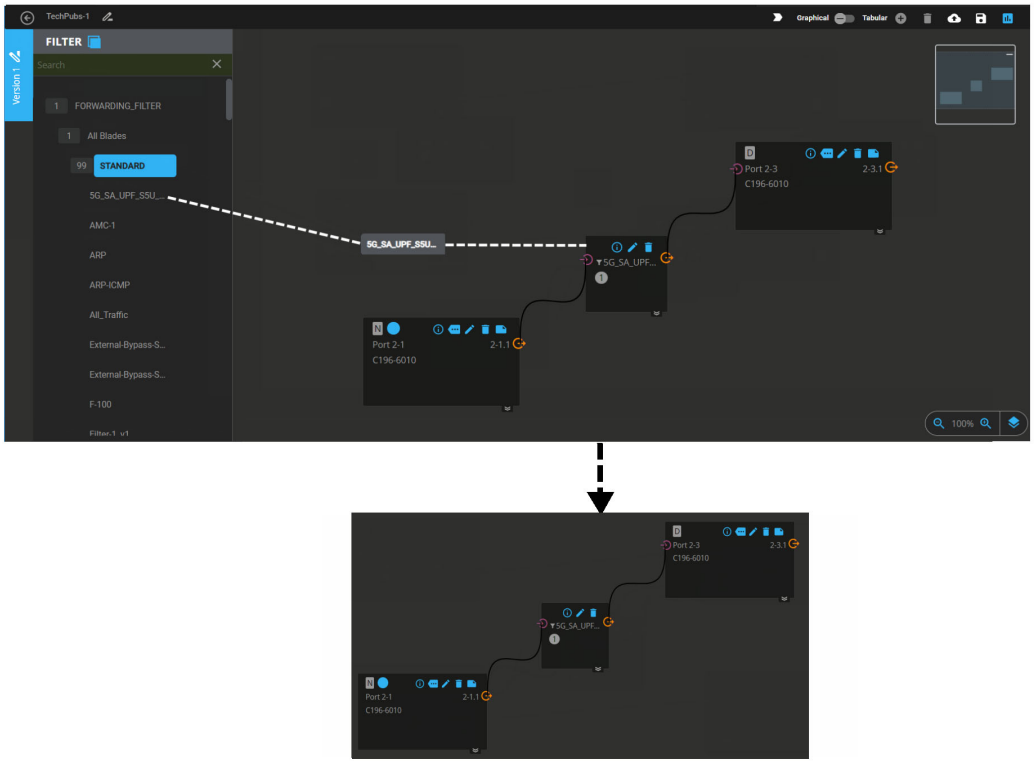
Making Connections

To make a connection between ports, port groups, and flow nodes:

- Users can create port connections with multiple endpoints
- Users can drag filters directly to topology to add a new flow node
- Users can set LBC on the flow node
- Users can drag a filter on top of a flow node to change the filter
- Users can connect source to destination directly as a shortcut to add a flow node



To add a filter to the topology, from the filter perspective, select and drag a filter to the topology. The selected connection line turns blue indicating the location to place the filter.



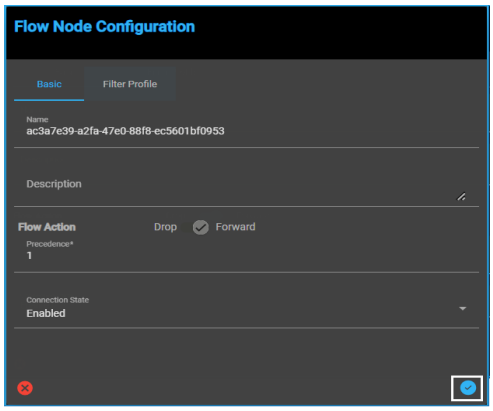
Flow Precedence

Flow precedence is used to establish a sequence in which the PFS examine incoming traffic and apply a policy rule. The first rule in the list to match the conditions of the packet is applied to the packet.

When connecting ports on the topology, after each connector line is drawn, a number representing the precedence level (e.g., 0, 1, 2, 3) is assigned to that point-to-point connection. This number represents the order in which the filters will be applied to the traffic received by the source port or port group.

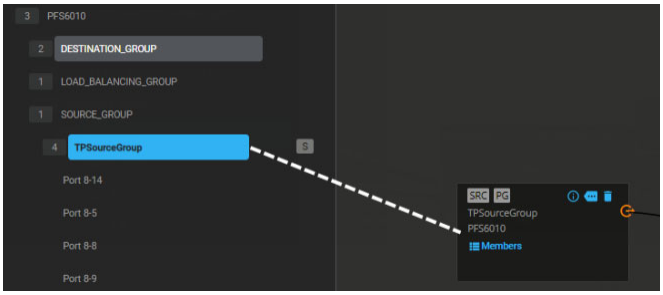
The precedence levels on the connections can be modified by selecting **Edit** from the Flow Node. Click on the up arrow/down arrow to decrease / increase the precedence level numbers. Click on the **Accept** check mark to save the change; the indicator on the selected Flow Node will update to reflect the new precedence value. The precedence order can be changed any time the displayed topology is unpublished.

Note: When a device topology is exported to a user topology, the precedence value is UNSET. In order to re-publish, the user must set the precedence level as required. Changing the precedence level can momentarily disrupt the traffic flow.

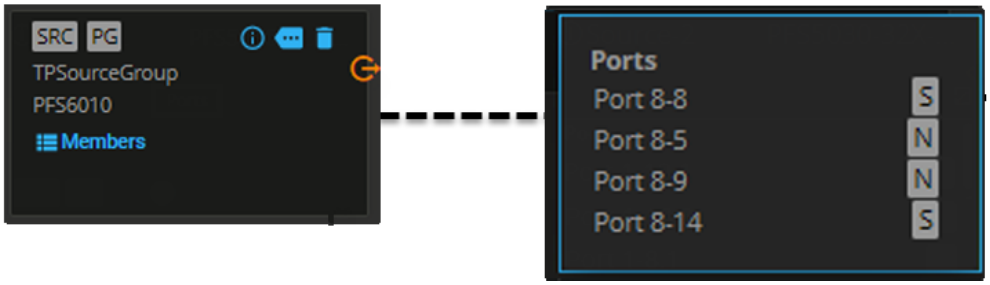


Adding Port Groups

Port groups can be incorporated into topologies with individual ports and filters by clicking on the selected version of a group and dragging it into the topology screen.



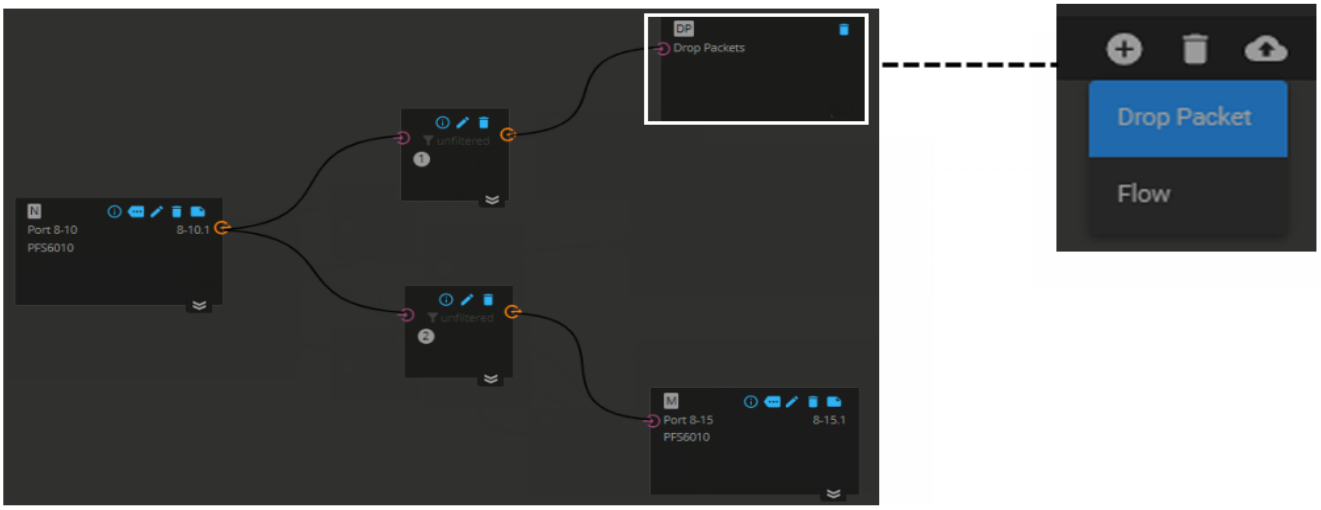
To view the ports associated with the group, click the **Ports** name to expand the field. Click on the **Collapse** icon to close the field.



Adding Drop Packets

Adding a Drop Packet node allows sending selected packets to a bit bucket, sending the remaining packets to a port.

Click on Add/Create > Drop Packet. A Drop Packet node is placed on the topology screen. Connect a Network port, Source port group, or flow node to the Drop Packets node similar to other destination nodes.



Adding Remote Monitor Groups

PFS Fabric Manager can use pfsMesh to make connections across switches, via a published topology, by using Remote Monitor Groups (RMG). The RMGs can be either managed by PFS Fabric Manager or those that are discovered through pfsMesh.

From Perspective > Group, select and drag RMGs onto the topology screen. You can connect the groups just like other port groups.

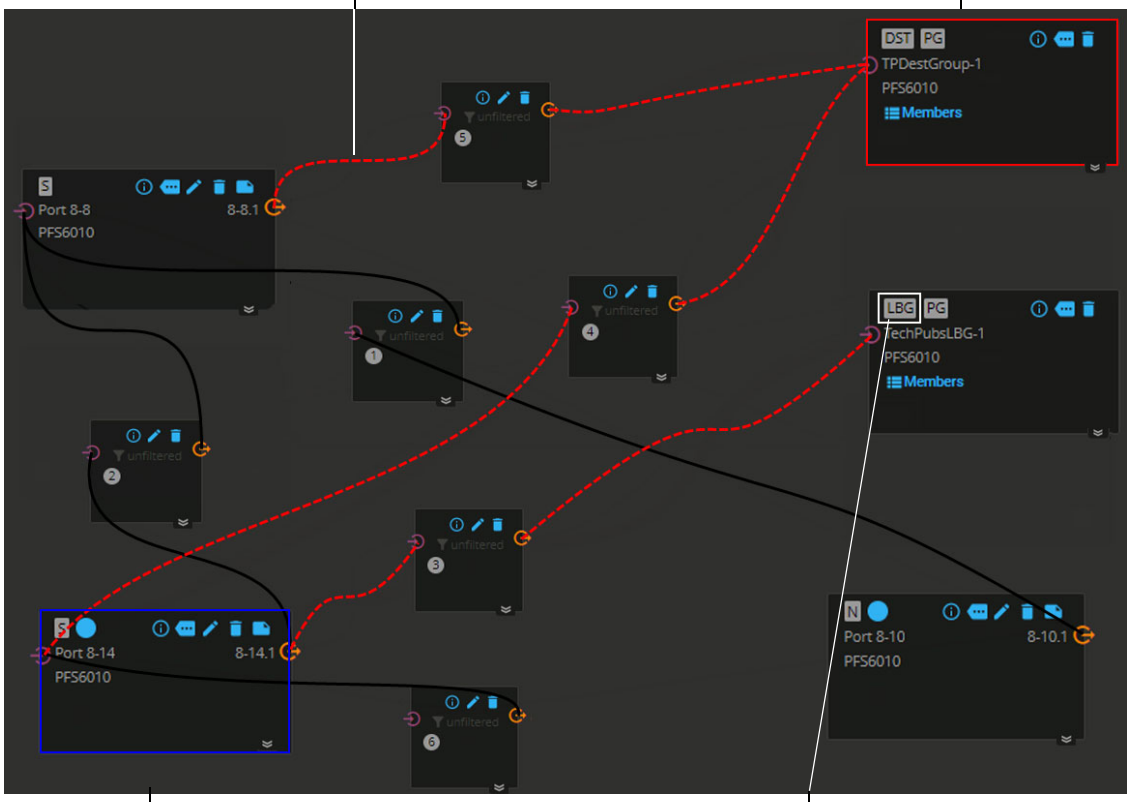
If PFS Fabric Manager detects that pfsMesh does not have visibility to the specified RMG, the connection is marked with a red dashed line.

An RMG which is published and marked as PFS Mesh Visible, but not discovered by any switches through the mesh is displayed on a published topology with a red border.

An RMG which is published and marked as PFS Mesh Visible, but not discovered by any switches through the mesh is displayed on an unpublished topology with a blue border.

RMG is not visible to the source device
(Red Dashed Line - published topology only)

RMG is marked as PFS Mesh Visible, but not discovered by any other switch
(Red Outline - published topology only)

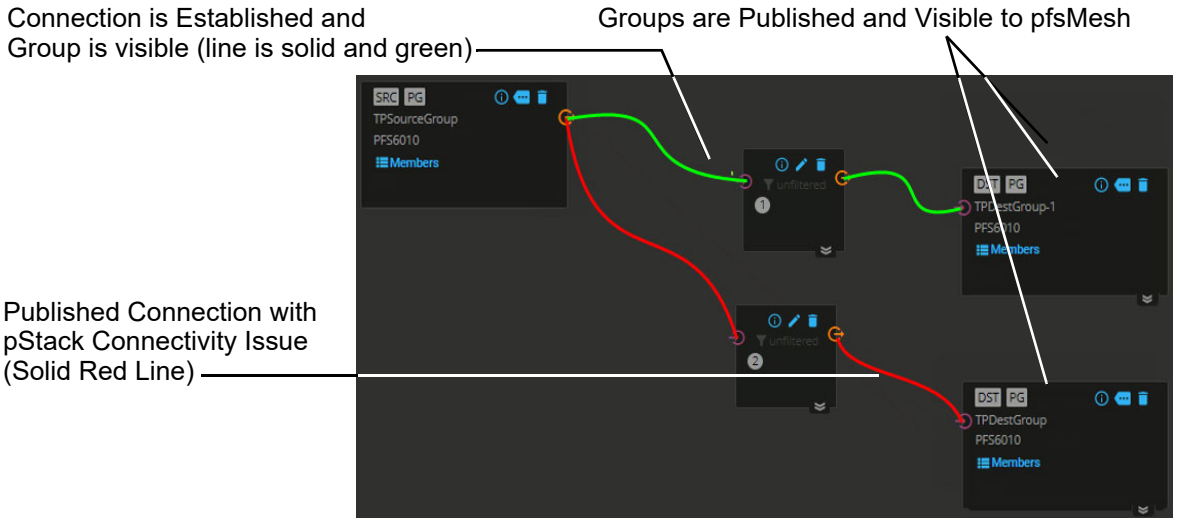


RMG is marked as PFS Mesh Visible, but not discovered by any other switch
(Blue Outline - unpublished topology only)

Managed Remote Group

NOTE: The red status only applies to published topologies.

Published topologies that have a connection which has some kind of problem (i.e., bad fiber along pStack path, bad pStack port transceivers, mis-configured pStack ports, etc), display the connection as a solid red line.



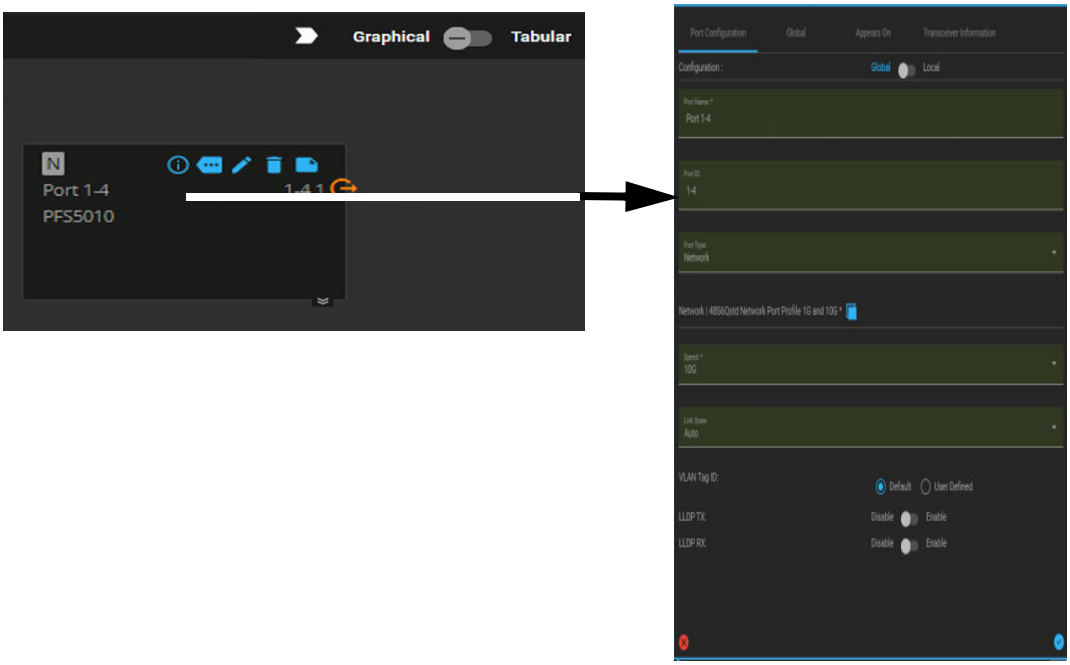
Enabling/Disabling Local Configuration

Port configuration on topology, by default, reflects the global configuration of the port.

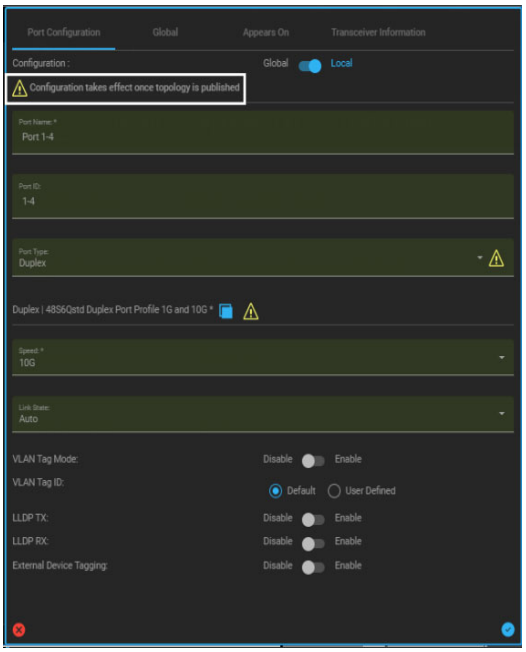
With global configuration selected, the user can change the global port configuration from topology. These changes are not stored with the topology but are published immediately to the port. When global port configuration conflicts with how a port is used on any topology, the topology will be marked as conflicted or mismatched. Conflicted topologies cannot be published.

When local configuration is selected, the configuration is decoupled from the global port configuration and a snapshot of the configuration, at that time, is stored with the topology. If the global port configuration changes, the change is not reflected on that topology. In order to locally configure a port on topology, the user must enable local configuration. The user can then configure all available options for that port. When the topology is published, the local configuration is published to the port, replacing the current global configuration.

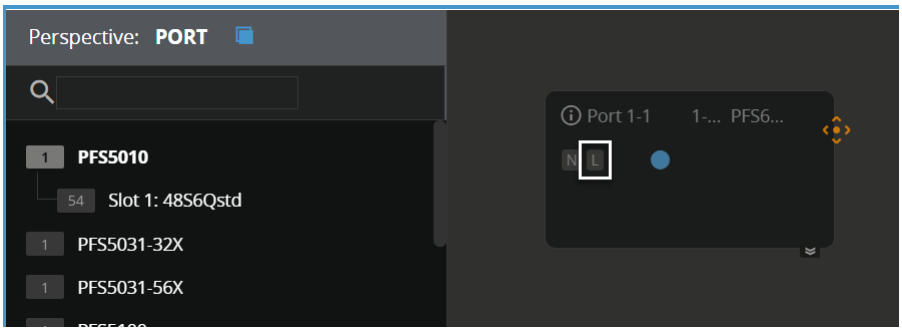
The user can select Global or Local configuration from the Port settings window.



A warning appears, notifying the user that this configuration is published (pushed to the device) only when this topology version is published.



A port will have an additional indicator in case the configuration is Local.

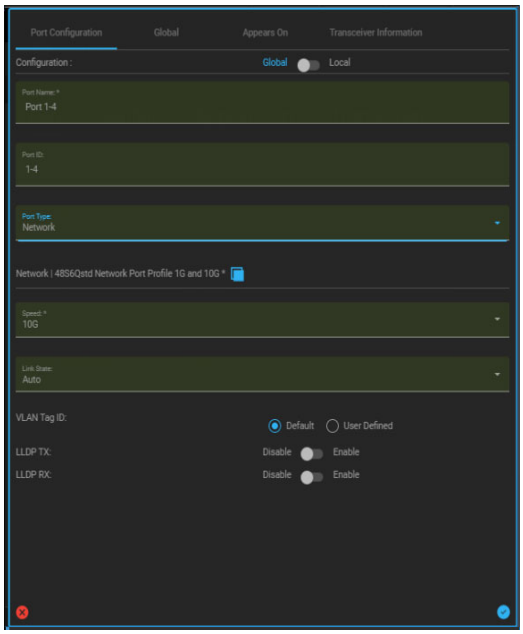


Local vs. Global

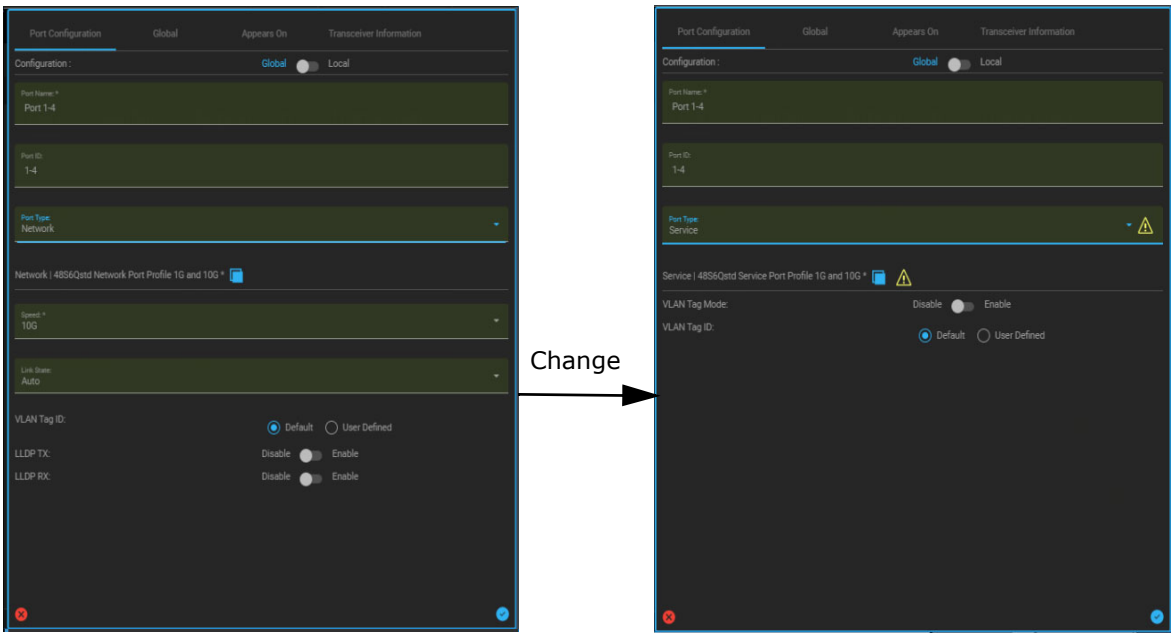
Users can see the difference between Local and Global configuration from the Port settings window. The Port settings window has two sub-tabs - Port (local to topology changes, if Local is selected) and Global (port settings as it appears in Configure lifecycle). Users can switch between the tabs to see the original/ global configuration for comparison.

> **Note:** The Global settings are always read only.

Port settings are read only if the topology version is published and they are editable if the topology version is unpublished.



A warning icon appears if any configuration settings differ between the port local version and global version.



Publication

Changes made to local port configuration must be published. When the topology is published, the local port configuration will overwrite the global configuration. Published topologies cannot be modified.

Conflicts and Validation

For a topology to be published, it must first pass topology validation.

The following are relevant topology validation rules:

- Two or more topologies cannot be published with different local configurations for the same port
- Local configuration cannot conflict with how a port is used in published traffic maps
- Local configuration cannot conflict with how the port is used in groups
- Local configuration cannot conflict with how the port is used in connections on the same topology
- Connections cannot use a port in a way that conflicts with the global configuration, unless the topology has local configuration for that port

For example, a port used as a map destination or in a Monitor group cannot be changed to a Network port as a result of topology publication.

A new topology icon indicates when a connection uses a port in a way that conflicts with the global port configuration.

Note: This icon applies to unpublished topologies when local port configuration is disabled and the global configuration has been changed to a port type that is not legal in the connection.

The following port types can be used as source ports:

- Network
- Service
- Duplex

The following port types can be used as destination ports:

- Monitor
- Service
- Duplex

Upgrade and Down-rev support

Upgrade migration does not preserve current local port configuration. All ports on existing topologies are marked as globally configured and all local configuration is deleted.

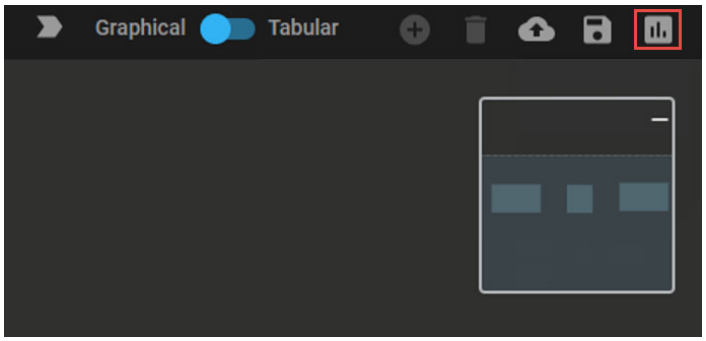
Down-rev switches are supported with no special cases. Global port configuration from topology is preserved when a port is changed from the Configure lifecycle. Local port configuration on topology is an existing use case and will be supported out of the box.

Topology Node Statistics

Statistics Toggle

Statistics for all nodes on the topology can be turned on with a single click in the statistics menu in the topology toolbar.

Note: Topology node statistics are only available on published user topologies.

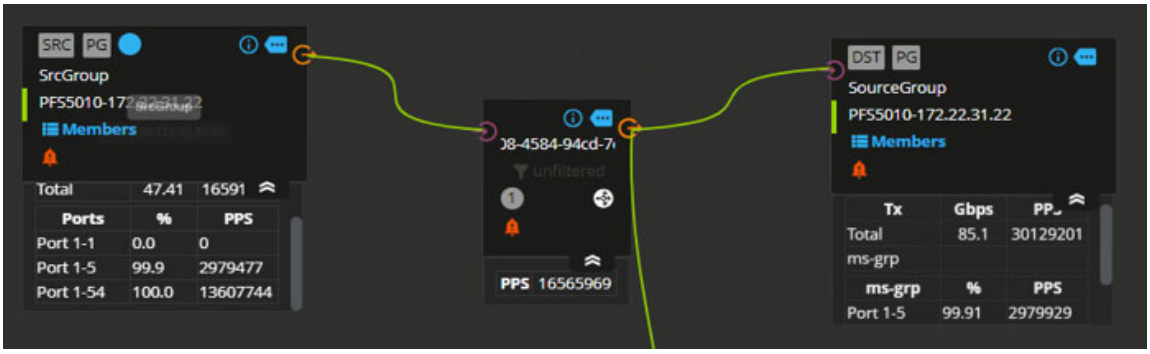


Topology Statistics Expand Button

Topology nodes have a *statistics expand* button used to display the statistics information for that node.

Clicking the node's statistics expand button displays the statistics in an extension panel. Each port group node independently maintains information for its statistics toggle. This allows for several nodes to have the statistics open at the same time, independent of every other node.

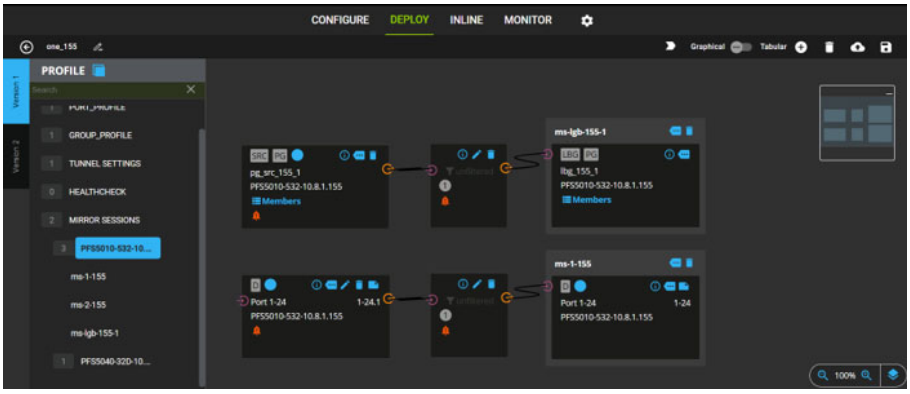
- Ports display *PPS* info for all nodes and % utilization info for port nodes.
- Flow nodes display *PPS* info.
- Tunnel nodes display PPS info.
- Port group nodes display aggregate throughput (in Gbps) and PPS info.



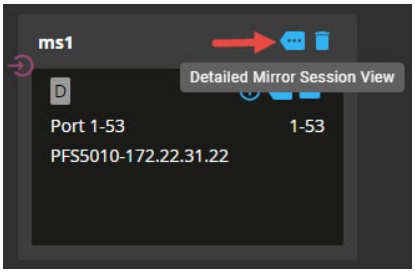
Note: Statistics information is a part of the node and moves with the node whenever the node is moved.

Mirroring on Deploy Lifecycle

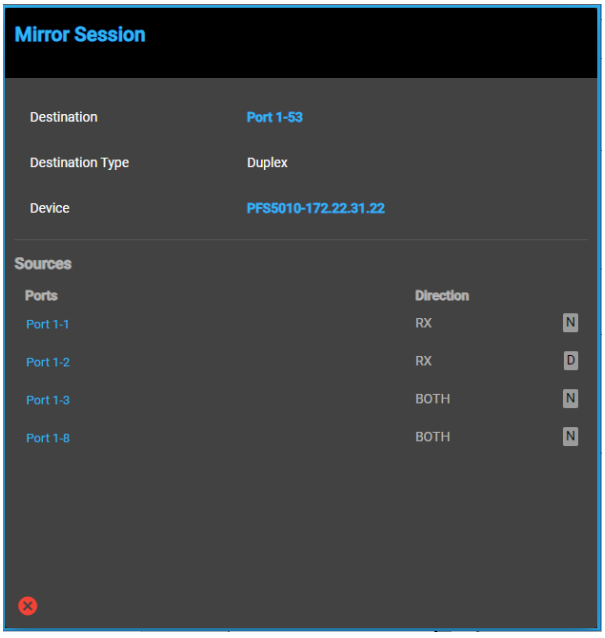
Mirror Sessions are added to a topology from the Profile perspective. They are dragged and dropped the same as all other nodes in a topology.



Detailed information about the mirror session is viewed in a by clicking on **Detailed Mirror Session View**.



A Mirror Session pop-up displays the mirror session information.



A Mirror node can be deleted by clicking **Delete Node**. Edges can be added between a source node or a flow node. If an edge is added between a source node and a mirror node, a flow node is automatically created and the source for the mirror node is the flow node.

Published topologies with mirror nodes look and behave the same as topologies without mirror nodes.

Topology Notes

The user can enter topology notes or version notes in one of the following ways:

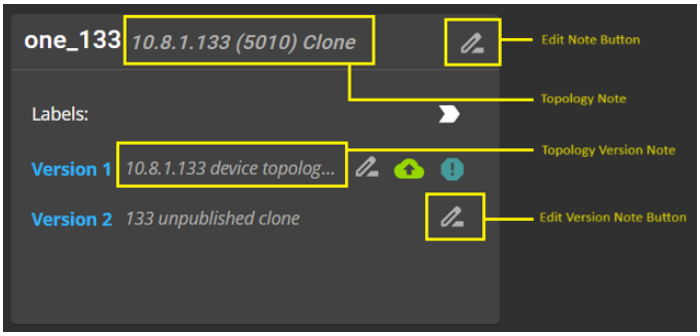
- Topology vCards
- New topology or saving as
- Topology Canvas

> **Note:** Topology notes are for user topologies only and not for device topologies.

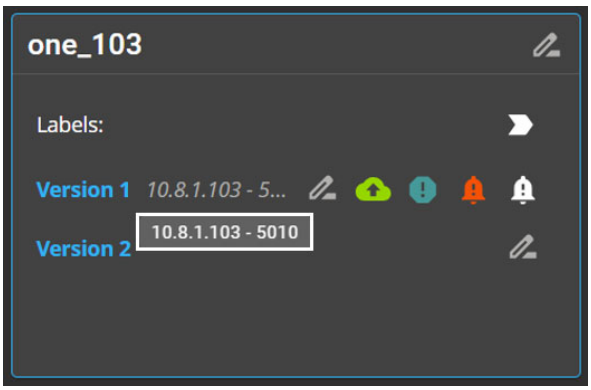
Topology vCards

Topology vCards display topology notes for the topology and each of its versions, next to the topology name, and the user is able to update the note with the adjacent pencil icon.

> **Note:** The pencil icon is different from the EDIT icon seen on other vCards. This is to differentiate that the pencil icon does not edit the topology, only the note.

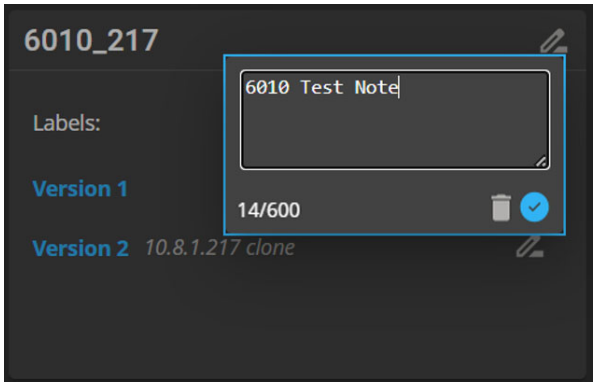


The note uses any available space on the vCard with the overflowing text represented by an ellipsis and the full message is viewed as a tool tip.

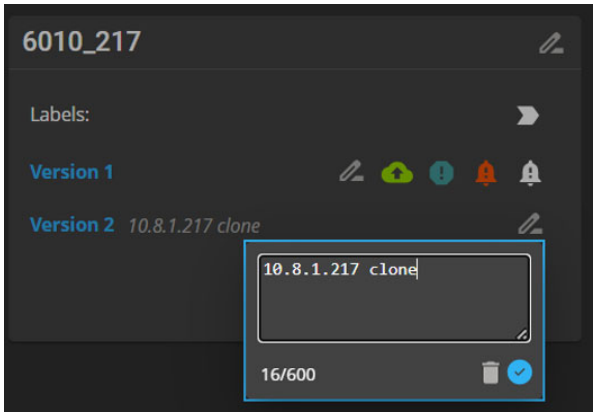


Clicking on the pencil icon displays a small pop-up dialog where the note can be updated.

Topology Note:

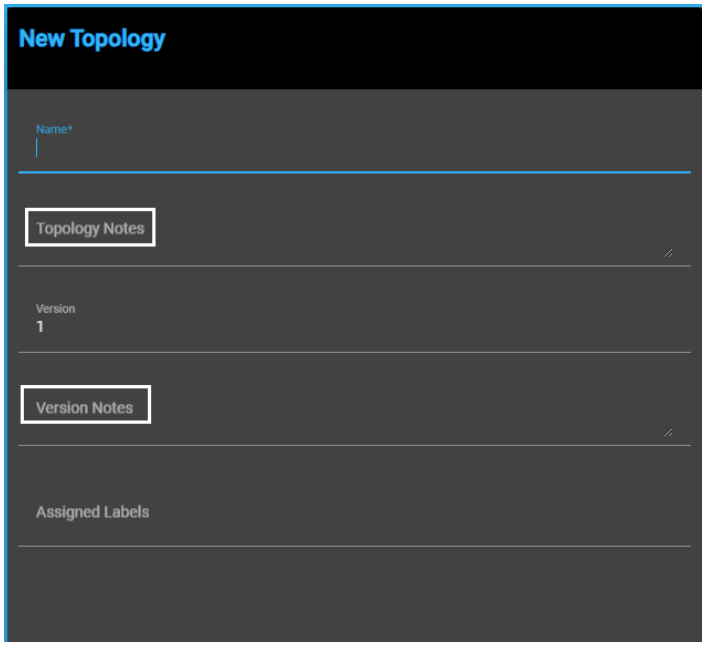


Version Note:



New Topology and Save As

When creating a new topology or performing a “Save As” on a topology, the screen displays “Topology Notes” and “Version Notes” text fields, where users can enter notes for the topology and for the version.



Topology Canvas

Topology notes can be edited on the canvas from the topology header.

Topology version notes can be viewed and updated in the version selector. If a note is available, an info icon is displayed. Hovering on the info icon displays the note in the form of a tooltip. The user can edit the note using the pencil icon. If a version does not have a note, the info icon will not be visible.

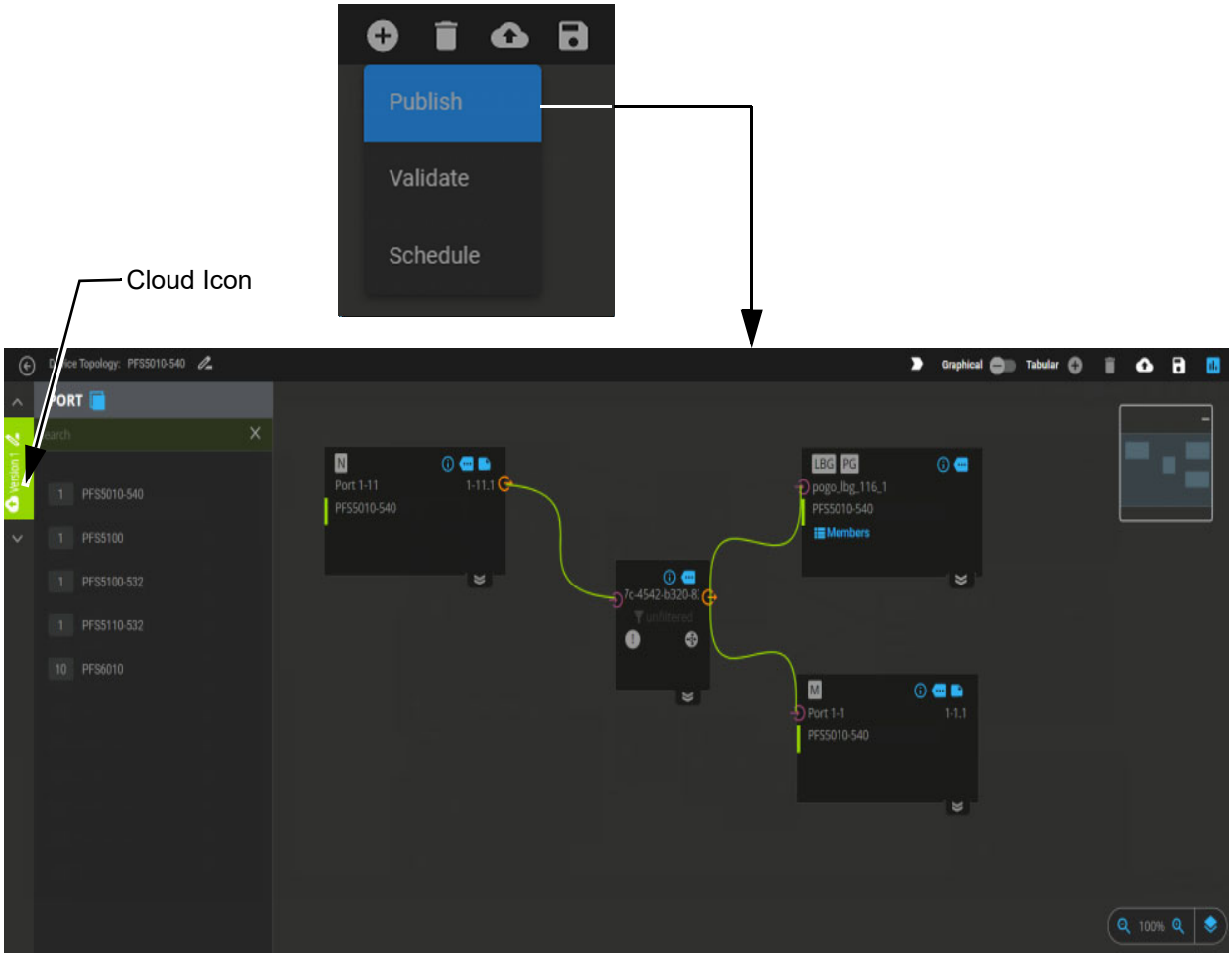
Publishing a Topology

To publish (activate) the connections in the current topology, click on the **Publish** icon then select **Publish Current Topology**. A confirmation message stating that the topology is being published is momentarily displayed. The connected nodes now display a green bar with green connection lines indicating a connection. In addition, the topology title block displays a small “cloud” icon indicating the published connection.

During topology publication, the following occurs:

- Topology configuration validation
- Configuration between the current topology and all published topologies are validated
- The topology is pushed to the devices

In the event of a connector error, the topology is rolled back and not published.

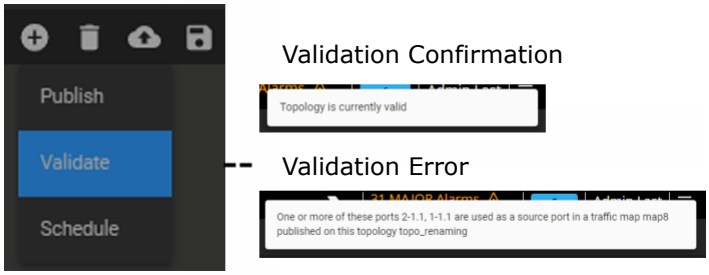


Unpublish a Topology

To unpublish (deactivate) the current topology, click on the **Publish** icon then select **Unpublish Current Topology**. A confirmation message stating that the topology is being unpublished is displayed.

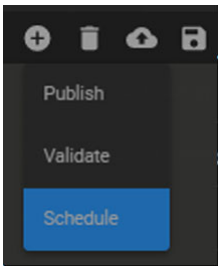
Validate a Topology

To Validate the current topology, click on the **Publish** icon then select **Validate Topology**. A confirmation message stating that the topology is valid or an error message is displayed.

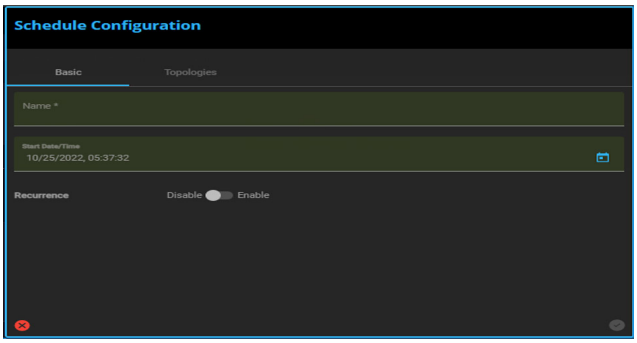


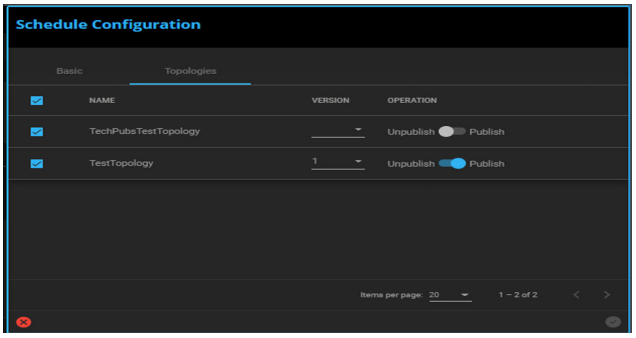
Schedule a Topology

To schedule a topology, click on the **Publish** icon then select **Schedule Topology**.



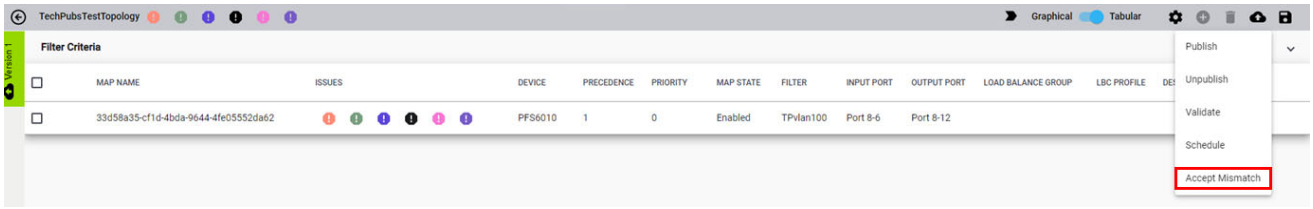
A Topology Schedule window is displayed.

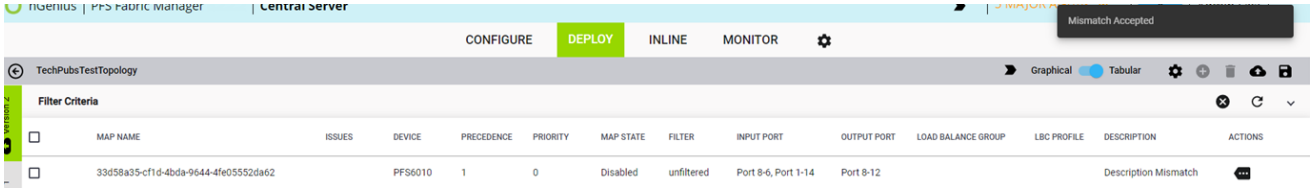




Accept a Mismatched Topology

To Accept a mismatched topology, click on the **Publish** icon then select **Accept mismatch**. A confirmation message stating that the topology is valid or an error message is displayed.





PFSMesh Topology - Items to Remember

- Status updates are automatic.
- Updates will appear within 25 to 60 seconds.
- Dashed lines displayed on unpublished topologies indicate that a connection does not yet exist.
- Solid lines are displayed on published topologies indicating that connections are installed on switches.
- Group borders indicate the current status of the group in relation to the mesh.
- Connection lines indicate the status of the group as seen by the switch containing the source port.

Save a Topology

Save the topology by clicking the **Export All To** icon and selecting **New Topology**. Enter a name for the topology and a version number. Click on the **Save As** check mark to save the topology.

To save (clone) the topology as a different version, select **New Version**.

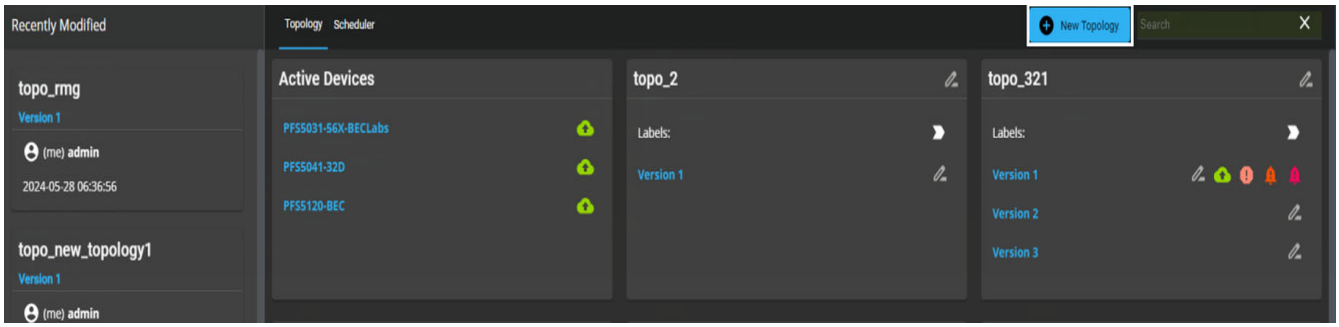
Topologies and Versions

You can have as many topologies (published / un-published) as necessary containing ports, connections / flows, and filters grouped in whatever combination is convenient. Resources can be utilized on multiple topologies.

Each topology can have many versions, however, only one version of a topology can be published at a time.

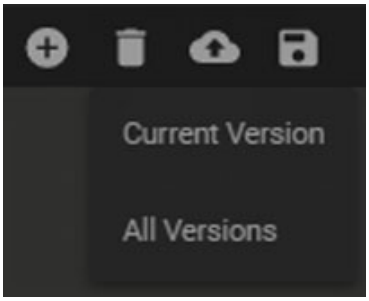
Viewing List of Topologies

All versions of created and published topologies are listed on the main Deploy screen.



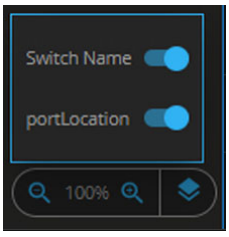
Delete a Topology

You can delete the current unpublished selected version of a topology or all saved unpublished versions of the selected topology. Click on the **Delete Topology** icon and select either **Delete Current Version** or **Delete All Versions**.



Topology Layers

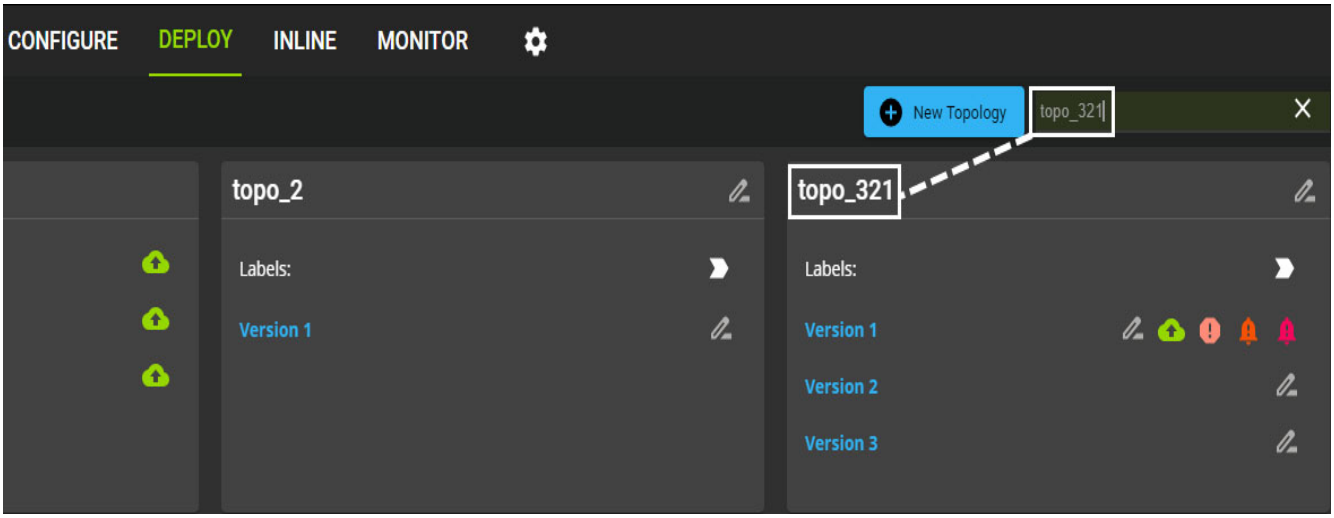
To allow easier viewing of complex topologies (from either a selected topology or the switch topology) by hiding specified layers, click on the topology layers menu to display a list of the associated layers that can be displayed (On) or hidden (Off). Dynamic Endpoints is an experimental feature that causes the port connectors on the topology to dynamically move to a more optimal location.



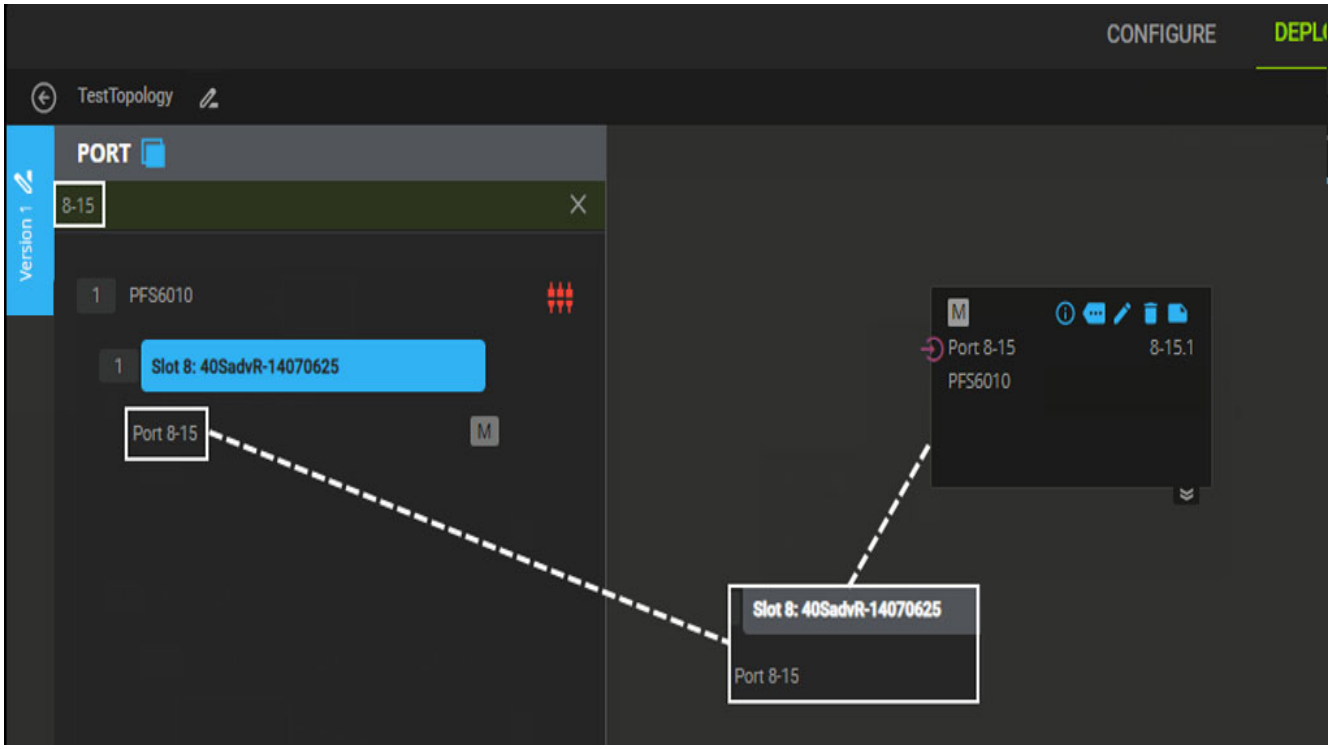
Topology Search

The Topology search allows searching for topologies by name.

Using the same port search criteria described in Configure Search Filter on page 3-32, enter a topology name (full or partial naming) in the Search text field. Any published / unpublished topologies containing the search name are displayed in the Deploy Lifecycle screen. Clicking on a version of a topology will open the screen of the selected topology.



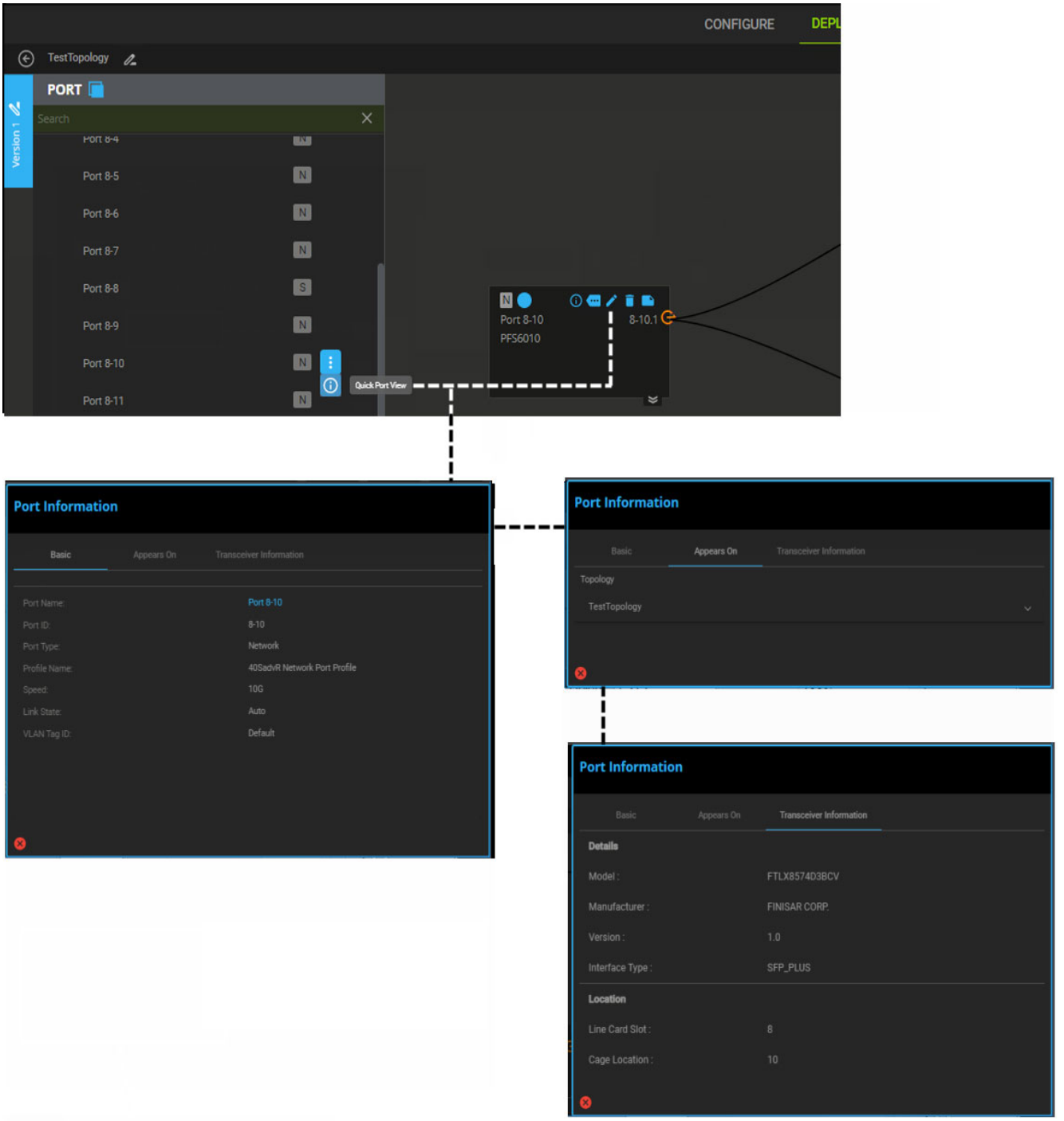
In addition, opening a topology allows using the search function to locate ports for placement in a topology.



Topology > Port on Topology Association

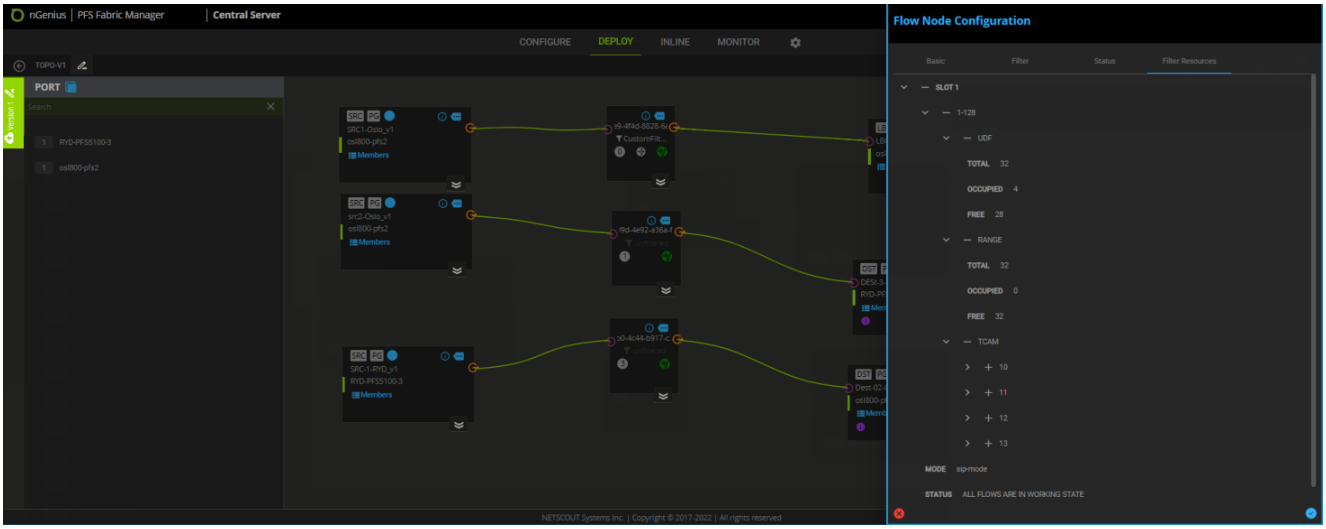
Hovering over / clicking on a port or a port on a topology allows access to the Information menu option. Clicking on the Information icon opens a new Port Information screen displaying the current configuration of the selected port and any associated topologies. Clicking on a topology version will open the screen of the selected topology from the Deploy Lifecycle.

In addition, selecting Transceiver Information displays the current transceiver status of the selected port (e.g., transceiver model, manufacturer, interface type, line card slot . cage location).



Topology > Port on Filter Resources

Hovering over / clicking on a filter allows access to the Detailed Flow View menu option. Clicking on the Filter Resources tab opens a new information screen displaying the current configuration of the selected filter.

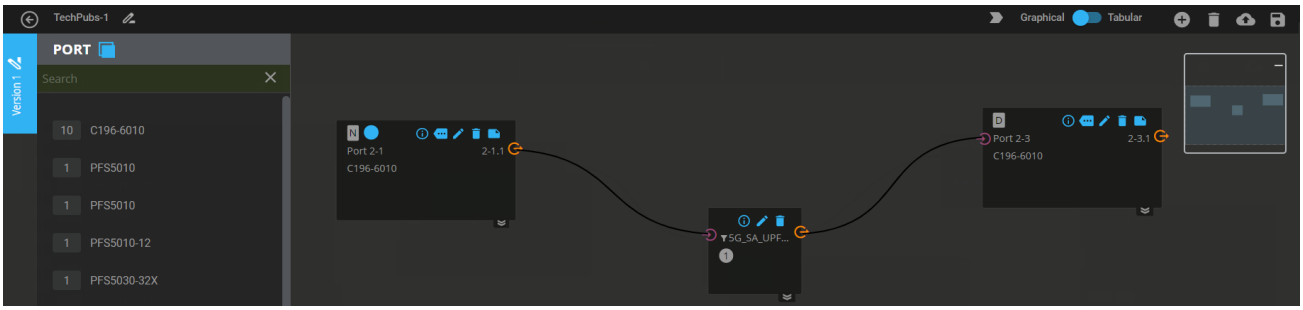


Topology > Tabular View

The tabular view of the topology allows for an increase in information density, so that users with large numbers of maps can view more of their configuration at once.

Deploy Lifecycle

Users can switch between the tabular and graphical views from the Topology canvas.

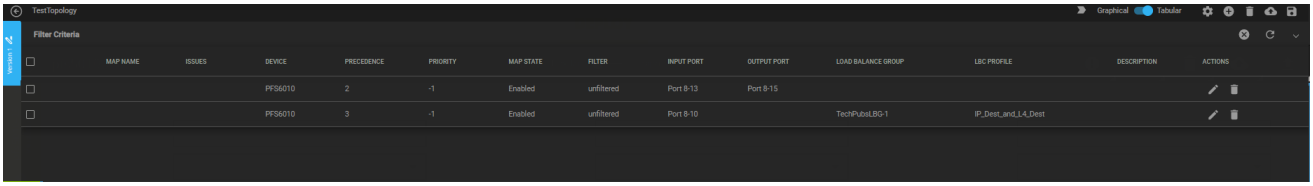


The tabular topology view includes:

- List of flows
  - All relevant info per flow
  - State of each flow as reported by the device
  - Indicators for any encountered issues like mismatches (user topologies)
- Filtering criteria
- Pagination
- Select which columns to display (Settings gear at the right bottom corner)

The filtering criteria set changes based on the selected columns.

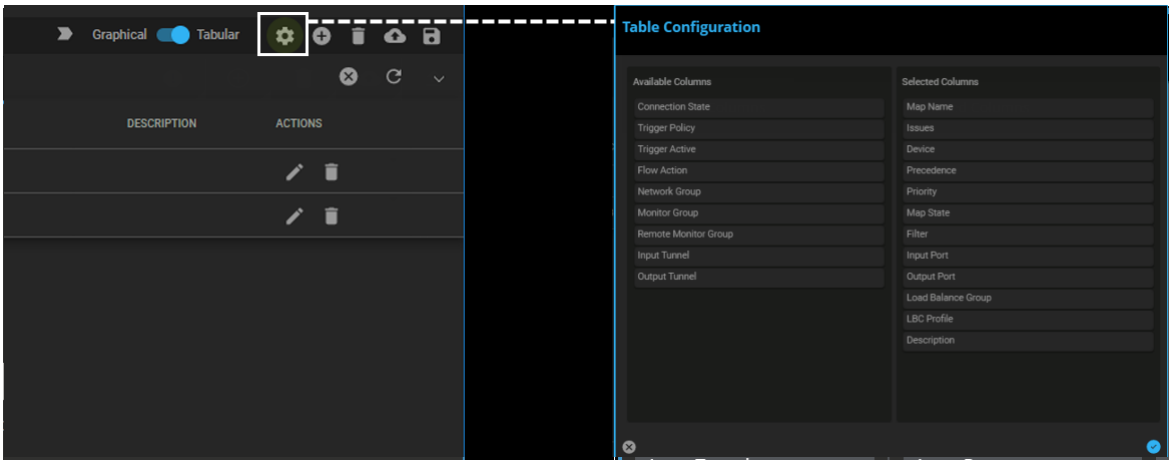
Device Topology:



Selecting Columns

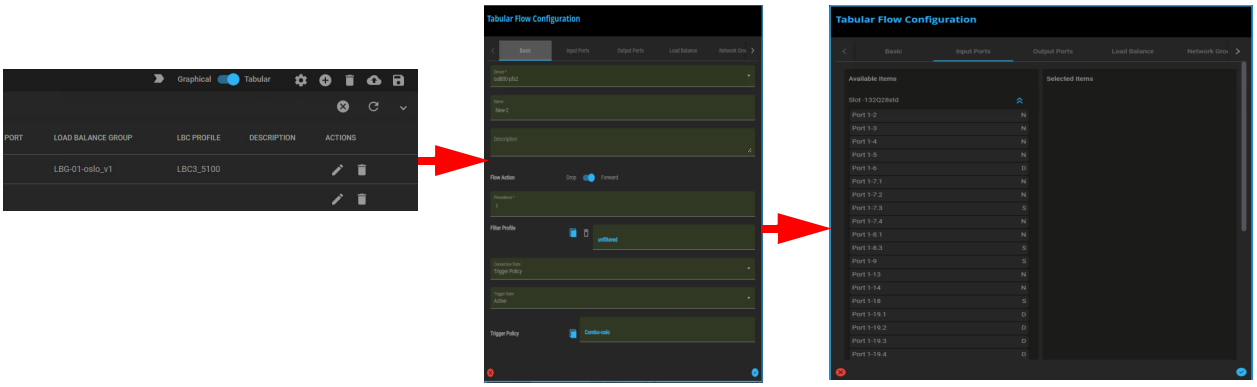
Click on the Settings icon to open a slide-out for columns selection.

Drag and drop desirable/appropriate columns columns and click on blue Save button to apply the selection.



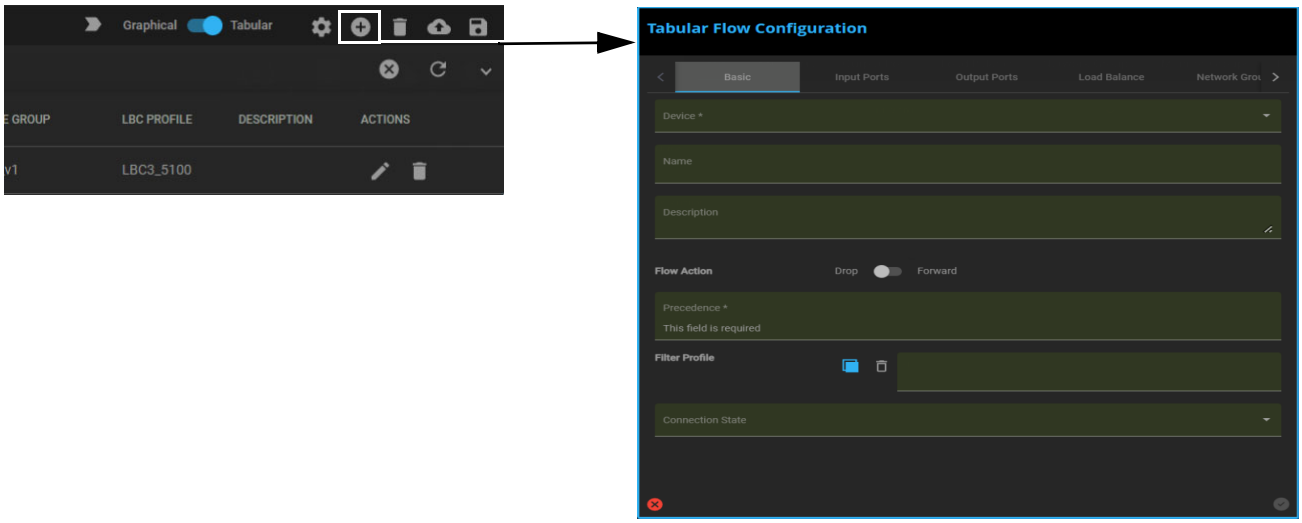
Editing Topology and Flows

Click on a traffic map name to edit a selected row in a slide-out:



Adding traffic maps

Click on the Plus button to add a new traffic map to the unpublished topology. The user must specify the device in order to provide a list of input/output sources.



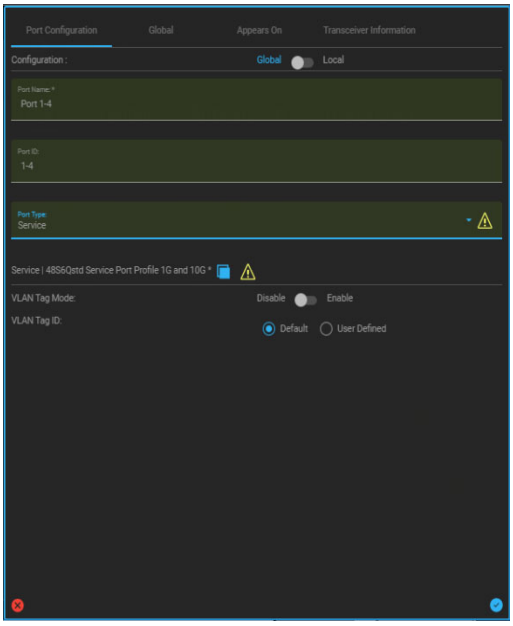
Ports and Groups

Click on a port/port group name to view or edit the information.

Port settings are editable if the topology version is unpublished, otherwise they are read only.

Port global settings are always read only and only for comparison.

> **Note:** A warning icon appears next to those fields that vary from the port global configuration (as it appears in Configuration lifecycle).



There is no change in the port group window, the same information is displayed after the user clicks on the port group name.

Topology Subsets

The user can create a new topology version or a new topology by selecting all or a subset of the current topology version traffic maps.

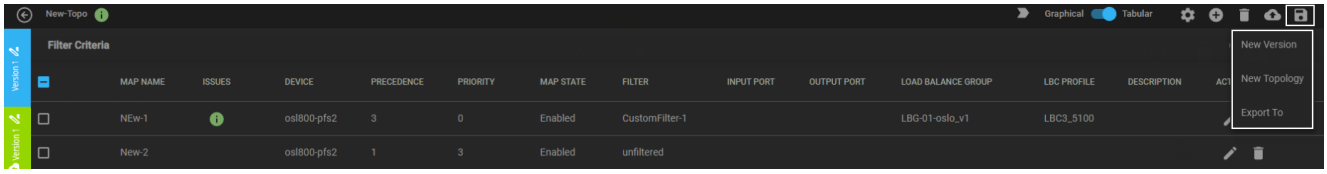
The mechanism is the same whether it is a device topology or a user created topology via PFS Fabric Manager (published or unpublished).

If no flows are selected then the Export-As operation will operate on all flows.

User topology has the following options available:

- New Version - creates a new unpublished version of the same user topology
- New Topology - creates a new unpublished topology with the specified version number. Depending on the published state and type of the original topology, additional prompt may offer to move (cut-and-paste) selected flows.
- Export To- merges selected traffic maps with another existing topology. Merge is allowed into unpublished topology only. Depending on the published state and type of the original topology, additional prompt may offer to move (cut-and-paste) selected flows.

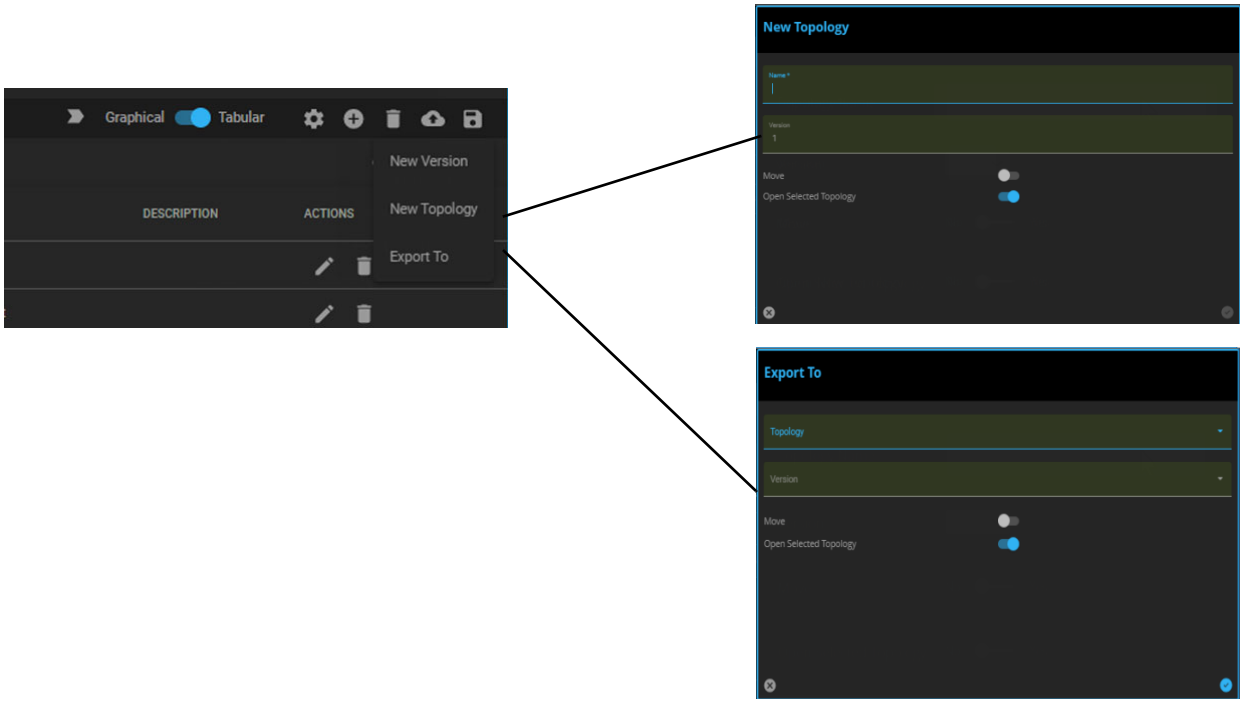
Move allows to quickly split a large topology into few smaller ones.



Device topologies cannot be modified. As a result selected flows/maps cannot be removed from the original topology while exporting into another topology.

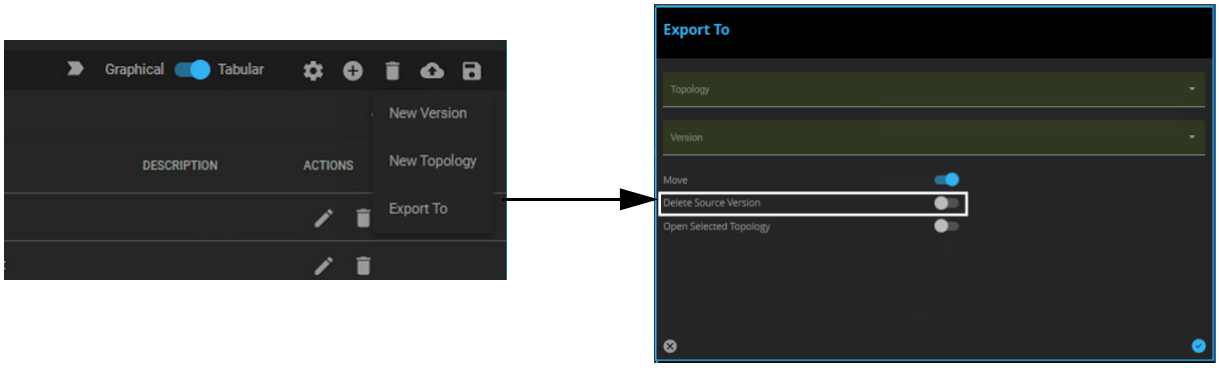
Published user topologies have all choices available but still cannot move (cut-and-paste) selected flows/maps from the original source.

Unpublished user topologies have all choices available and can be modified. As a result, selected flows/maps can be moved (cut-and-paste) from the original source into another topology.

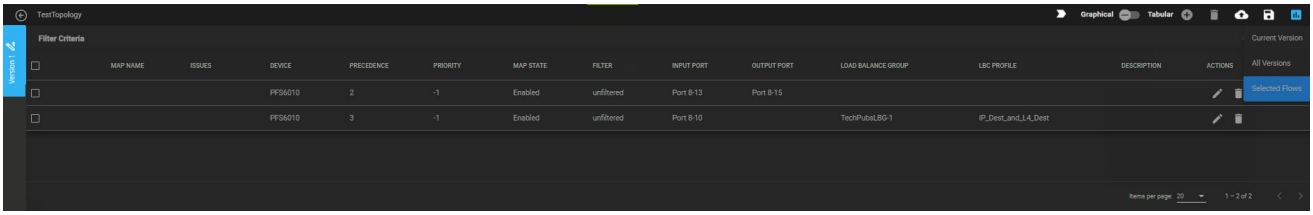


An additional field - Delete Source Version, appears if the user checked the Move (cut-and-paste) check box and all flows were selected.

The original (source) topology version is deleted after the confirmation if the user selects to do so.



Users can delete selected flows if the topology version is unpublished.

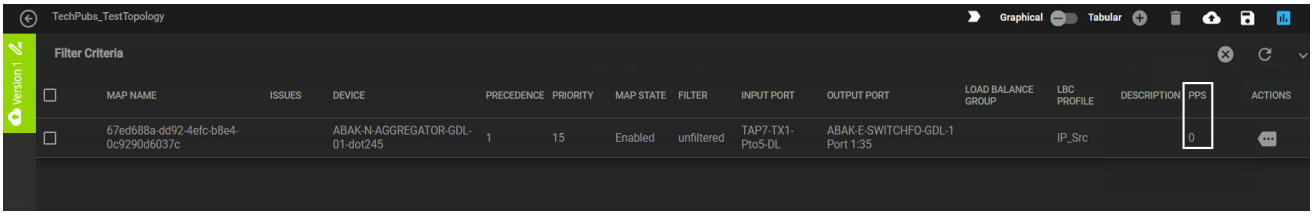


Tabular Topology Statistics

Statistics for all nodes on the topology are displayed by clicking the Statistics icon in the topology toolbar.

Note: Topology node statistics are only available on published topologies.

When the statistics are enabled, a PPS column is automatically added to the tabular view.

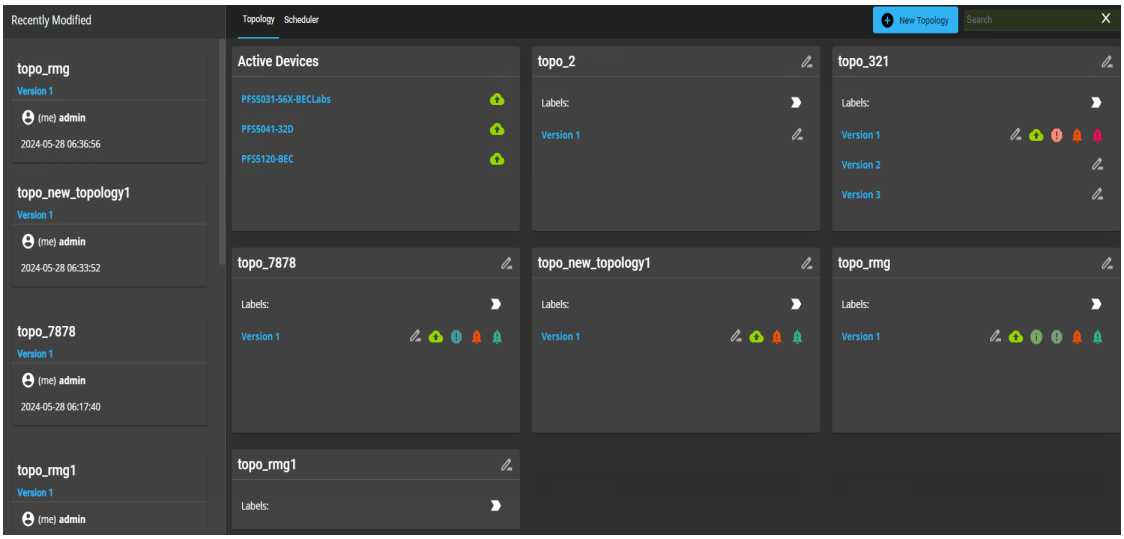


Topology > Configuration Changes Scheduling

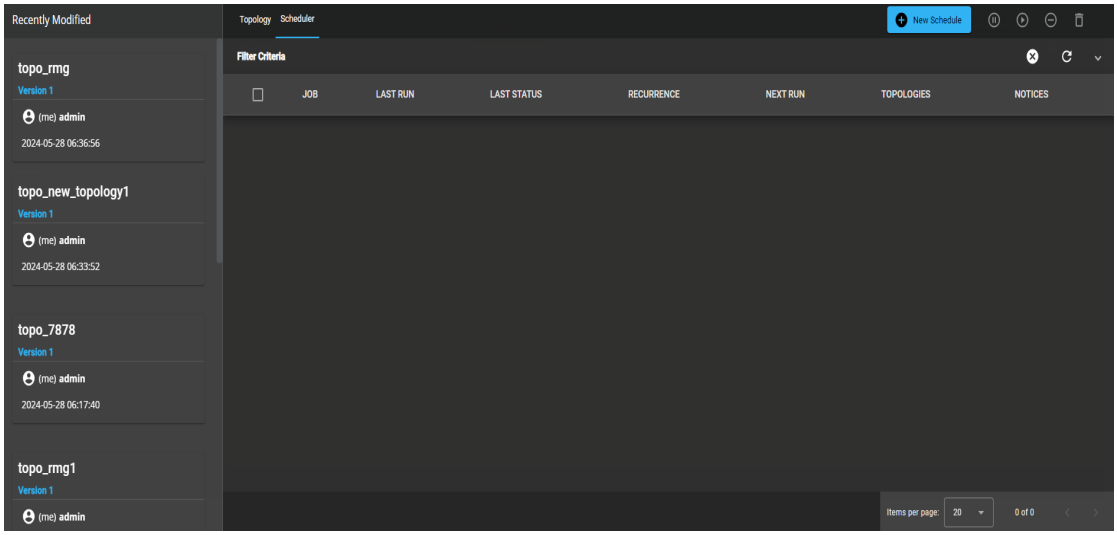
Publish/unpublish configuration changes can be scheduled from the PFS Fabric Manager. The user can schedule configuration changes for one or more topologies together in a single scheduler with mixed publish/unpublish operations.

The Deploy lifecycle main landing page has two tabs: Topology and Schedule.

Topology Tab



Schedule Tab



Managing Scheduled Jobs

From the Schedule tab, the user can view, add or delete scheduled jobs.

The Plus (+) icon allows the user to add a new job and the Trash icon allows to cancel jobs or delete/cleanup old ones.

Click on a table row to edit an existing job or view its status.

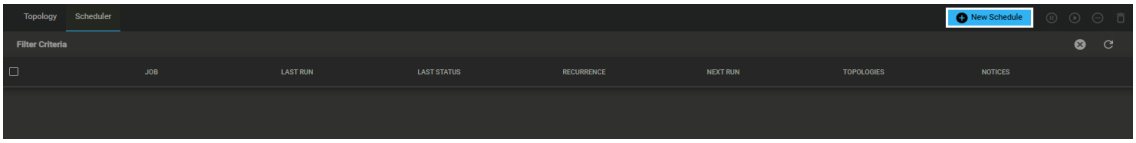
The table lists all jobs, including completed jobs to see their status. After reviewing the status, users should delete those jobs by clicking on the Trash icon.

Creating a Scheduled Job

There are two ways to schedule topology configuration changes:

- Click on the Plus (+) icon at the top right corner.
- Navigate to a specific topology, click on the Cloud icon and select Schedule.

Plus (+) Icon



Cloud Icon

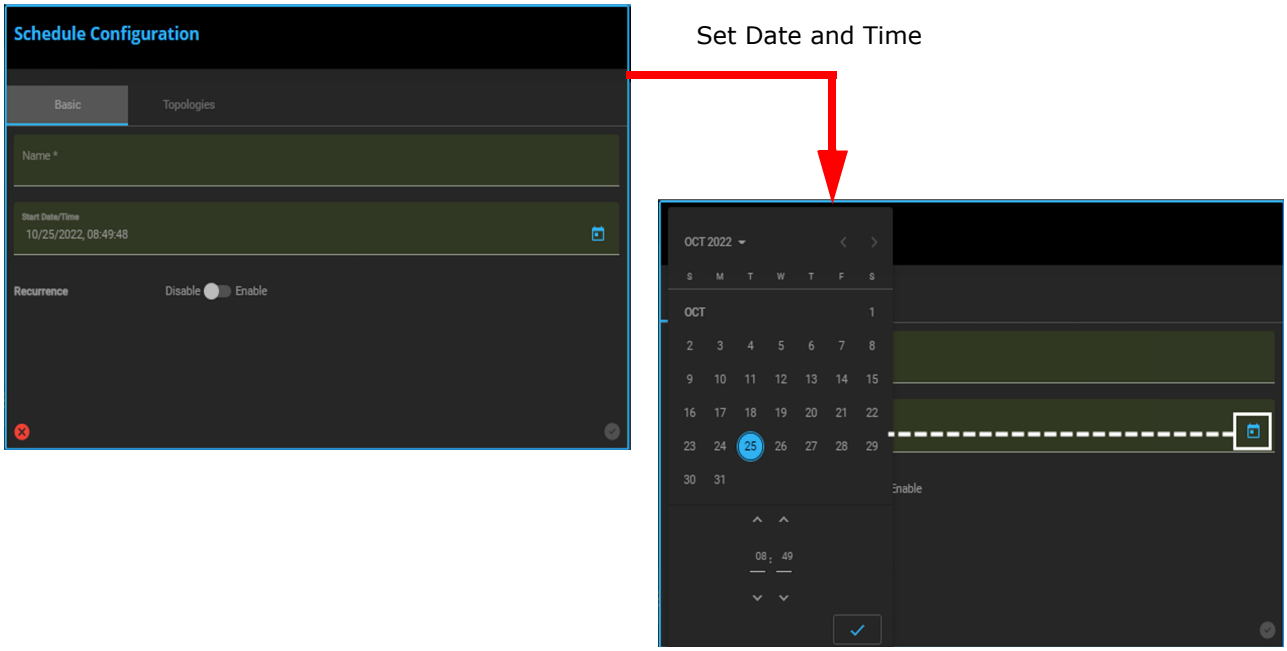
A Topology Schedule screen is displayed, where users can select the **Start Date/Time** for the job and **Recurrence**, if needed, on the **Details** tab. The user then selects topologies and the operation for each on the **Topologies** tab.

> **Note:** If a user comes to this screen from a specific topology, then that topology and version are preselected on the slideout.

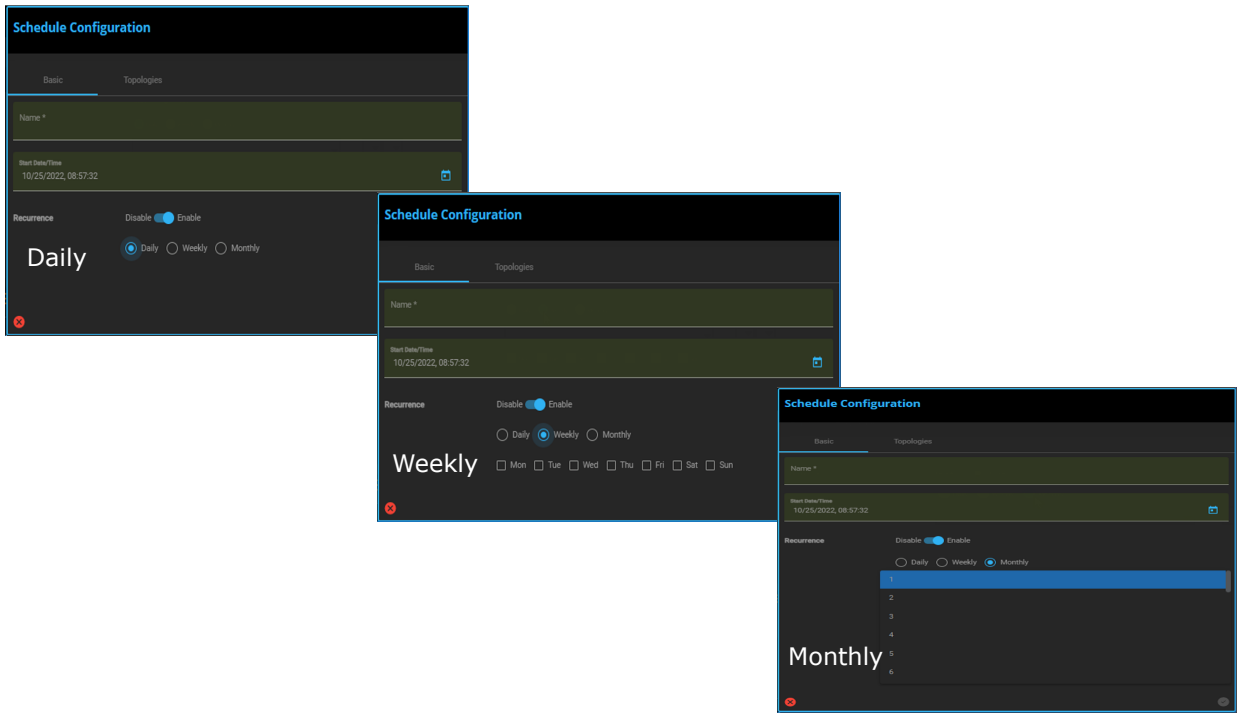
If recurrence is disabled, then users just need to select the date/time.

If recurrence is enabled, then users need to select date/time and other parameters based on the recurrence type.

There is no end date for the job. The user has to pro-actively cancel the job if it is no longer required.



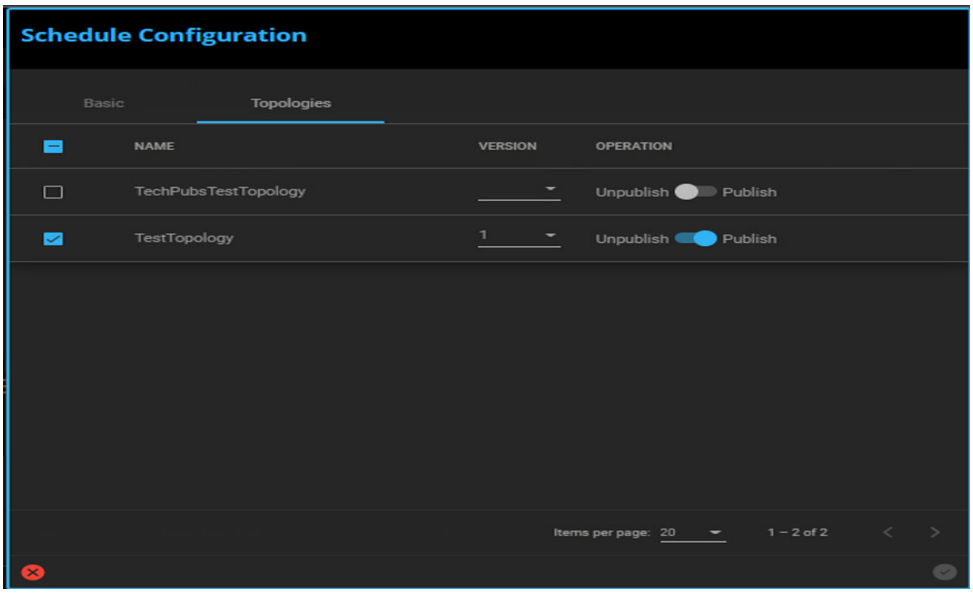
There are several options if the user enables the **Recurrence** option.



After the scheduled date is set, the user needs to select topologies and the operation: publish or unpublish.

Navigate to the **Topologies** tab on the Topology Schedule screen, to select specific topologies/versions to be publish or unpublished.

The table lists all available topologies and their versions. The user needs to click on the check box for the specific topologies and then select the operation for each topology.



Editing a Scheduled Job

To edit an existing scheduled job, click on a specific scheduled job in the summary table. The Topology Schedule screen is displayed with pre-populated fields.

The user can change the job settings, cancel the job, pause the job, or resume the job (if the job is not in progress). The Cancel and Pause options are provided with a confirmation dialog, based on user input action will be taken. If it is yes Job will be canceled/paused else it will be scheduled as before without any change.

The job is not executed if it was paused and the scheduled date/time has passed. In a case where the job is recurrent, the job will resume execution as per schedule after it was started again. The job is canceled and marked as Expired if the job is not recurrent and the scheduled date/time has passed.

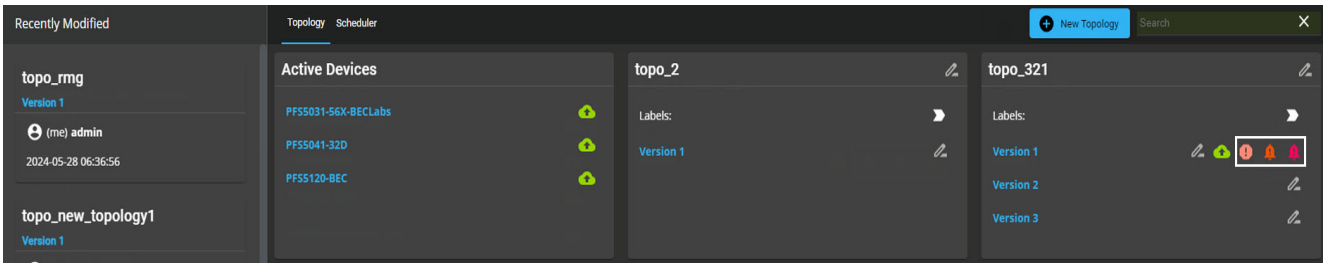
Viewing a Scheduled Job Status

A detailed status is available for a scheduled job after the job has been started or is already completed.

Topology > Alarm Indicators

Topology alarm indicators are shown only in published user topology not in device topology.

Topology alarm indicators are shown at the Topology summary level, port node level, and flow node level.

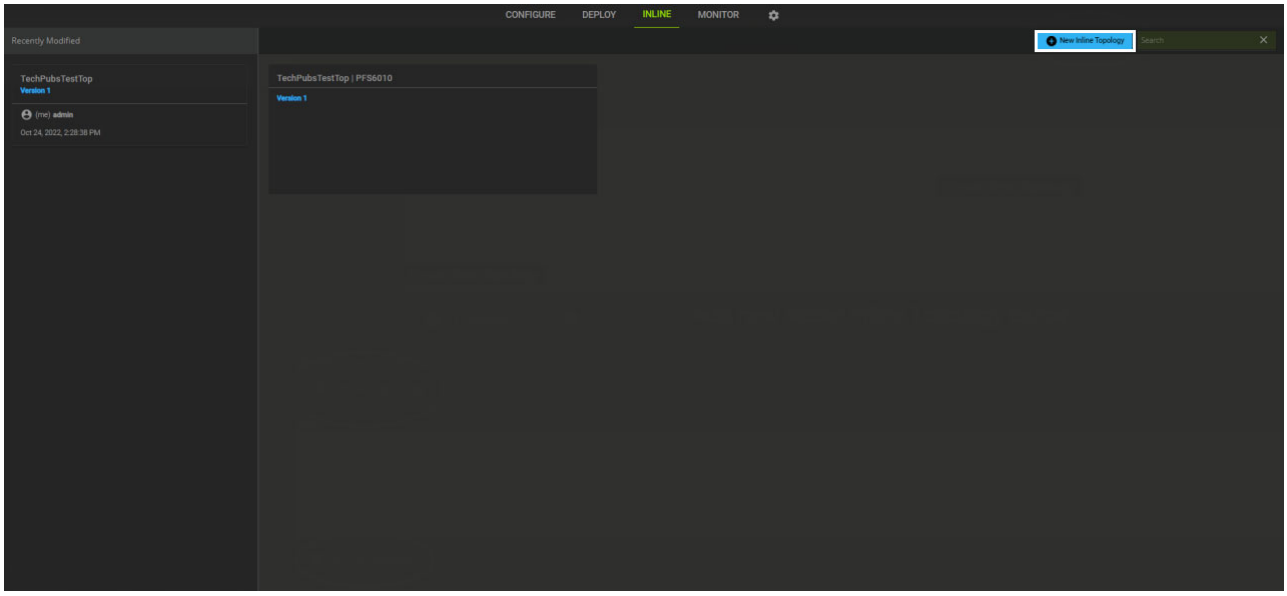


Chapter 5
Inline Lifecycle

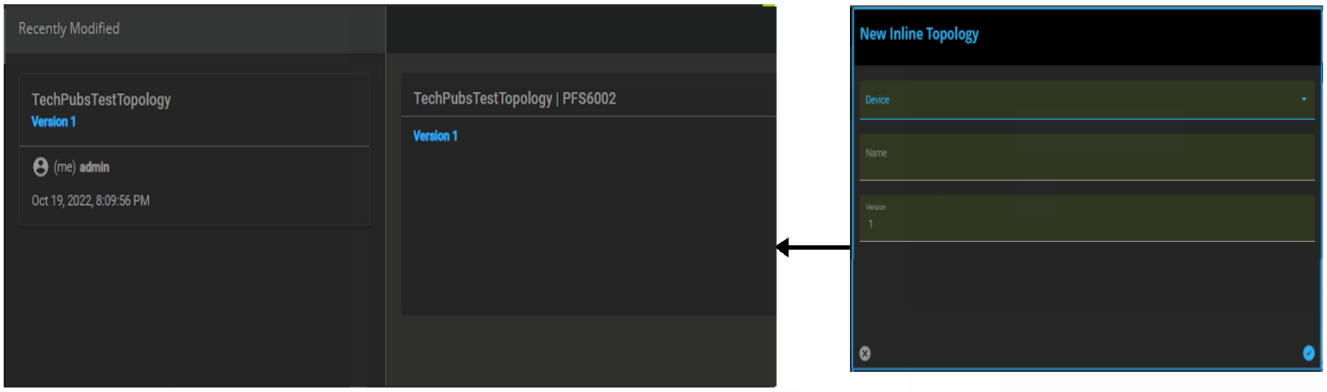
This chapter describes how to create inline network topologies in PFS Fabric Manager.

Assign a New Inline Topology

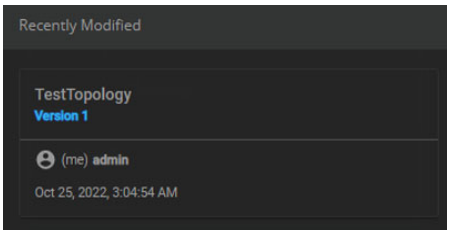
From the interface screen, select Inline then click on New Inline Topology - a new Inline Topology screen displays.



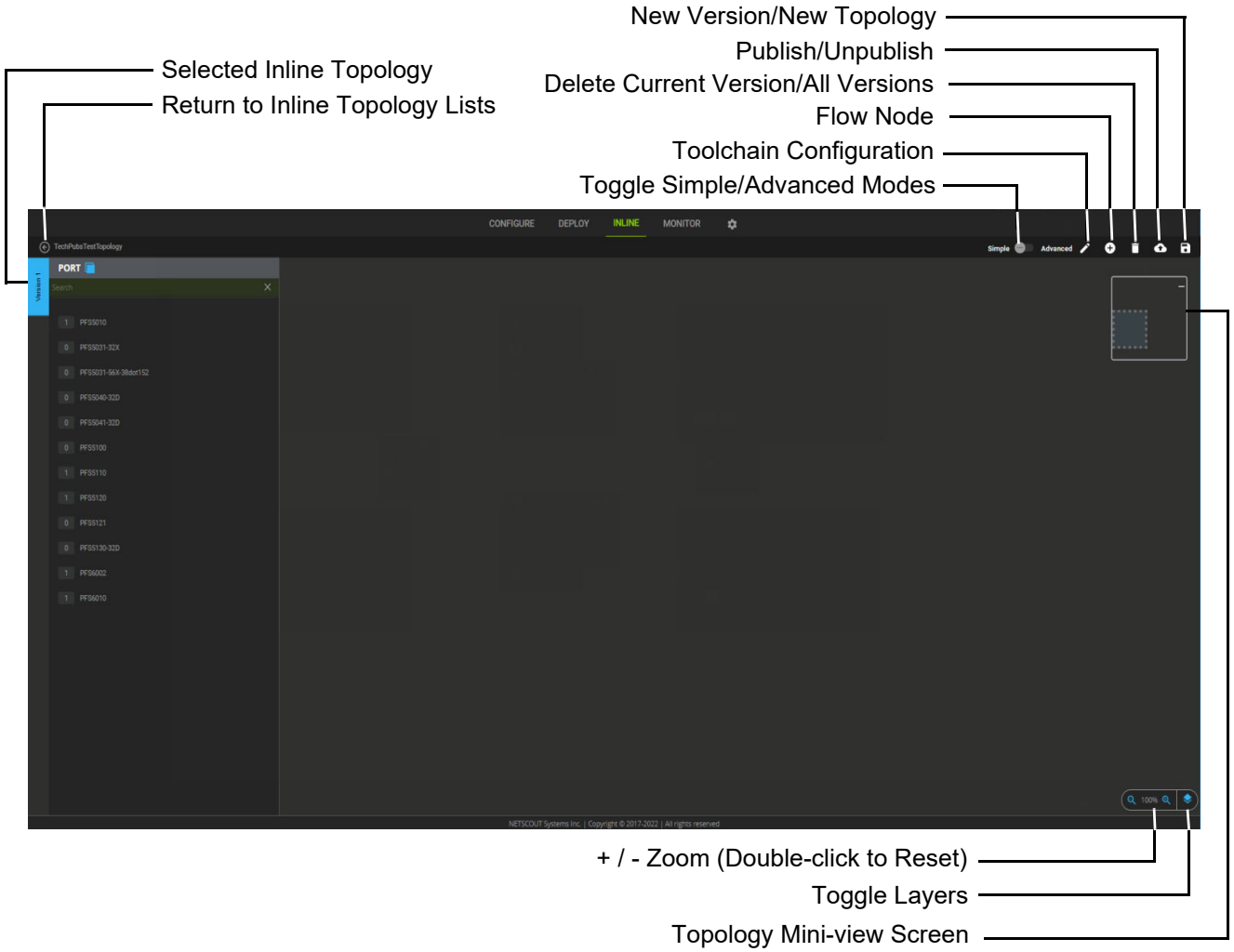
Enter a name plus any additional information for the new Inline topology then accept (check mark) the topology. The new topology is now listed.



Click on the topology title to open the main topology screen.



Inline Topology Screen / Features

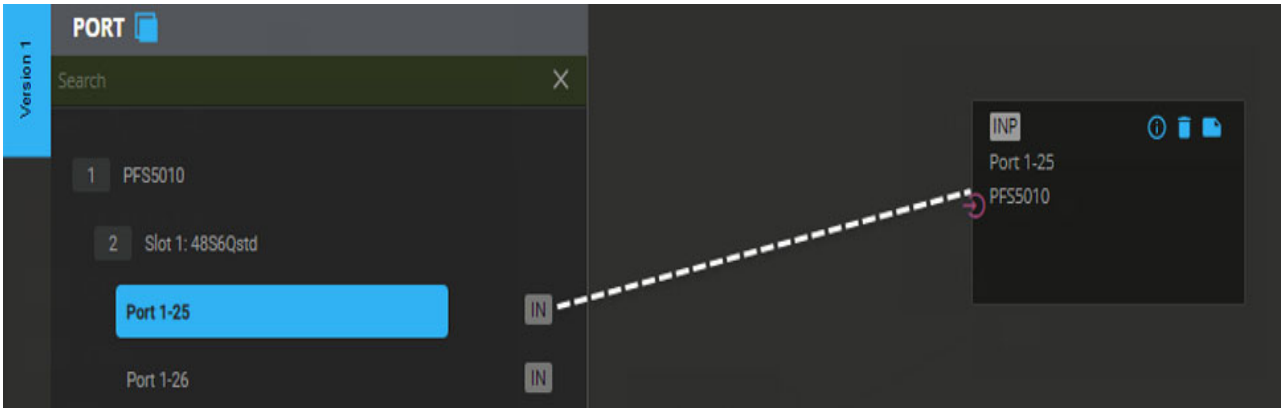


Creating an Inline Topology

After you have assigned a new Inline topology, you can begin creating a topology.

From the Perspective > Port menu, select a line card port and drag the port to the topology screen. For each port bought onto the screen, a separate port node is added.

> **Note:** After the port has been dragged to the topology, the port's configuration on the topology is now local to that topology. Any further configuration changes to the port, in the Configuration lifecycle or other topologies, will not affect the port's configuration on the current topology. To refresh the port's configuration on a topology, remove it from the topology and then add it again.



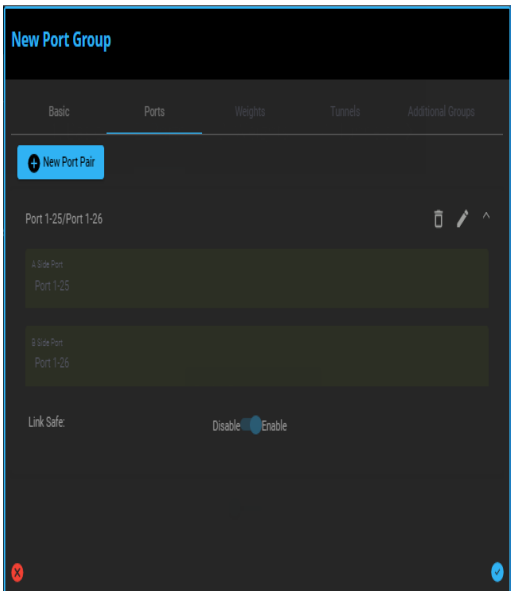
Inline Ports and Groups

Inline ports and groups can be defined from the Configure lifecycle or learned from PFOS. Inline port and group types include Inline Network and Inline Monitor.

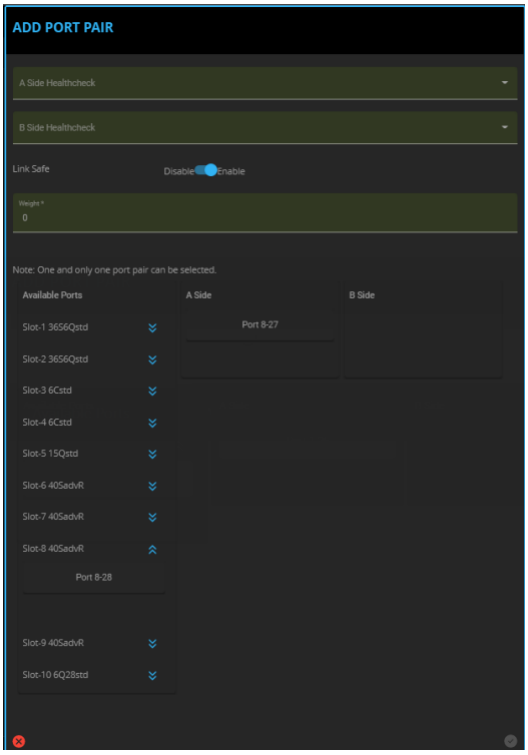
Inline port configuration from the configure lifecycle behaves just like other port configuration. Changes are published immediately when submitted after validation is complete. Validation depends on group membership and published maps or topologies.

Inline groups are represented as a new group type in fabric manager.

Inline network groups have a set of port pairs, each with a link safe and weight setting. VLAN tagging can also be configured for the group. For each pair, an "A Side" and "B Side" port is required. When an "A Side" port is added, the "B Side" port will default to the next port.



Inline monitor groups also have a set of port pairs, each with a link safe setting. Either an "A Side" or a "B Side" port must be configured. For each port in the pair, a health check library can be assigned.

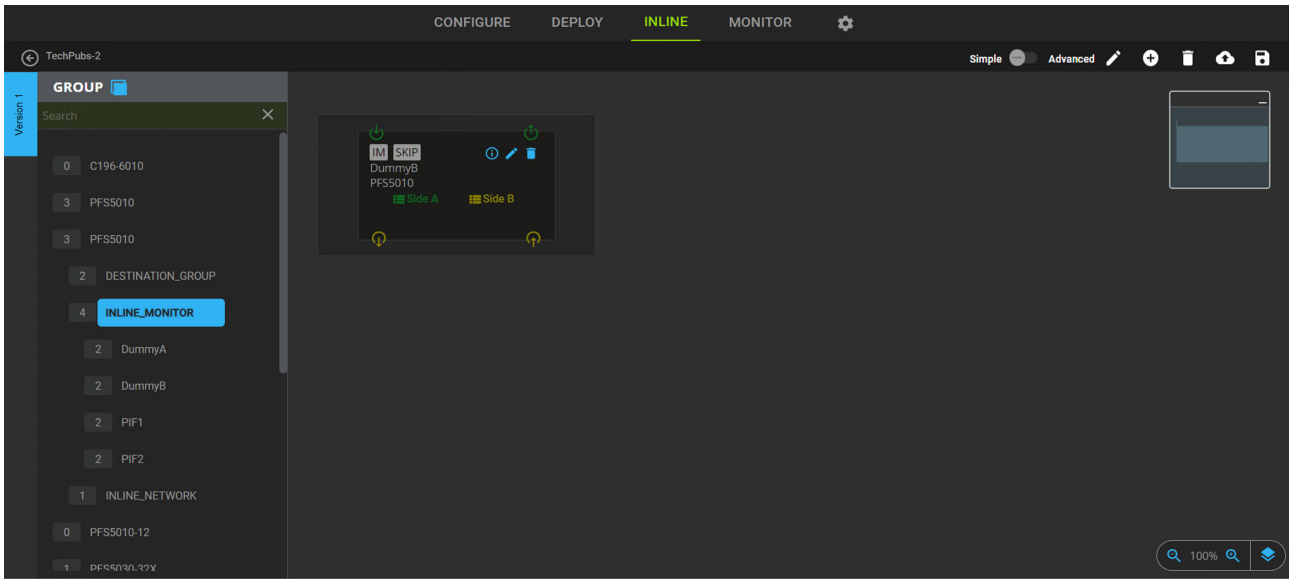


When viewing Inline groups from the Configure lifecycle, Inline topologies and triggers where the group is used should be listed, with links to navigate to the topology or trigger respectively.

Inline Topology Overview

Each inline topology contains a single toolchain. The toolchain is represented as a grouping of tools, each representing an Inline monitor group on the topology.

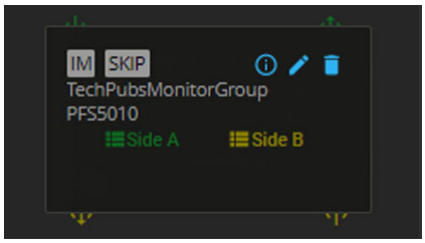
New tools can be added to the toolchain, by dragging Inline monitor groups from the group perspective. By default, each tool will have a "Next Tool" connection to the next tool in the chain. Tools can be reordered with drag and drop or removed, when the toolchain is in edit mode. Toolchain configuration has defaults which can be overridden.



Inline traffic maps can be defined by dropping inline network groups onto the canvas. Each port group will be automatically connected to the toolchain, with a default nonmatch "A Side" and "B Side" filter. Additional inline traffic maps can be defined by adding "A Side" and "B Side" flow nodes or dropping filters on the canvas.

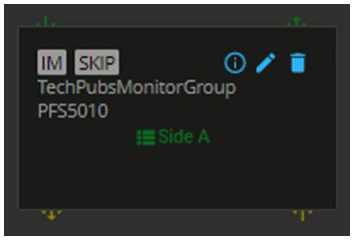
When filters are dropped onto the canvas, a flow node will be created and can be used as "A Side" or "B Side" filters in a traffic map or in "Next Tool" connections within the toolchain.

The group node can be expanded to show all port pairs belonging to the group.

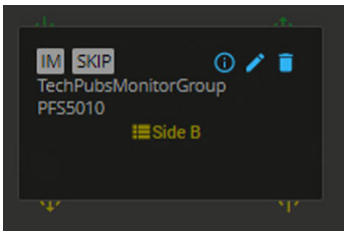


The toolchain can also be collapsed to focus on connections

By clicking on the Toggle filters icon (lower right corner), users can hide A Side or B Side to simplify the current view



OR

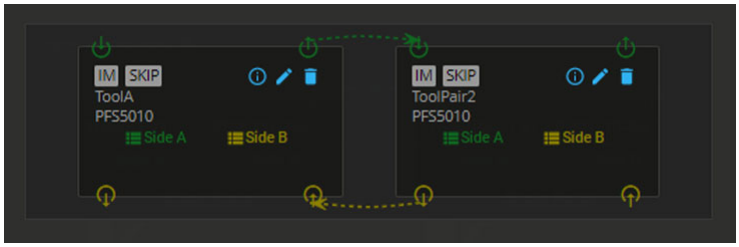


Passive Monitor groups can be dropped onto the topology canvas for use in toolchains or inline maps.

Port or port group configuration is not available fromInline topologies, unlike standard topologies where ports can be configured globally or locally.

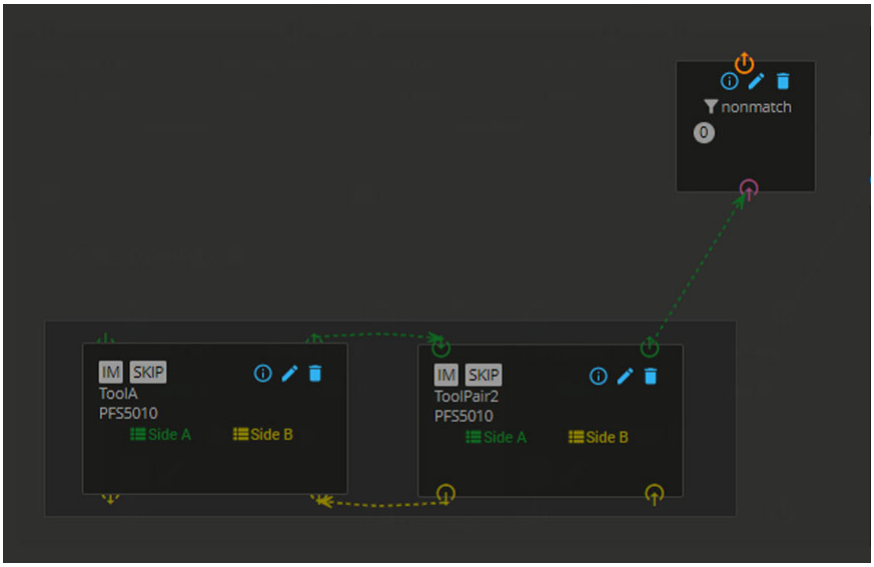
Inline Topology Connections

Next Tool connections can be created by drawing connections from one tool's A Side or B Side egress endpoint to another tool's same side ingress endpoint. In this case, the connection will default to a nonmatch filter. For these connections using nonmatch filters, no filter will be displayed to improve layout. Nonmatch rules drawn in this way are always applied last. Filter nodes can have a nonmatch filter applied, in which case normal precedence rules apply.



Additionally, connections can be drawn from a tool's egress endpoint to a flow node. This connection will use the filter defined on that flow node. The filter can be changed by dragging another filter from the perspective onto the node or using the configure option from the hover menu. VLAN options can also be configured from the flow node.

When a Next Tool connection is drawn to a flow node, with no return to any tool, the connection will result in a last tool rule and exit the tool chain if hit. This last tool rule is the bypass case. Graphically, this is represented as a connection back to the Iinline network group. If no group is present, meaning no traffic maps are configured, the connection will terminate in a special end flow icon.



Connections can be drawn from a flow node to a tool's ingress node, to modify the last tool rule to use a next tool. It is required to draw a connection from a tool to the flow node before drawing a connection from the flow node to a tool. The connection from the tool to the flow node defines if the rule is on the A Side or B Sid and that is it used in a Next Tool connection, not as a traffic map A Side or B Side filter. Existing connections define validation for additional connections to the flow node. Additionally, connections can be drawn from the flow node to an Inline network port, if the switch is running PFOS 5.6 or greater.

Multiple Next Tool connections can be defined for each tool in a toolchain. Users can define the order of how these rules will be published using the precedence configuration of each flow node.

Additionally, connections can be drawn from tools directly to passive monitor groups (one per tool). Users can drop monitor groups onto topology, then draw connections from A Side or B Side egress endpoints to the group. It is also possible to draw connections from an A Side or B Side filter flow node, which is connected to an Inline network port group, to the passive monitor group. This will define the group's use in the traffic map.

Flow Nodes

Flow nodes will allow the following configuration when connected directly to tools:

- Filter
- VLAN options
- Precedence

Flow nodes will allow the following configuration when connected directly to inline network groups:

- Filter
- Precedence
- LB criteria

Inline Topology Publication

Just like standard (monitor) topologies, none of the configuration on an Inline topology will be pushed to the PFOS switch until the topology is published. When an Inline topology is published, all relevant configuration is pushed to the device, if required, and marked as published to that device.

Port Groups

Just like standard topology behavior, port groups are published on demand. Groups are published to PFOS only when used on a topology of either type.

Relevant port group types:

- Inline Monitor
- Inline Network
- Passive Monitor

Filters

Filters behave like port groups. Filters are published to PFOS only when used on a topology of either type.

Tools

A tool will be created for each inline monitor group on the topology.

Toolchain (one per topology)

A toolchain will be created for each published topology. The name of the toolchain will be the same as the name of the topology. "Next Tool" rules will be derived from the connections on the inline topology.

Inline Traffic Maps

For each inline network port group on the topology, at least one traffic map will be created. Each set of "A Side" and B Side" filters connected to the inline network group will result in a traffic map.

Several options will be configurable for each map:

- Failover mode
- Forward, drop, bypass
- Failover mode

It is legal to publish inline topologies with only toolchains and no traffic maps, meaning no inline network groups are present on the topology.

Inline Topology Versioning

Inline topologies are versioned just like standard (monitor) topologies. Only one version of a topology can be published at a time. When a new version is published while some other version of the same topology is currently published, the behavior mirrors standard (monitor) topology publication. A delta is calculated between the two topology versions to affect the change.

- Entities which are present only on the old version will be unpublished.
- Entities which are present only on the new version will be published.Entities which are present on both versions will be untouched.
- Each relevant entity will be published or unpublished accordingly.

Note: The publication key of a toolchain will match the name of the Inline topology, with no version or UUID.

Learning

Toolchains can be learned from PFOS either during initial learning or due to configuration in the CLI or PFOS WebUI. In this case, the toolchain will be learned as the next version of an Inline topology by the same name. This topology will be marked as published.

All learned traffic maps using that tool chain, will be reflected on the topology.

If a version of the topology by the same name is already published, then the existing published topology will be changed as a result. This behavior differs from standard topologies. Standard topologies will never change as a result of learning, but instead reflect mismatches.

When a topology is created or modified due to learning, new nodes on that topology will be subject to auto-layout. Users can override this by dragging nodes to a different configuration.

Rule: for any Inline configuration in PFOS (tools, toolchains, maps), there will be a published Inline topology that reflects it.

When a toolchain is deleted from PFOS, the Inline topology will be marked as unpublished.

Chapter 6
Monitor Lifecycle

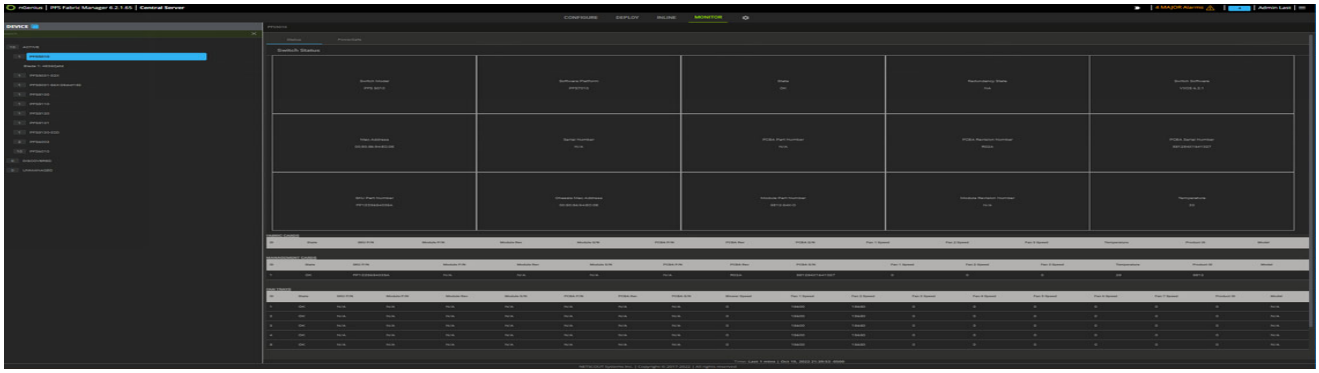
This chapter describes the switch and port monitoring functions of PFS Fabric Manager.

Monitor allow viewing system statistics from the switch, blade, pfsMesh, and port / filter levels. From the Device level, switch and blade status is displayed; from the Port level, selecting a port node displays multiple statistical data for the port; from the pfsMesh level, interconnection of multiple devices are displayed; from the Events level, Syslog History and Alarms are displayed.

Device Status

From the Perspective > Device menu, selecting an active device (switch) displays an overview graphic of the internal functions of the selected switch:

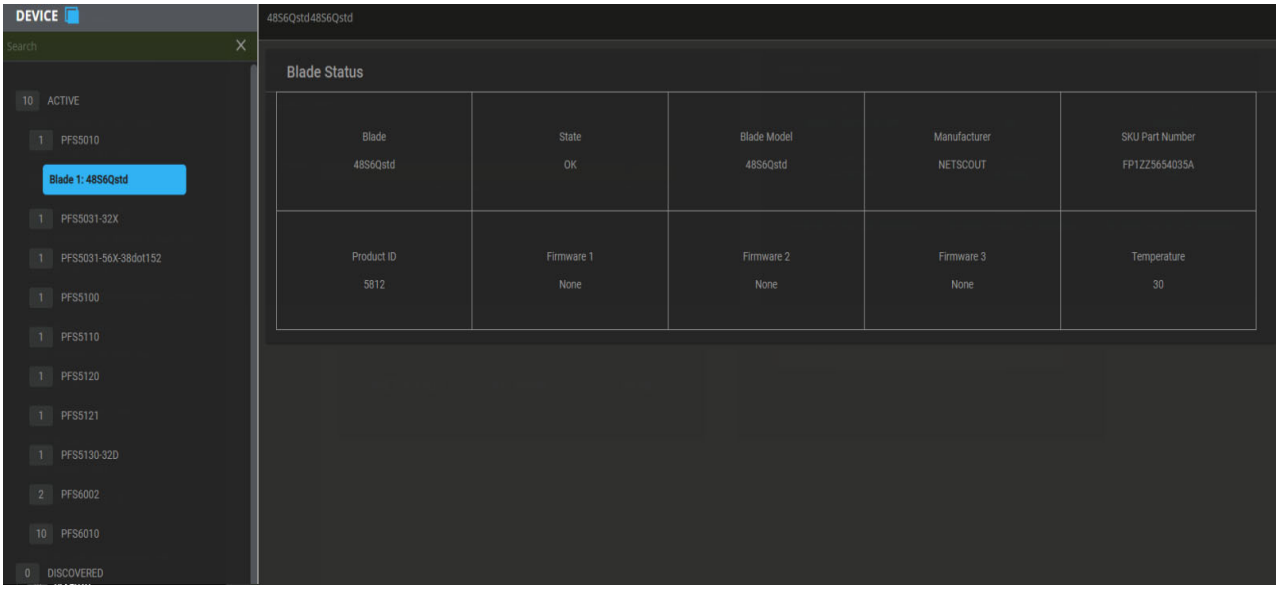
- Switch Status - lists the following:
  - Switch Model (e.g., 5010).
  - Software Platform (e.g., PFS7010)
  - State: Operating condition of switch.
  - HA State: High Availability state of switch.
  - Switch Software (e.g., VXOS 5.5)
  - Mac Address
  - Serial Number
- Fabric Status -
- Fabric Temperature -
- Management Status (Mgt Status) -
- Management Temperature (Mgt Temperature)- Indicates internal operating temperature of switch.
- Fan Status - Displays the rotational speed (in RPM) of each installed fan in the switch.



Blade Status

From the Perspective > Device menu, selecting a line card (Blade) from the blade listing of an active switch displays an overview graphic of the status of the selected blade:

- Blade Status - lists the following:
  - Blade - Type of card (e.g., 36S6Qstd-vCard1002)
  - State - Operating condition (e.g., active / inactive, online / offline)
  - Blade Model - (e.g., 36S6Qstd)
  - Manufacturer - Blade vendor.
  - SKU Part Number - Vendor part number.
  - Product ID - Blade Identifier
  - Firmware 1 -Firmware version
  - Firmware 2 -Firmware version
  - Firmware 3 -Firmware version
  - Blade Temperature - Current operating temperature of the blade.

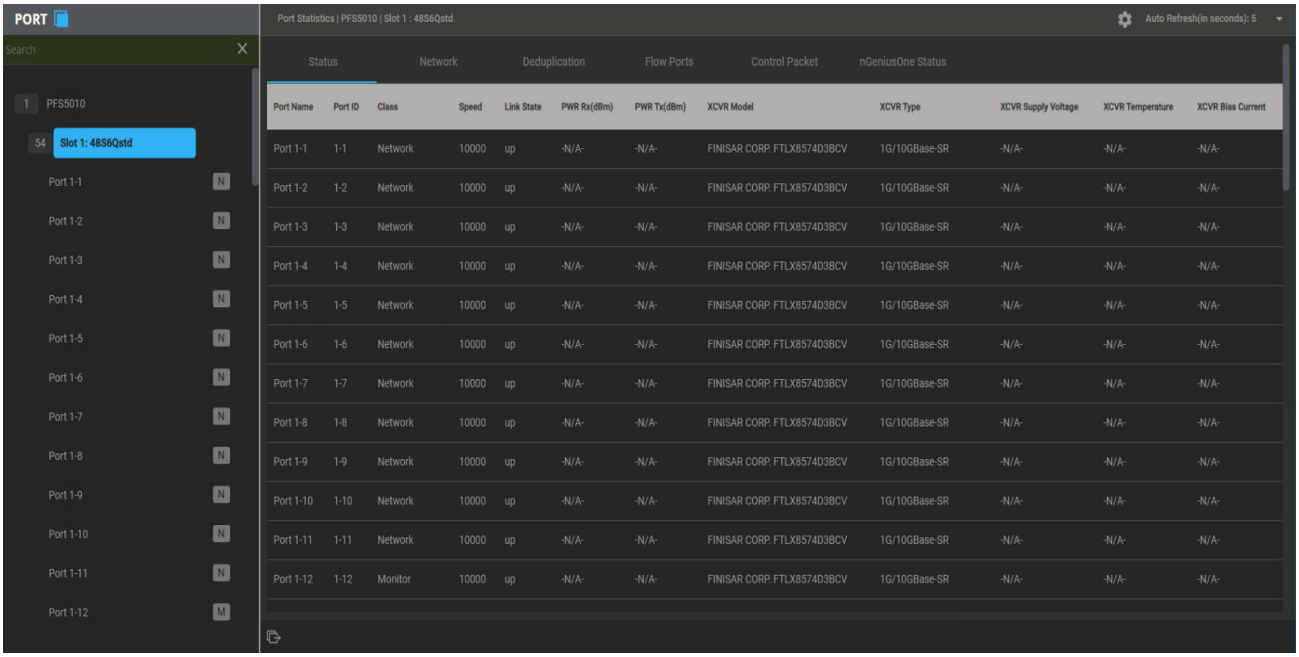


Port Monitor

Port Status Indicators

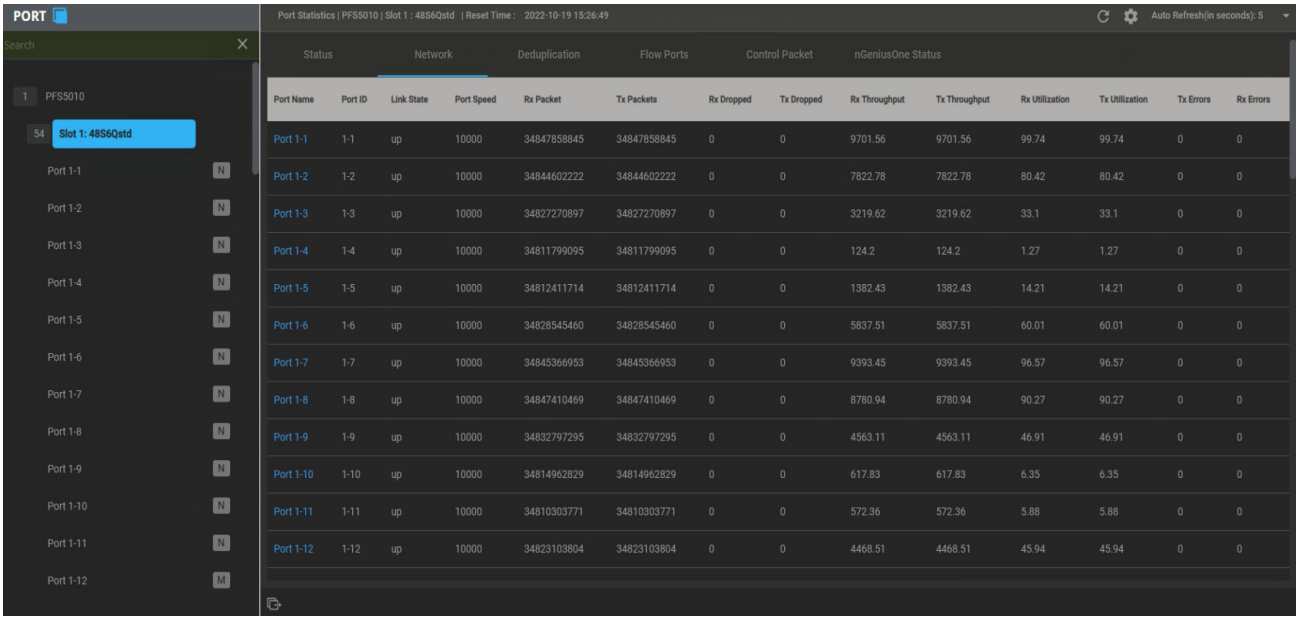
From the Perspective > Port menu, selecting a line card port automatically displays the Port Status Indicators page providing operational status for the selected port / transceiver including:

- Port Name
- Port ID
- Class - Network, Monitor, Duplex, Service, pStack, Inline Network, Inline Monitor
- Speed
- Link State - Up/Down
- Transceiver Power Receive / Transmit (Xcvr Power) - Transceiver average receiver / transmitter power levels.
- Transceiver Model (Xcvcr Model) - Transceiver model number.
- Transceiver Type (Xcvr Type) - Transceiver type (e.g. 10GBase-SR or 1G/10GBase -SR)
- Transceiver Supply Voltage (Xcvr Supply Voltage) - Transceiver operating voltage.
- Transceiver Temperature (Xcvr Temp) - Transceiver current operating temperature.
- Transceiver Bias Current (Xcvr BiasCurrent) - Operating current of the selected transceiver.



Network Statistics

From the Perspective > Port menu, selecting a line card automatically displays the Port Statistics page providing the port information for the ports configured on the line card. The user can select from Status, Network, Deduplication, Flow, and Control Packet.



Port Name	Port ID	Link State	Port Speed	Rx Packet	Tx Packets	Rx Dropped	Tx Dropped	Rx Throughput	Tx Throughput	Rx Utilization	Tx Utilization	Tx Errors	Rx Errors
Port 1-1	1-1	up	10000	34847858845	34847858845	0	0	9701.56	9701.56	99.74	99.74	0	0
Port 1-2	1-2	up	10000	34844602222	34844602222	0	0	7822.78	7822.78	80.42	80.42	0	0
Port 1-3	1-3	up	10000	34827270897	34827270897	0	0	3219.62	3219.62	33.1	33.1	0	0
Port 1-4	1-4	up	10000	34811799095	34811799095	0	0	124.2	124.2	1.27	1.27	0	0
Port 1-5	1-5	up	10000	34812411714	34812411714	0	0	1382.43	1382.43	14.21	14.21	0	0
Port 1-6	1-6	up	10000	34828545460	34828545460	0	0	5837.51	5837.51	60.01	60.01	0	0
Port 1-7	1-7	up	10000	34845366953	34845366953	0	0	9393.45	9393.45	96.57	96.57	0	0
Port 1-8	1-8	up	10000	34847410469	34847410469	0	0	8780.94	8780.94	90.27	90.27	0	0
Port 1-9	1-9	up	10000	34832797295	34832797295	0	0	4563.11	4563.11	46.91	46.91	0	0
Port 1-10	1-10	up	10000	34814962829	34814962829	0	0	617.83	617.83	6.35	6.35	0	0
Port 1-11	1-11	up	10000	34810303771	34810303771	0	0	572.36	572.36	5.88	5.88	0	0
Port 1-12	1-12	up	10000	34823103804	34823103804	0	0	4468.51	4468.51	45.94	45.94	0	0

The statistics table of a specific blade can also be undocked, by clicking on the Undock icon in the lower left hand of the screen, to be displayed in a standalone window. No more than 8 undocked windows are allowed for all applications.

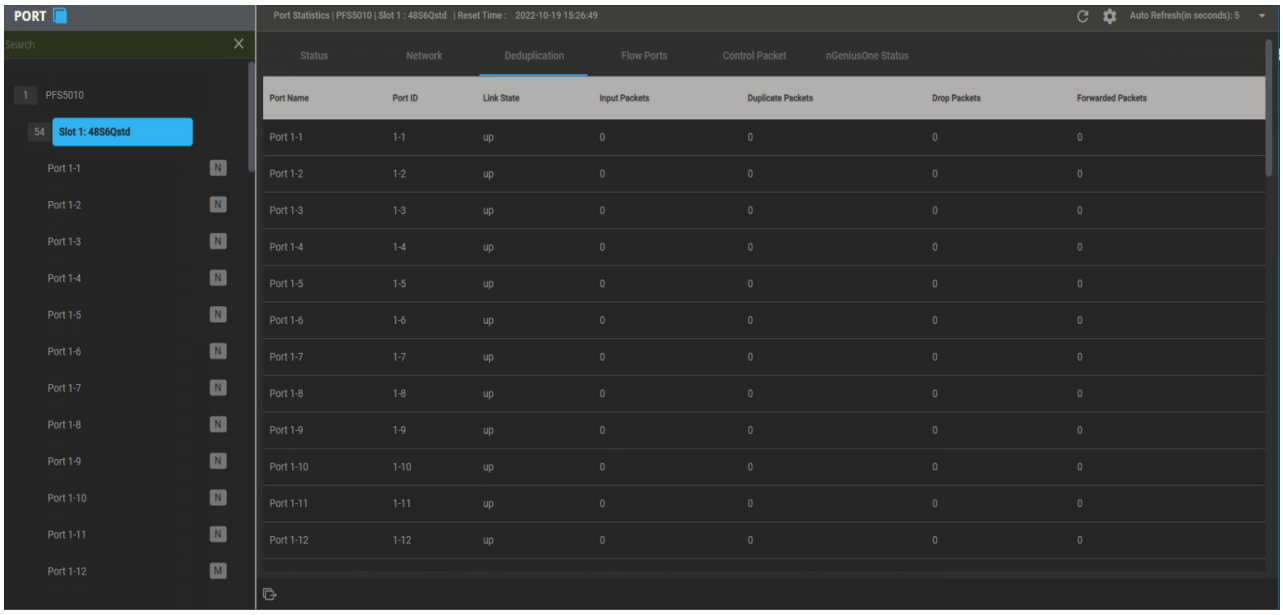
The Status, Deduplication, Flow, and Control Packet statistics tables can be modified (adding/removing columns) by clicking on the Gear icon, top right on the Tab bar.

Note: The Flow port statistics are only supported on 6000 series devices.

Deduplication

The Deduplication Packets page provides statistics for a selected port which include:

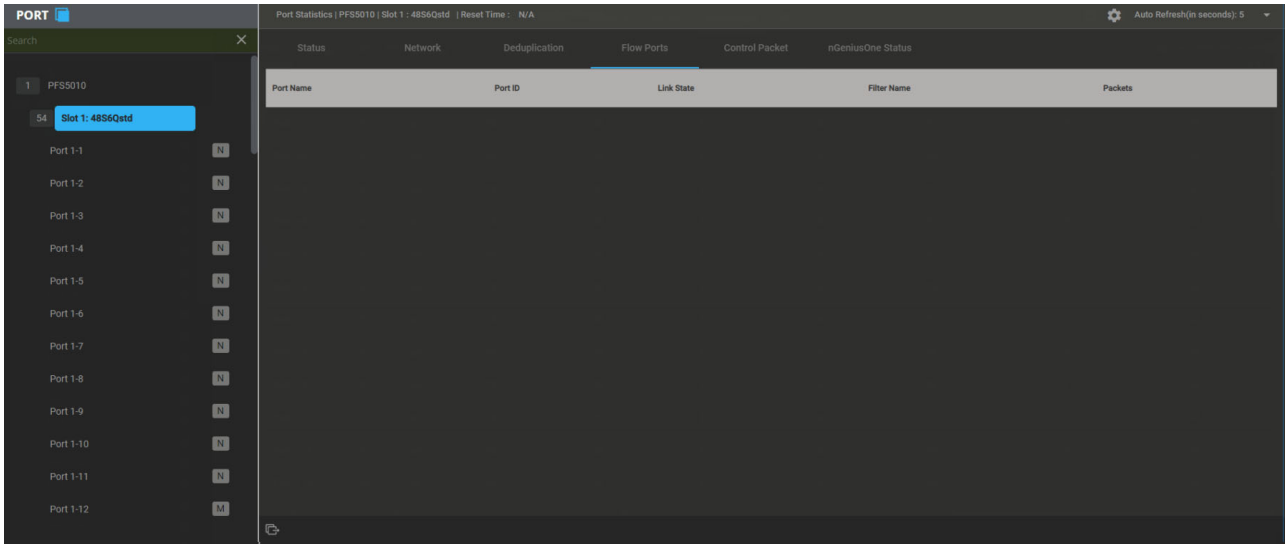
- Port Name
- Port ID
- Link State - Up/down
- Input Packets - Ingress packet count.
- Duplicate Packets - Number of duplicate packets received subject to a specified time window.
- Drop Packets - Number of erroneous packets received, whether they were duplicates or not.
- Forward Packets - Number of packets forwarded over the egress interface.



Flow Ports

The Flow Ports page provides port flow statistics for a selected port flow which includes:

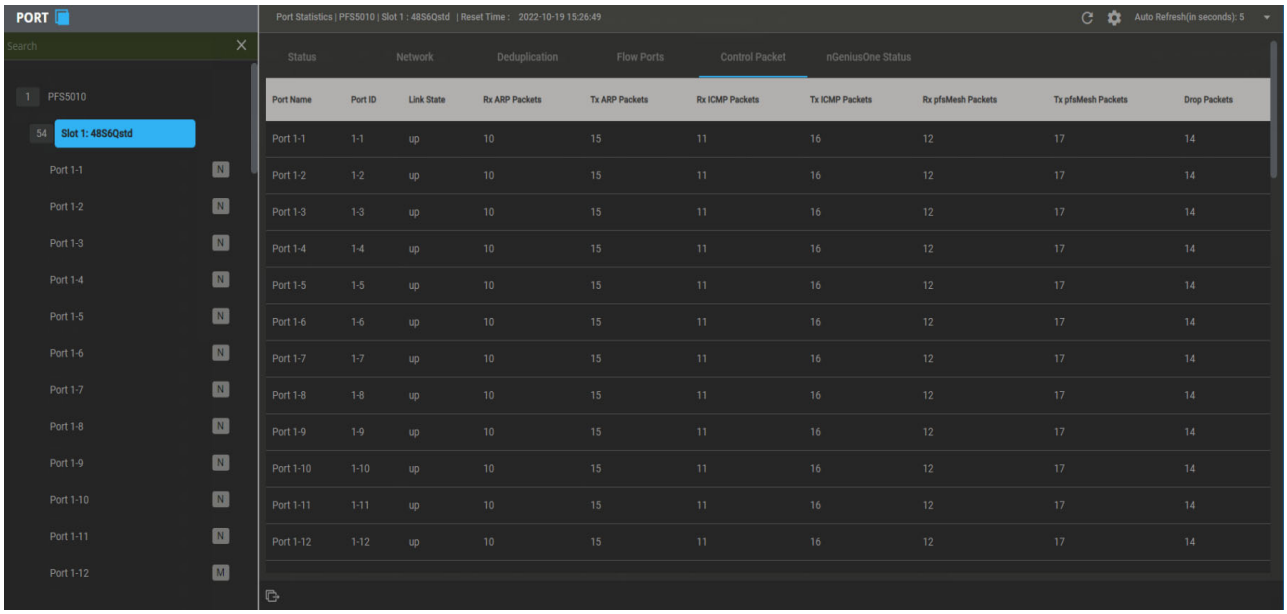
- Port Name
- Port ID
- Link State - Up/down
- Filter Name
- Packets - Flow Ports packet count.



Control Packets

The Control Packets page provides control packet statistics for tunnel termination for a selected port which include:

- Port Name
- Port ID
- Link State - Up/down
- ARP Packets (Tx/Rx) - Address Resolution Protocol (ARP) packet count.
- ICMP Packets (Tx/Rx) - Internet Control Message Protocol (ICMP) packet count.
- pfsMesh Packets (Tx/Rx)
- Drop Packets - Dropped packets, either excessive or checksum failure packets.



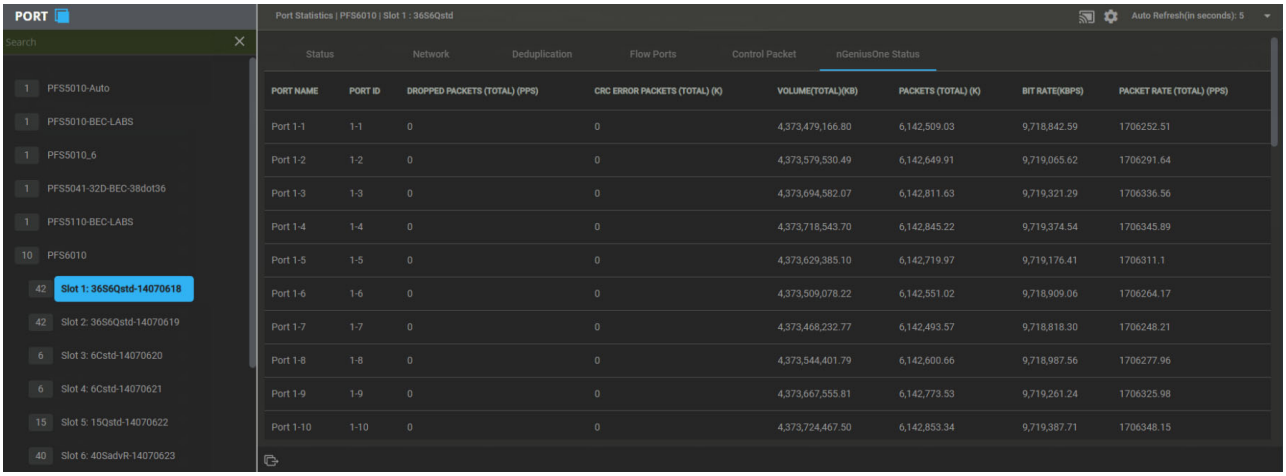
nGeniusOne Status

Note: At the time of publication and software release, the PFS-FM integration with PFS Monitor/ nGeniusOne functionality is being released as Early Field Trial (EFT) to a specific group(s) of NETSCOUT customers until required field testing is successfully completed. Please contact your NETSCOUT representative for more information.

The nGeniusOne Status page provides nGeniusOne statistics for a selected port which include:

- Port Name
- Port ID
- Dropped Packets - Total (PPS)
- CRC Error Packets - Total (K)
- Volume - Total (KB)
- Packets - Total (K)
- Bit Rate (KBPS)
- Packet Rate - Total (PPS)

Note: More columns (metrics) are available using the Gear icon at the top right of the screen. These statistics match the PFS Monitor statistics in nGeniusOne for the specified switch - per blade level.



Click the **Connect to nGeniusOne** icon (located at the top right of the screen) to connect to nGeniusOne with the Switch as a context (launches PFS Monitor module in nG1 with the current switch selected and start/end time - aligned by 1 hour to the time at which the statistics were launched).

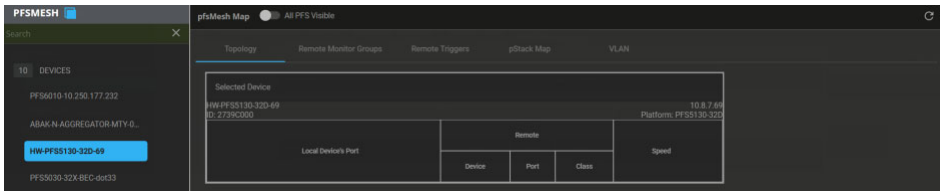
pfsMesh

From the Perspective > PFSMESH menu, selecting a device (switch) from the device listing of an active switch displays how the switches are connected.

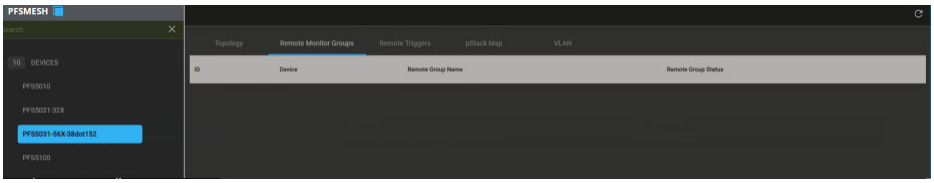
A user can click on any of the switches that are participating in pfsMesh and see the other devices that are connected to it. Depending on the Direct Connects setting, you can control what you are viewing:

- Direct Connects ON - Direct Connections:
  Displays all of the devices / ports that are directly connected to the selected device through pfsMesh.

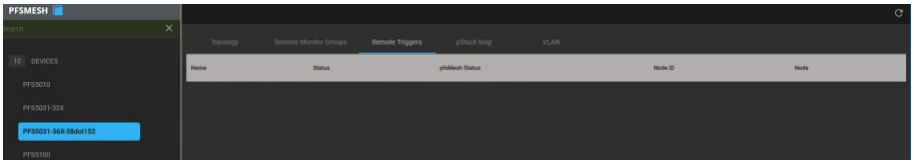
Topology Tab



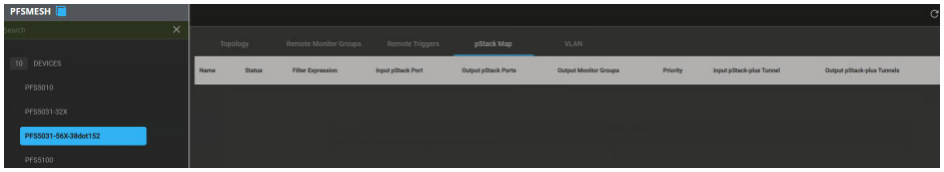
Remote Monitor Groups Tab



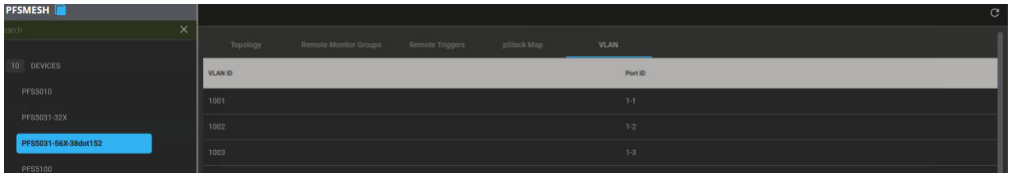
Remote Trigger Tab



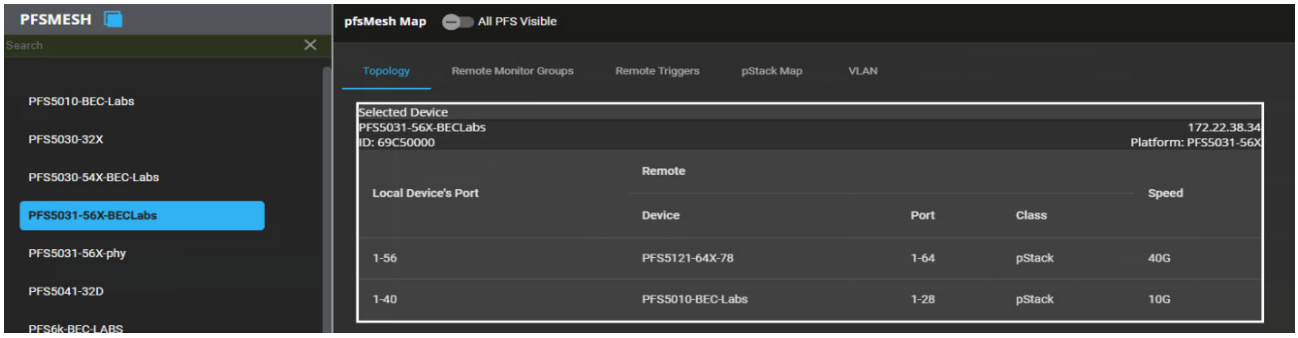
pStack Map Tab



vlan Tab

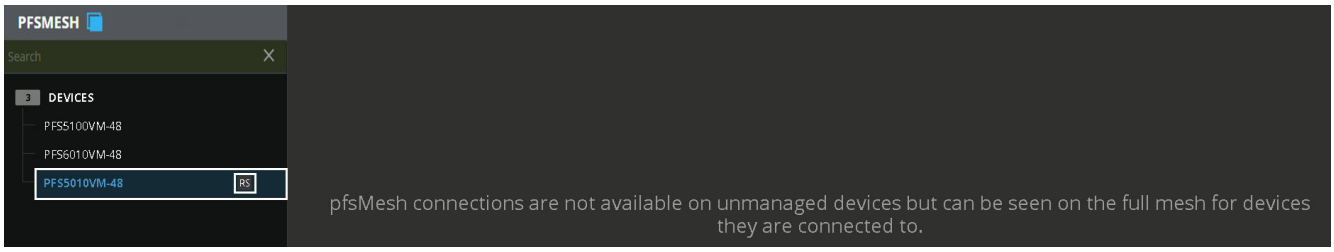


- Direct Connects Off - All Connections:
  Clicking on a device displays all of the nodes that are visible to the device via pfsMesh, regardless if the device is directly connected or not, or whether it is managed or unmanaged.



Viewing Combination of Managed / Unmanaged Devices

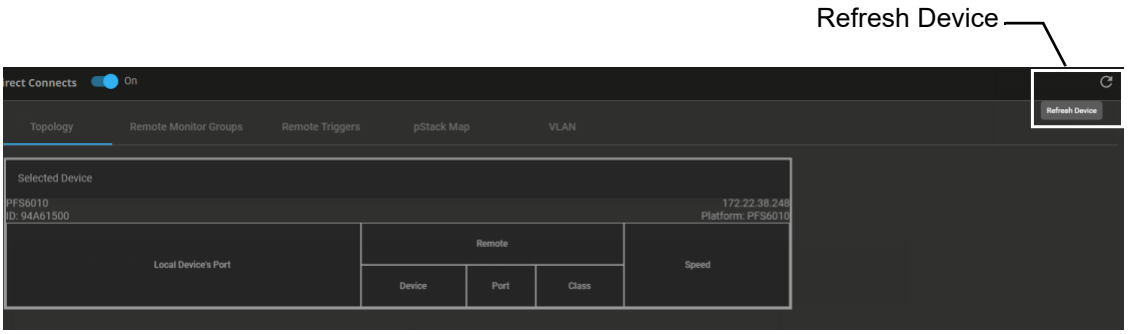
Unmanaged (remote) devices are indicated by the RS indicator next to the device name. Clicking on an unmanaged device in pfsMesh displays the following message.



However, clicking on a managed device will still show the unmanaged device as part of the full mesh of the devices where it is connected.

PFSMesh - Refresh Display

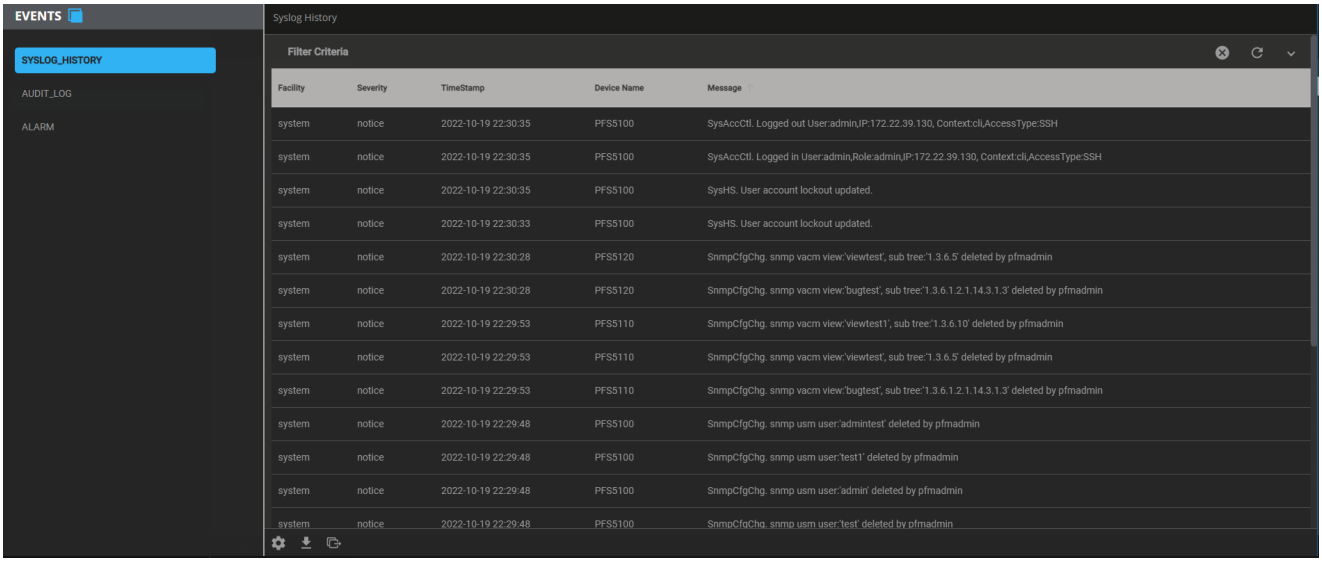
PFSMesh does not automatically refresh the information displayed from the currently selected switch. The information can be updated / refreshed by clicking on the **Refresh** icon on the pfsMesh monitor screen. You can also select an active switch to retrieve the current information.



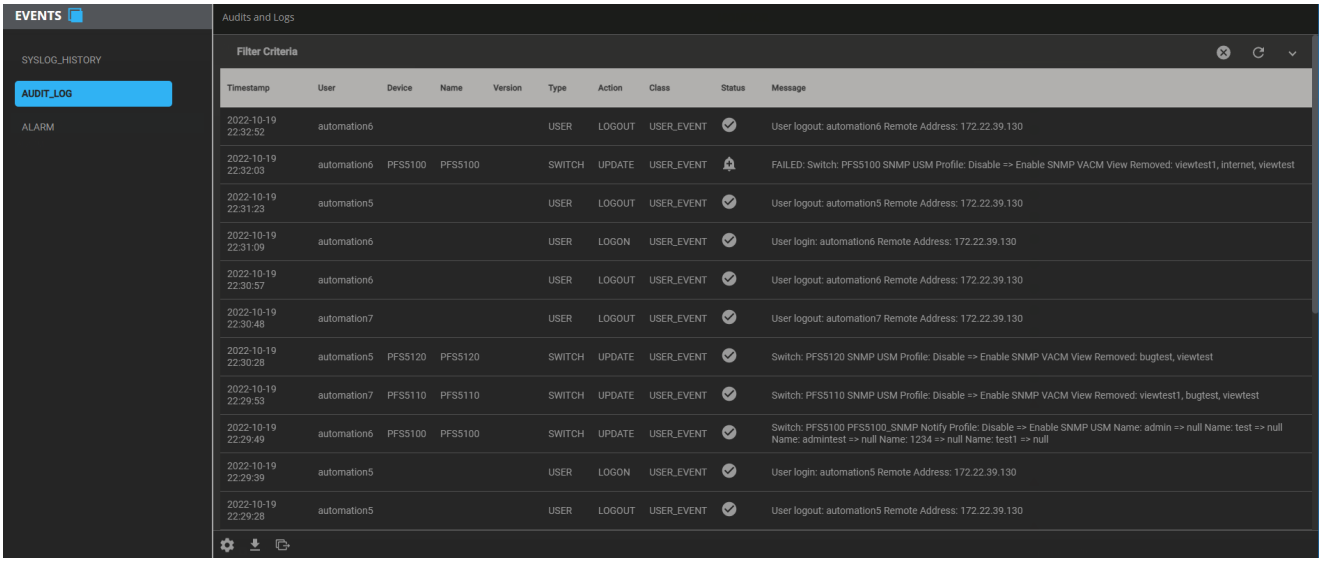
Events

From the Perspective > Events menu, the user can select to view the Syslog History, Audit Log or Alarms.

- Syslog History:
  - Displays all of the configuration changes in the device.

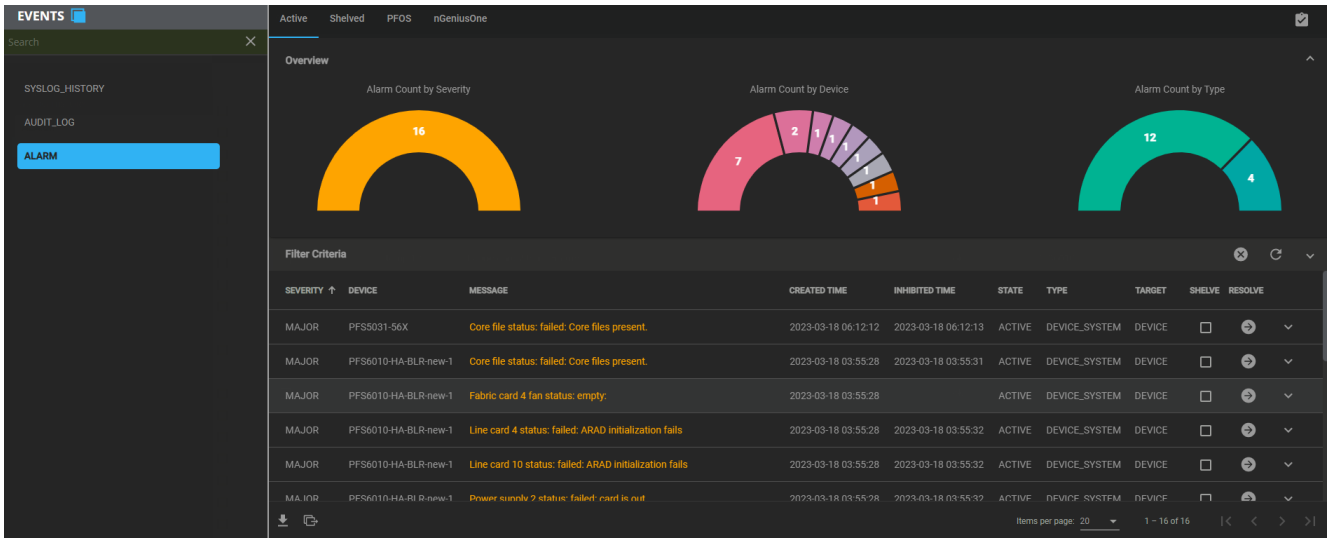


- Audit Log:
  - Displays all of the actions performed on the device.
  - Displays the class of the event: USER_EVENT or SYSTEM_EVENT

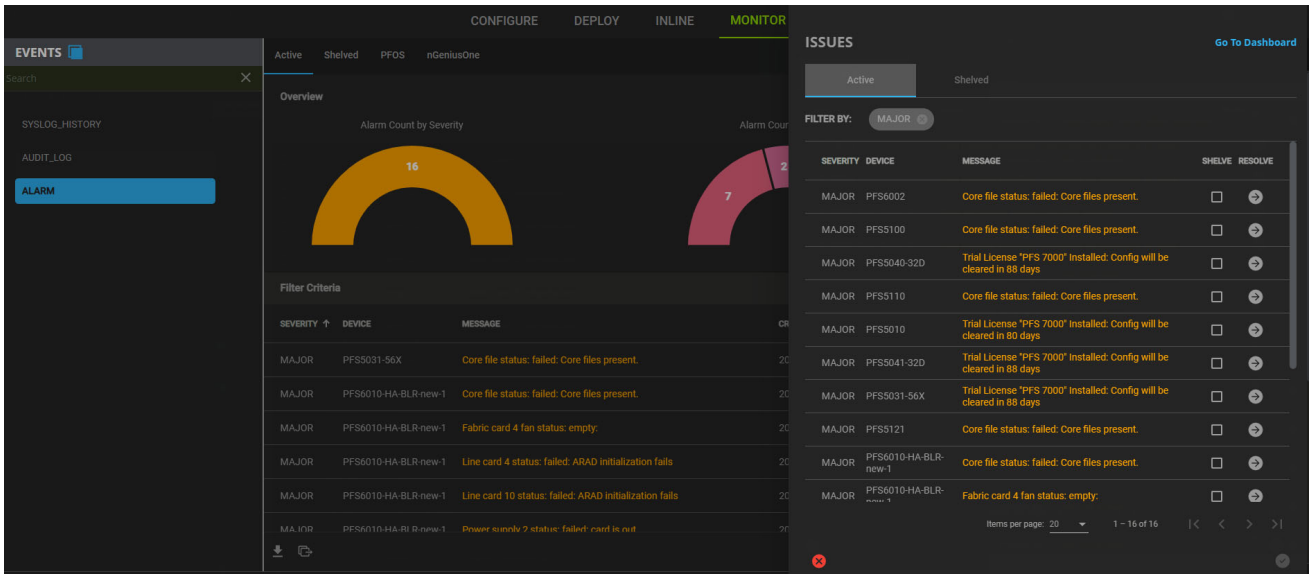


- Alarms:
  - Displays all of the Alarms present on the device.
  - Acknowledge a failed alarm entry by selecting the Acknowledge field.
  - Clean up the acknowledged alarm entry by de-selecting the Acknowledge field.
  - View the times of the displayed events and alarms in the user's time zone.
  - Shelved alarms are unshelved by clicking **UNSHELVE** check next to each alarm, then clicking **SEARCH/REFRESH**.
  - Clicking **RESOLVE** navigates the user to the context of the alarm.
  - The nGeniusOne tab displays all the device specific alarms received from nGeniusOne. This requires an active configured nGeniusOne (refer to nGeniusOne for configuration details) and for the switch to be added as a Trusted Server in nGeniusOne.

Note: The graphs on this screen are clickable. Hover over each slice to see the specific details for that slice. Clicking on the desired slice auto-filters the Alarms table (Active).

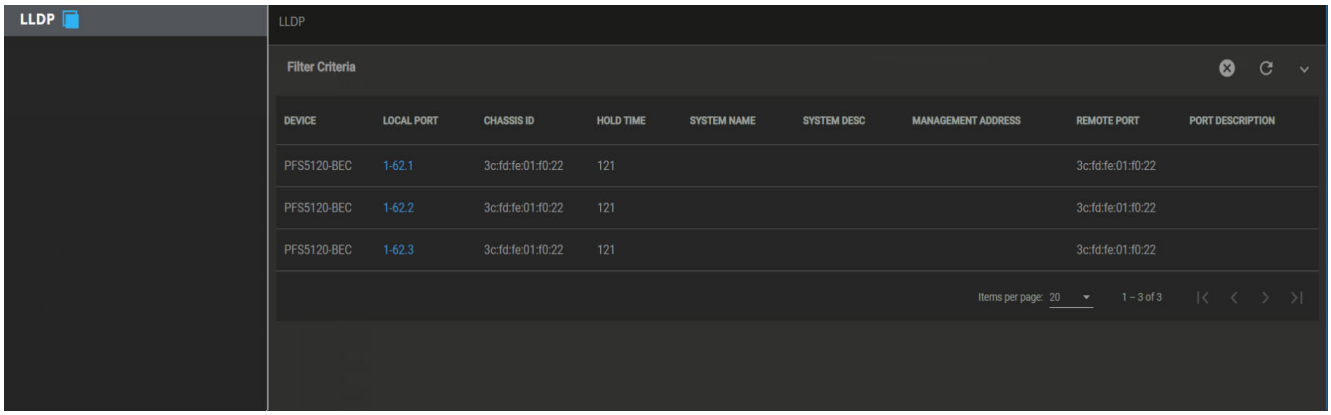


  - View the details of an alarm by clicking on the down arrow next to the alarm.

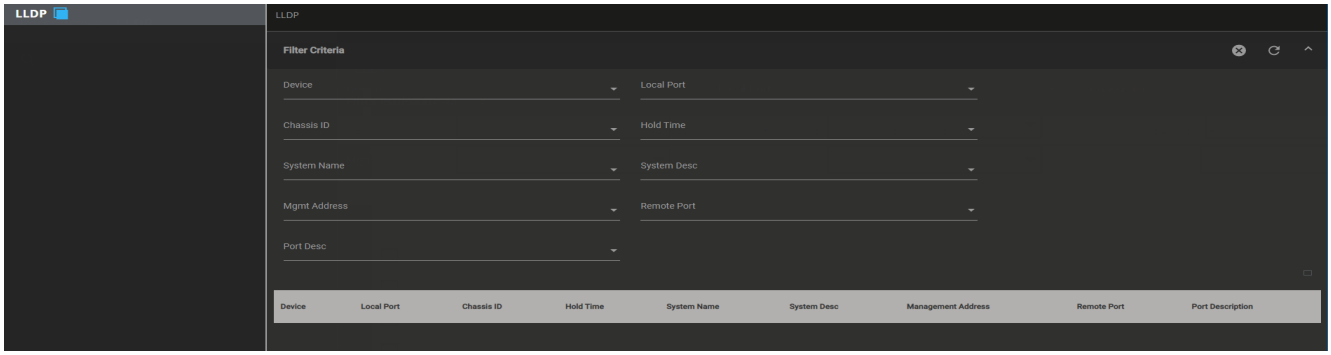


Link Layer Discovery Protocol (LLDP)

From the Perspective > LLDP menu, the user can view all of the managed devices with their corresponding information.



You can use filters to limit the information displayed for all the devices.

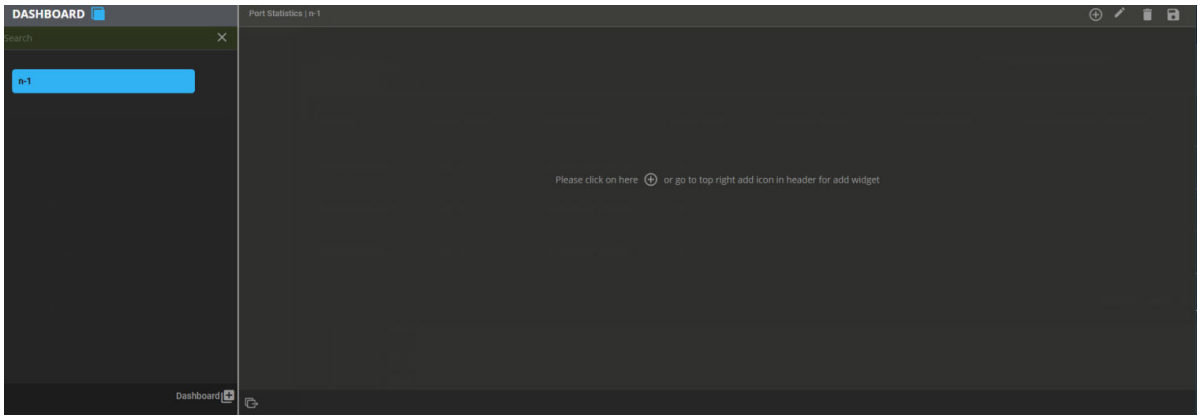


Profile Property	Description
Device	Displays the local switch name (source)
Local Port	Displays the local port details (source switch)
Chassis ID	Identifies the device
Hold Time	Displays LLDP hold timer
System Name	Displays given name for the device
System Desc	Displays version of the software
Management Address	Displays the IP or MAC address of the device
Remote Port	Displays the remote port details of the peer
Port Description	Displays details about the port

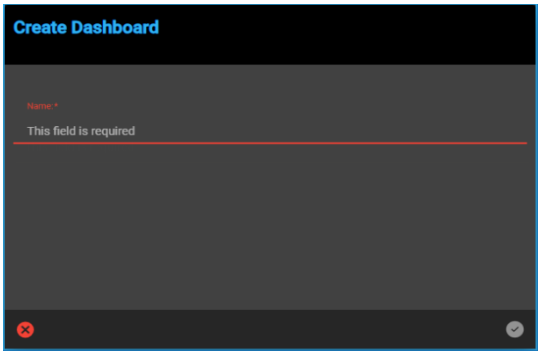
Note: This feature requires the PFS 7000 functionality license. If you apply configuration files that contain the LLDP feature, but do not have a PFS 7000 license installed, the configuration will be applied without error. However, the LLDP feature is not enabled until the PFS 7000 license is installed.

Dashboard

From the Perspective > Dashboard menu, selecting a dashboard from the perspective tree displays the widgets created and saved by the user.

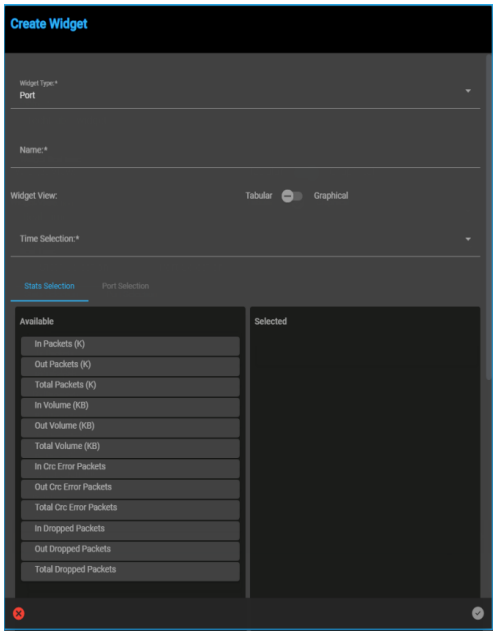


You can create a new dashboard by clicking **Dashboard+** at the bottom of the perspective tree.



Enter the dashboard's name and click **Save**.

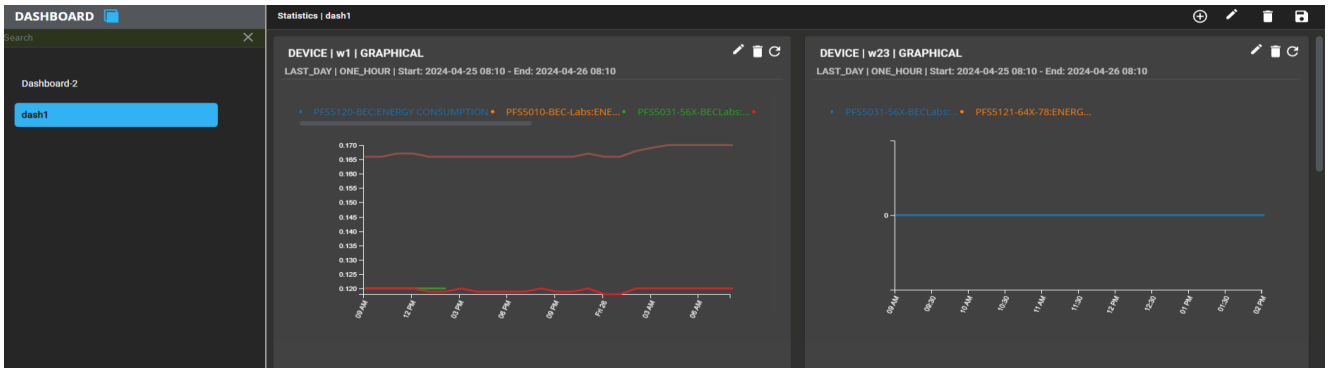
To create a widget, click the + icon in the center of the main screen or the + icon in the header.



Profile Property	Description	
Widget Type	Port or Device	
Name	Enter the widget name	
Widget View	Select Tabular or Graphic	
Time Selection	**Port** Select the monitor time frame: • Real Time • Last Day (Historical Statistics) – Time resolution: 5 min • Last Hour (Historical Statistics) – Time resolution: 1 or 5 min • Custom (Historical Statistics) – Time resolution: 1 or 5 min – Select Start Time/End Time	**Device** Select the monitor time frame: • Last Day (Historical Statistics) – Time resolution: 1 hour
Stats Selection	**Port** • In Packets (K) • Out Packets (K) • Total Packets (K) • In Packet Rate (pps) • Out Packet Rate (pps) • Total Packet Rate (pps) • In Bit Rate (Kbps) • Out Bit Rate (Kbps) • Total Bit Rate (Kbps • In Volume (KB) • Out Volume (KB) • Total Volume (KB) • In Crc Error Packets • Out Crc Error Packets • Total Crc Error Packets • In Dropped Packets • Out Dropped Packets • Total Dropped Packets	**Device** • Energy Consumption(kWh)
Port/Device Selection	Available port(s)	Available device(s)

Note: At the time of publication and software release, the Historical Statistics functionality is being released as Early Field Trial (EFT) to a specific group(s) of NETSCOUT customers until required field testing is successfully completed. Please contact your NETSCOUT representative for more information.

After you configure the widget, click **Save**.

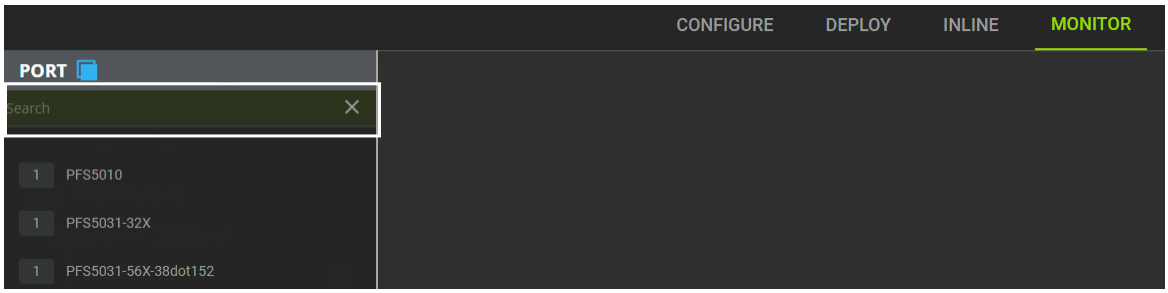


To delete the widget, click the trash can icon in the widget screen.

To delete the dashboard, click the trash can icon in the perspective tree or the trash can icon in the header.

Monitor Search Filter

From Monitor Lifecycle, using the same port search criteria described in Perspective > Trigger on page 3-87, enter a port name (full or partial naming) in the Search text field. Any port containing either the full port designation / name (or a portion of the designation) is listed in the tree view - broken out by switch > blade > port name. Select a displayed port to view its functionally through the monitor palettes.



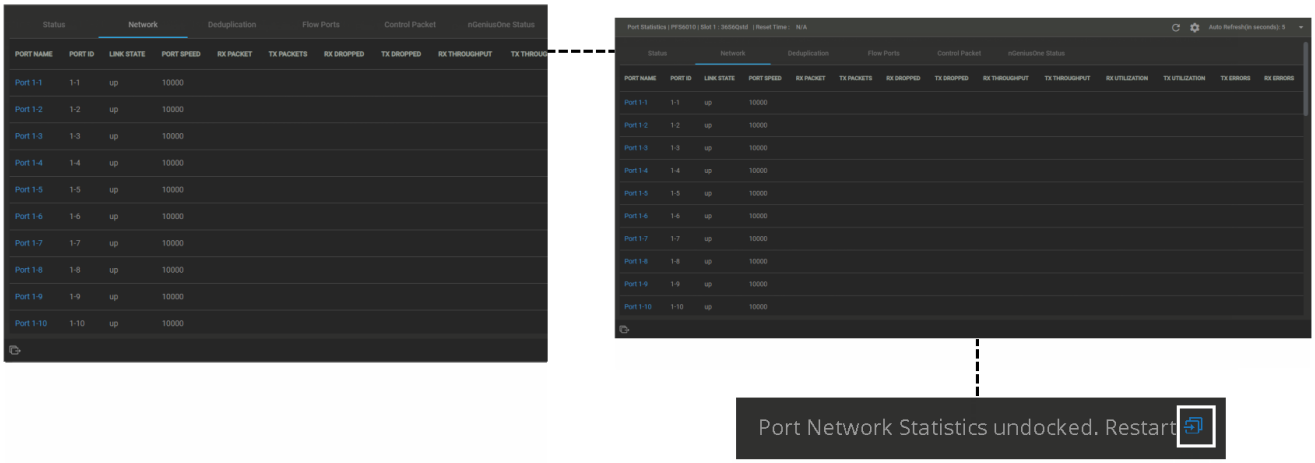
Undocking Monitor Palettes

Many of the monitor windows can be separated (undocked) from the main PFS Fabric Manager application and viewed in separate browser windows. You can minimize, maximize, or close the windows.

Click on the Undock icon of a selected monitor to create a new browser window of the monitor.

Note:
Closing an undocked monitor palette will not automatically reattach it to the main window.

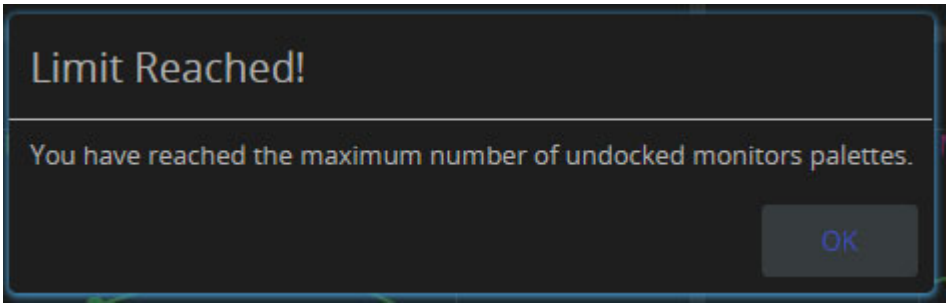
Undocking and reattaching will refresh the monitors palettes and display the statistics from that point in time.



Undocking Limits

You can undock up to 8 monitor palettes belonging to the same or different ports. You can still view an additional monitor palette on the main application window, apart from the 8 undocked palettes.

When attempting to undock a 9th monitor palette, the following error message is displayed:

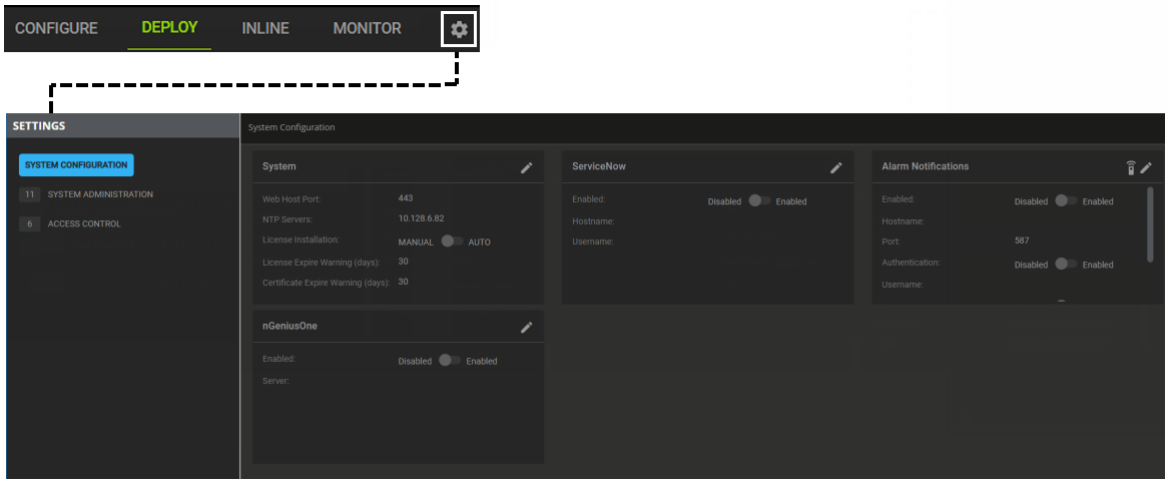


Chapter 7
System Settings

This chapter describes the system settings for the PFS Fabric Manager.

System Configuration

Selecting System Configuration allows viewing and editing the Web Host port and NTP servers of the PFS Fabric Manager Central Server.

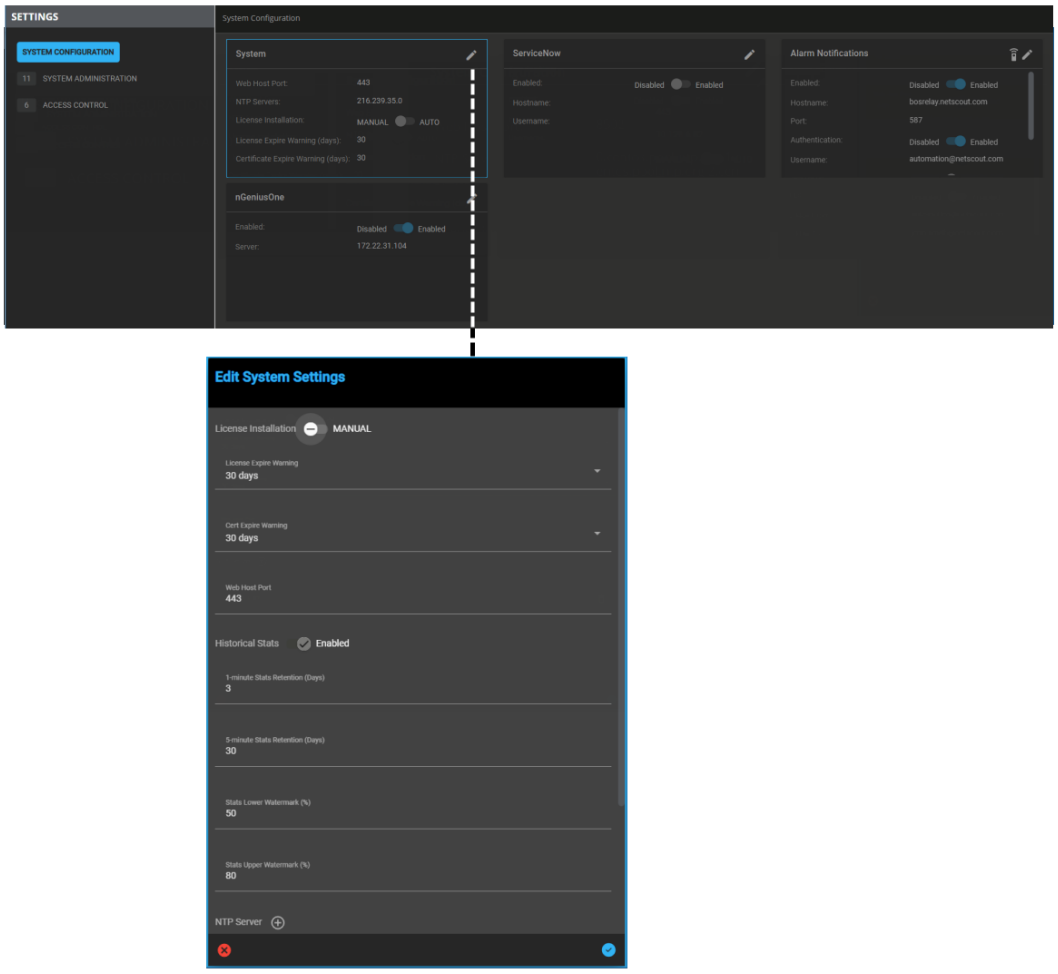


System

Selecting System allows viewing and editing the following parameters for the PFS Fabric Manager Central Server:

- License Installation (Manual/Auto)
  - License Expire Warning
  - Certificate Expire Warning
- Web Host port
- Historical Stats (Enabled/Disabled)
  - 1-minute Stats Retention (Days)
  - 5-minute Stats Retention (Days)
  - Stats Lower Watermark (%)
  - Stats Upper Watermark (%)
- NTP servers

> **Note:** At the time of publication and software release, the Historical Statistics functionality is being released as Early Field Trial (EFT) to a specific group(s) of NETSCOUT customers until required field testing is successfully completed. Please contact your NETSCOUT representative for more information.

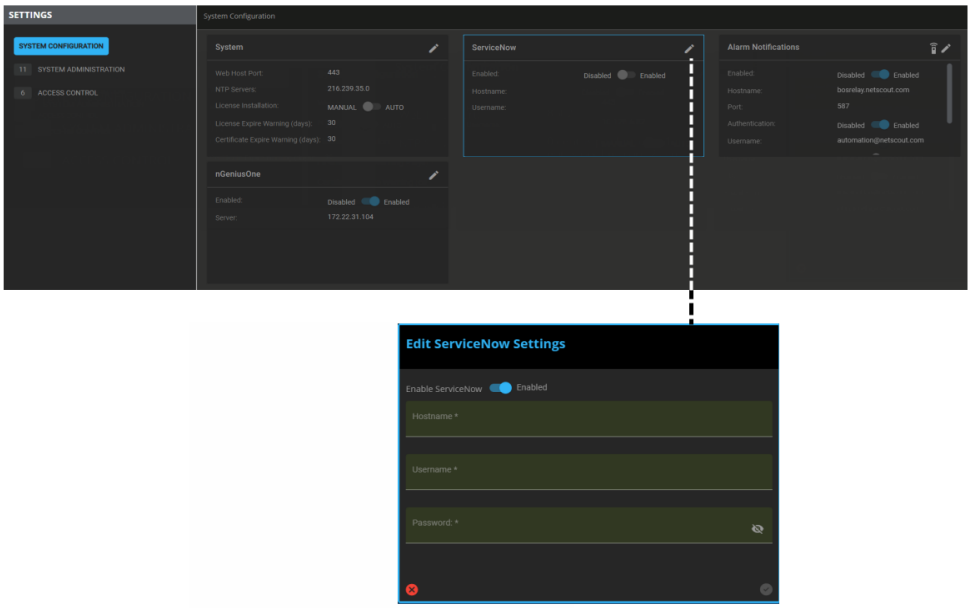


ServiceNow

When a ServiceNow server is configured, PFS-FM pushes alarms (alarm raised, alarm severity changed, alarm cleared) to ServiceNow.

Selecting ServiceNow allows viewing and editing the following parameters of the ServiceNow Server:

- Enable/Disable the ServiceNow server.
- Hostname
- Username

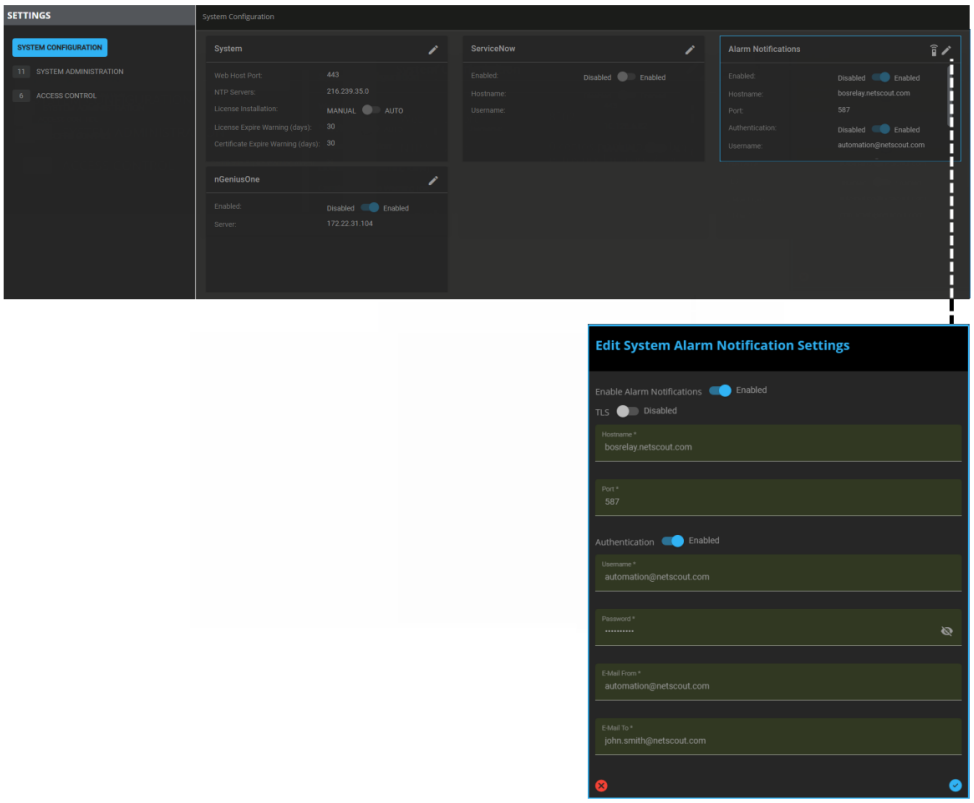


Alarm Notifications

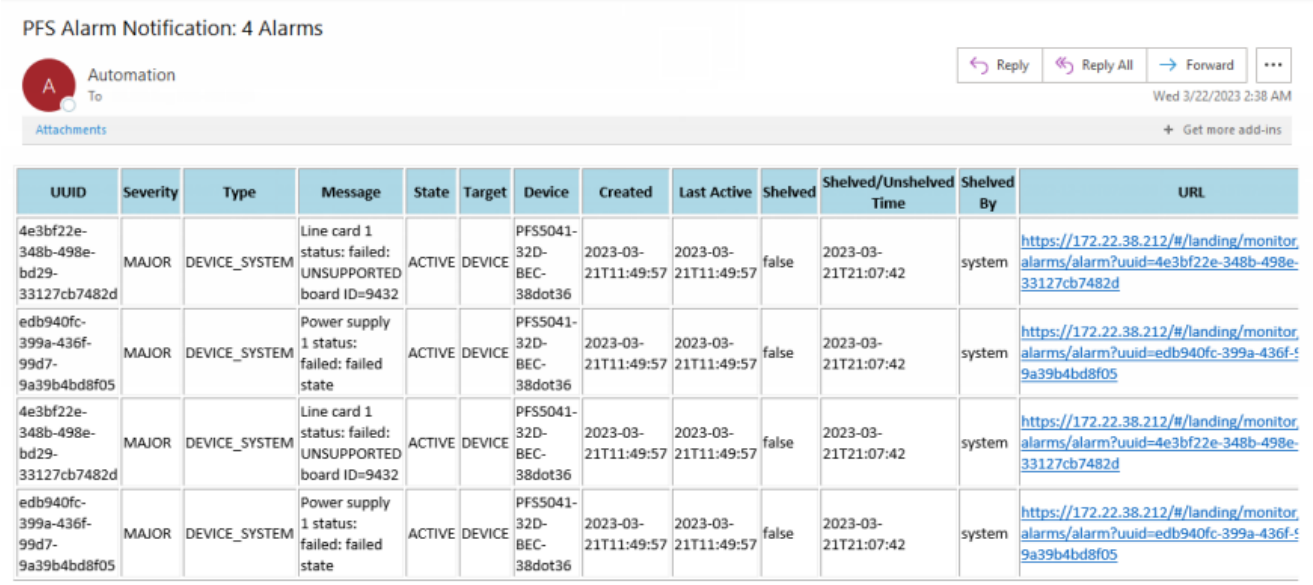
PFS-FM allows users to configure an SMTP mail server to send alarm notifications. The PFS-FM sends email notifications (alarm raised, alarm severity changed, alarm cleared) to a configured email address. Email notifications are batched so multiple alarm notifications may be present in a single email.

Selecting Alarm Notifications allows viewing and editing of the following parameters on the PFS Fabric Manager Central Server:

- Enable/Disable Alarm Notifications
- Hostname of the email server (reachable from the NMS server)
- Port
- Authentication (Enable/Disable)
- Username & Password (when Authentication is Enabled and user’s email ID is configured)
- TLS (Enable/Disable TLS as required by the email server)
- E-Mail From
- E-Mail To (multiple addresses are not supported, email distribution lists are acceptable)


SETTINGS
System Configuration
SYSTEM CONFIGURATION
11 SYSTEM ADMINISTRATION
6 ACCESS CONTROL
System
Web Host Port: 443
NTP Servers: 216.239.35.0
License Installation: MANUAL AUTO
License Expire Warning (days): 30
Certificate Expire Warning (days): 30
ServiceNow
Enabled: Disabled Enabled
Hostname:
Username:
Alarm Notifications
Enabled: Disabled Enabled
Hostname: bosrelay.netscout.com
Port: 587
Authentication: Disabled Enabled
Username: automation@netscout.com
nGeniusOne
Enabled: Disabled Enabled
Server: 172.22.31.104
Edit System Alarm Notification Settings
Enable Alarm Notifications Enabled
TLS Disabled
Hostname * bosrelay.netscout.com
Port * 587
Authentication Enabled
Username * automation@netscout.com
Password *
E-Mail From * automation@netscout.com
E-Mail To * john.smith@netscout.com

Sample Email:



PFS Alarm Notification: 4 Alarms

Automation
To

Reply | Reply All | Forward | ...

Wed 3/22/2023 2:38 AM

Attachments

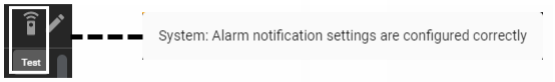
+ Get more add-ins

UUID	Severity	Type	Message	State	Target	Device	Created	Last Active	Shelved	Shelved/Unshelved Time	Shelved By	URL
4e3bf22e-348b-498e-bd29-33127cb7482d	MAJOR	DEVICE_SYSTEM	Line card 1 status: failed: UNSUPPORTED board ID=9432	ACTIVE	DEVICE	PFS5041-32D-BEC-38dot36	2023-03-21T11:49:57	2023-03-21T11:49:57	false	2023-03-21T21:07:42	system	https://172.22.38.212/#/landing/monitor/alarms/alarm?uuid=4e3bf22e-348b-498e-33127cb7482d
edb940fc-399a-436f-99d7-9a39b4bd8f05	MAJOR	DEVICE_SYSTEM	Power supply 1 status: failed: failed state	ACTIVE	DEVICE	PFS5041-32D-BEC-38dot36	2023-03-21T11:49:57	2023-03-21T11:49:57	false	2023-03-21T21:07:42	system	https://172.22.38.212/#/landing/monitor/alarms/alarm?uuid=edb940fc-399a-436f-99d7-9a39b4bd8f05
4e3bf22e-348b-498e-bd29-33127cb7482d	MAJOR	DEVICE_SYSTEM	Line card 1 status: failed: UNSUPPORTED board ID=9432	ACTIVE	DEVICE	PFS5041-32D-BEC-38dot36	2023-03-21T11:49:57	2023-03-21T11:49:57	false	2023-03-21T21:07:42	system	https://172.22.38.212/#/landing/monitor/alarms/alarm?uuid=4e3bf22e-348b-498e-33127cb7482d
edb940fc-399a-436f-99d7-9a39b4bd8f05	MAJOR	DEVICE_SYSTEM	Power supply 1 status: failed: failed state	ACTIVE	DEVICE	PFS5041-32D-BEC-38dot36	2023-03-21T11:49:57	2023-03-21T11:49:57	false	2023-03-21T21:07:42	system	https://172.22.38.212/#/landing/monitor/alarms/alarm?uuid=edb940fc-399a-436f-99d7-9a39b4bd8f05

Clicking on any alarm from the email or ServiceNow will open the Alarm Dashboard, displaying only the specific alarm context. Reset the filter or navigate away from the alarm page, to any other tab or lifecycle, to reset the specific alarm context filter.

Profile Property	Description
UUID	A unique identifier for an alarm (any updates to the alarm will use the same UUID)
Severity	Alarm severity (see Alarms and Severities)
Type	Type of alarm (e.g., DEVICE_SYSTEM, DEVICE_DOWN, PORT_DOWN)
Message	The text of the alarm
State	ACTIVE or CLEARED
Target	The device (PFS or NMS) which triggered the alarm
Device	Server on which alarm appears
Created	Timestamp when the alarm was created
Last Active	Timestamp when the alarm was last active
Shelved	True if the alarm has been Shelved in PFS-FM, otherwise false
Shelved/Unshelved Times	Timestamp when the alarm was last shelved or unshelved
Shelved By	Name if the user that shelved the alarm. If system is displayed, the alarm was auto-shelved by the system.
URL	Current NMS IP with alarm specific context (only the specified alarm is displayed). Reset the alarm context using X reset on filters or navigate to another tab and back. Clicking on the URL opens a new window to the PFS-FM. Provide your username/ password, for the PFS-FM, to display the alarm specific details.

The user can test the Alarm Notification configuration by clicking on the Test icon. Pressing the Test icon will send a test email using the Alarm Notification settings.



nGeniusOne

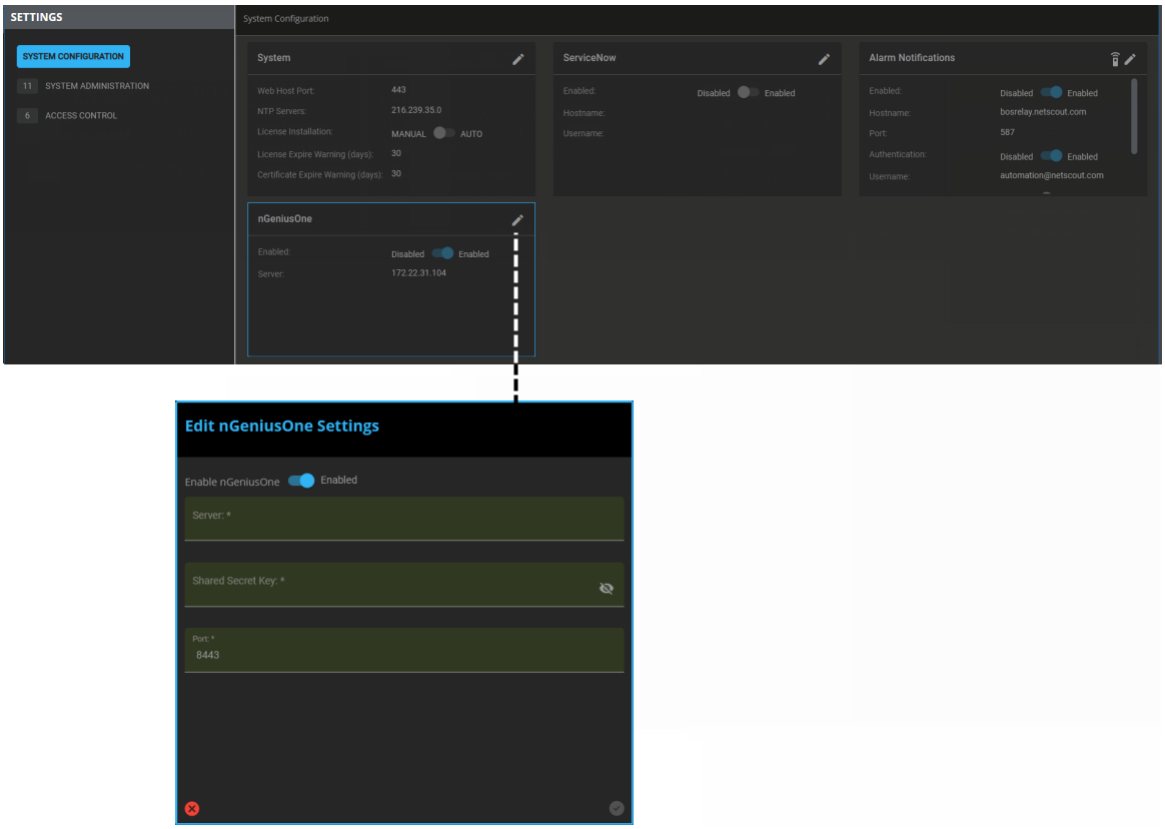
PFS-FM allows users to connect to the nGeniusOne PFS Monitor, to view the ASI metrics from the switch and also to retrieve the nGeniusOne switch alarms (as per the nGeniusOne Notification Center) in Fabric Manager, providing seamless access to the metrics from either nGeniusOne or PFS-FM.

To connect to nGeniusOne, perform the following:

1. Add the PFS Fabric Manager as a Trusted Server in Server Management on the nGeniusOne server.
2. Ensure nGeniusOne has PFS License option appropriately enabled in order to view the PFS Monitor statistics in Fabric Manager and related switch alarms from nGenusOne. Also, ensure that Fabric Manager is added as a Trusted Server in nGeniusOne (Global or Standalone).
3. Copy the trusted key from the nGeniusOne server management for this PFS-FM clicking **Copy**.
4. Enable the System Configuration in PFM > Toggle Enable > set the nGeniusOne server IP Address and the copied trusted key.

Selecting nGeniusOne allows viewing and editing of the following parameters on the PFS Fabric Manager Central Server:

- Enable/Disable nGeniusOne
- Server



System Administration

Selecting System Administration allows viewing and editing the Backup/Restore, Certificates, Licenses, Storage, Switch Configs, Software and Firmware, and Managed Devices of the PFS Fabric Manager.

Backup/Restore

The Backup/Restore feature allows the user to perform backups and restores of the PFS Fabric Manager's configuration and environment. This includes the database and configuration files.

Backup data holds data for the NMS (central server) and all managed PFS that are connected at the time of the backup. During the restore operation, any switches that are connected to the NMS before the restore operation is started will have their configuration replaced with that from the backup data and any switches that are not connected when the restore operation will not have their configuration replaced.

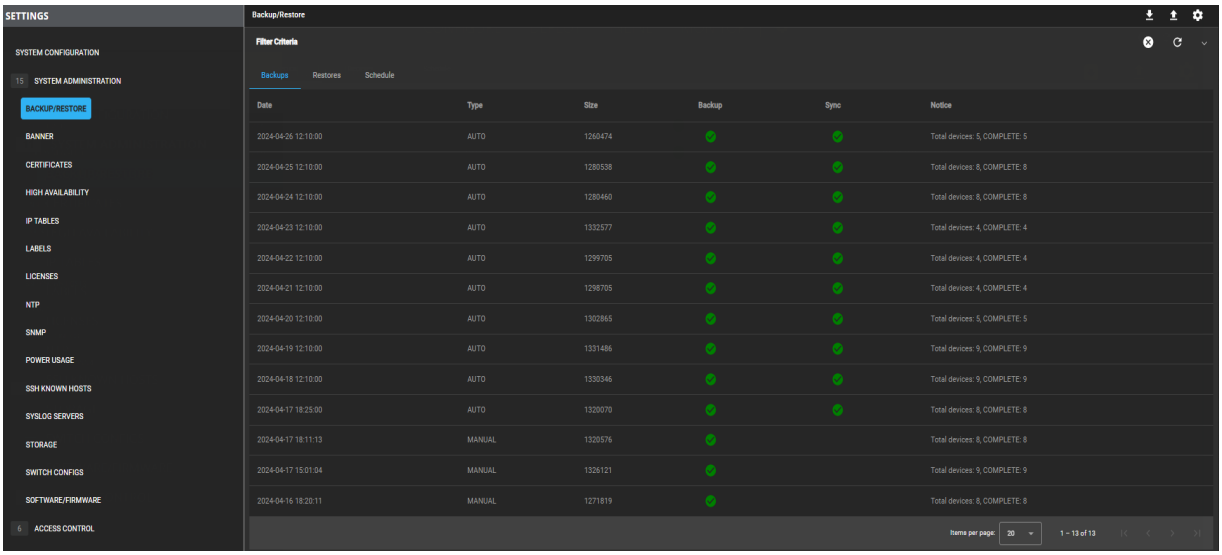
Specifically, if the NMS does not have its configuration (e.g., because it is a cold standby or it was reinstalled from scratch) the PFS will not be connected to it at the time of the restore operation. During the restore operation the switches' configuration will not be replaced but the NMS will be configured to connect to the switches; the NMS will reconnect to the switches after the restore operation is complete.

Backup/Restore Dashboard

The dashboard tabs show the current status and history of backups and restores, as well as the current automated backup settings. In each tab, the user can access the manual backup/restore and configuration panels.

Backups Tab

The backups tab shows all currently accessible (stored on NMS) backups. It shows basic information about the backup, its synchronization status, and any important messages.

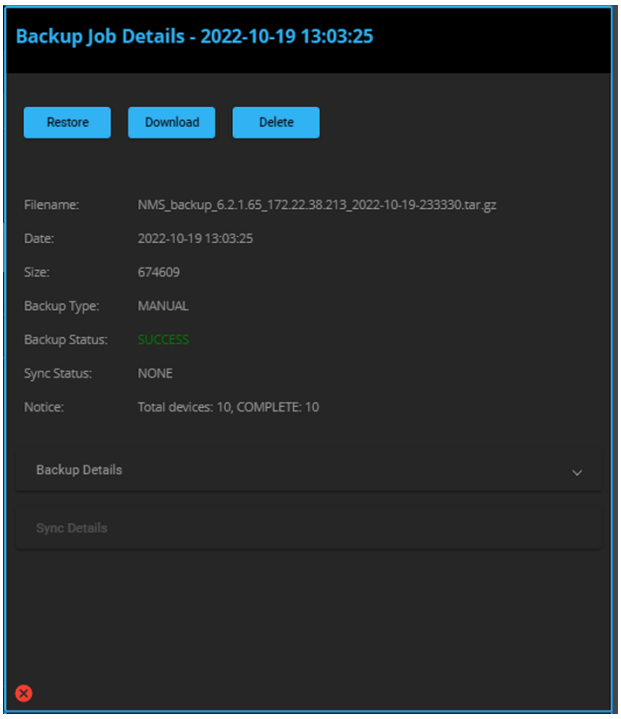


Backup Detail

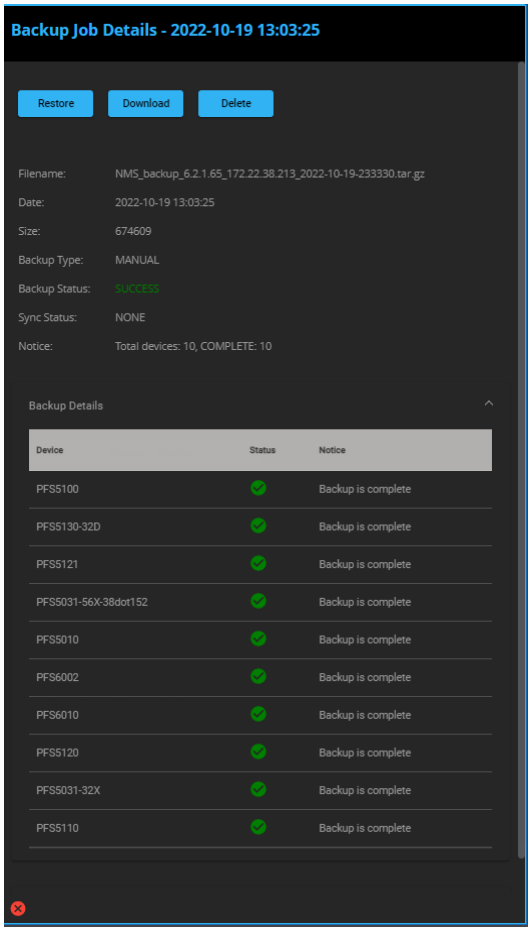
To restore an automatic or manual backup that is stored on the NMS, click on a backup from the dashboard. This brings up the Backup Detail slideout which has more information about the backup, and if the backup file is available on the NMS, a set of buttons to restore, download, or delete the backup.

Click on a button to perform the desired operation.

Note: If the backup fails, there will be no file and the buttons will be inactive.

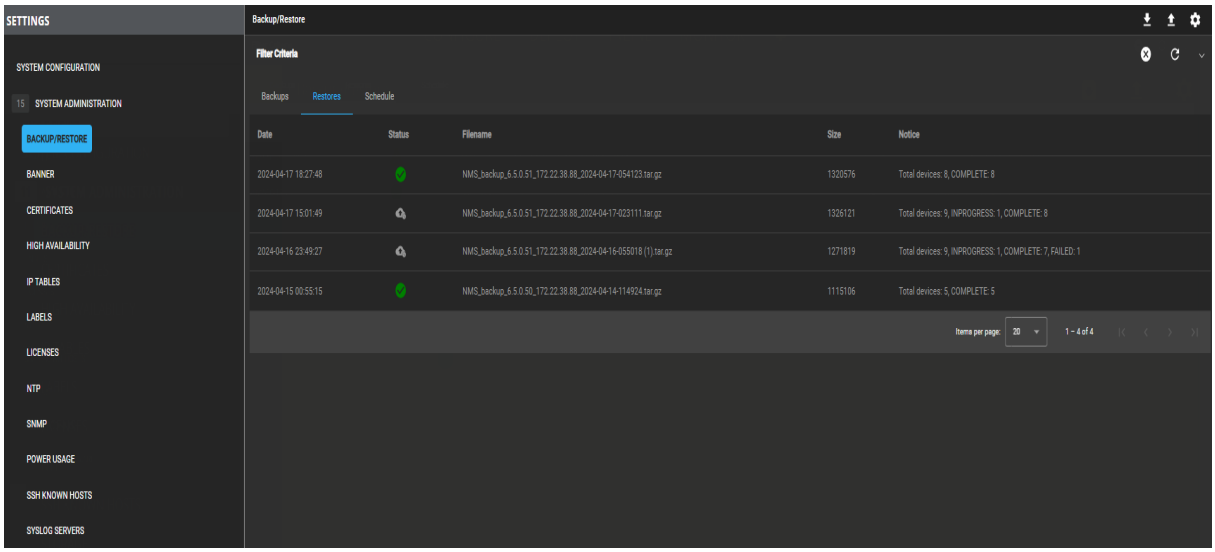


The backup detail allows the user to view details of the backup itself. Click on the chevron next to Backup Details.



Restores Tab

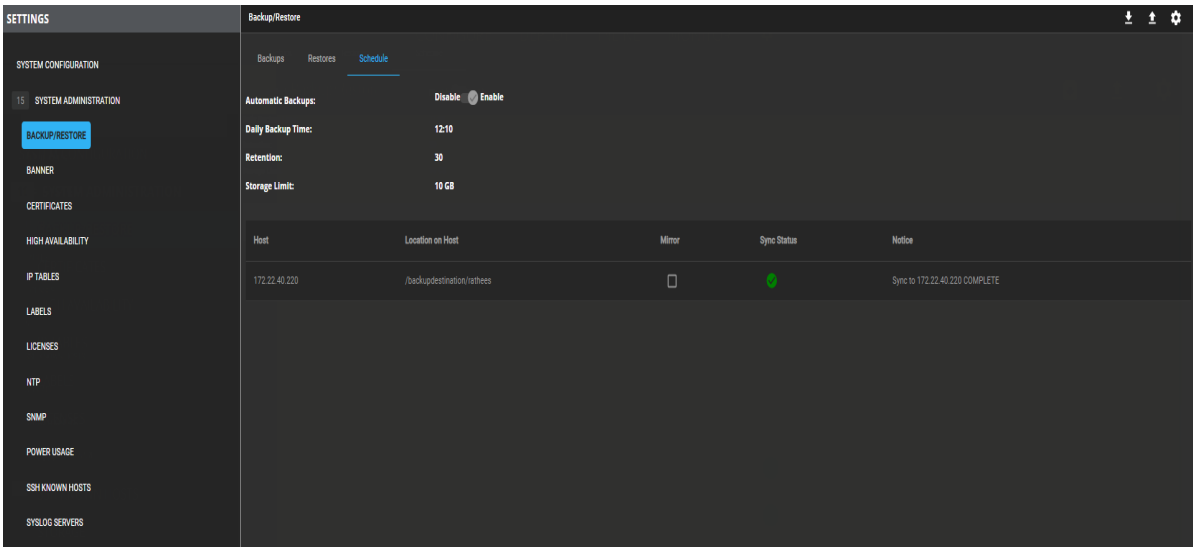
The Restores tab displays a filtered list of the user's invoked restores and their status.



The restore detail is informational only and shows the last known state of the restore. Click on the chevron next to Restore Details.

Schedule Tab

The Schedule tab displays the current Automated Backup configuration. It also shows the status of the last sync to the backup destinations.

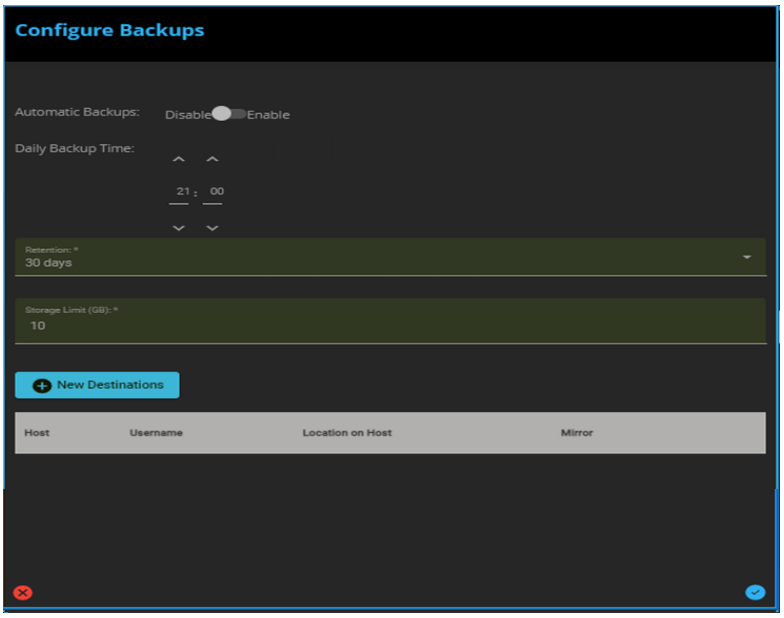


Configure Backups

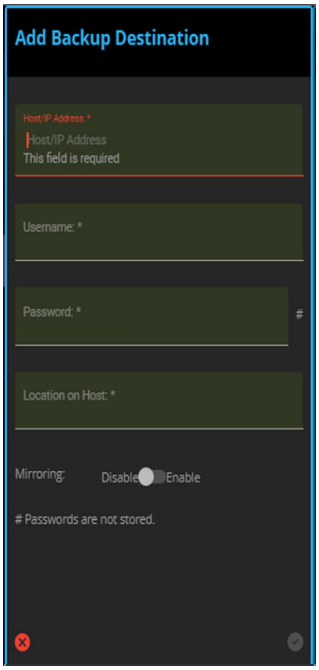
Click the Configure icon (Gear) at the top of any dashboard tab to access the Configure Backups panel. The panel contains the following editing options:

- Automatic backups enable/disable: Enables/disables the daily backup job (automatic as per the Daily backup time)
- Daily backup time: Time set by the user to start the automated backup
- Retention pulldown. Retention values (in days):
  - 7, 14, 30 (default), 60, 90

- Storage limit: 1-10GB
- Backup destinations. There are control icons.
  - Blue "+" icon. Adds a destination if the limit has not been reached (limit is 3 backup destinations).
  - Trash can icon. Removes the destination
  - Pencil icon. Edit the destination.



To add a destination click the "+" icon. This displays a slideout to the left of the Configure Backups, which is now disabled.



Profile Property	Description
Host/IP Address	Hostname or IPv4 address of the target backup server running a Linux based OS. (IPv6 is not supported at this time.)
Username	Linux OS user on the remote server (except root). The remote user must have read/write privileges in the backup location.
Password	Password for the remote user on the remote server. Passwords are not stored, they are used only once to install the NMS SSH public key on the backup server.
Location on Host	Directory where the backup files are stored on the remote server. If the home directory is used, ensure that the location is a subdirectory. **Note:** The directory must have read/write access for the associated username.
Mirroring	Allows the user to define a destination as a mirror of the NMS local backup repository, which also performs rotation and size management. If the destination is not mirrored, the backups are transferred to the destination, which must manage its own file rotation. **Note:** The destination will hold a full copy of the backup repository. In this way, the remote destination will reflect the retention policy defined for the NMS. Assuming there is sufficient space on the destination, this is an easy way to ensure that the destination has up to date files and the backups will not consume all the disk space. If mirroring is disabled, PFS-FM copies the latest backup to the destination and the remote server administrator is responsible for defining and implementing the retention policy on the remote server.

Manual Backup/Restore

Backup Now and Restore from Workstation icons appear in the top right of the dashboard screen. These options are displayed by rollover text when the mouse hovers over the icons. The desired actions present confirmation dialogs before executing the action.

Backup Now

- Click the icon
- Confirmation dialog asks if they wish to make a backup now.

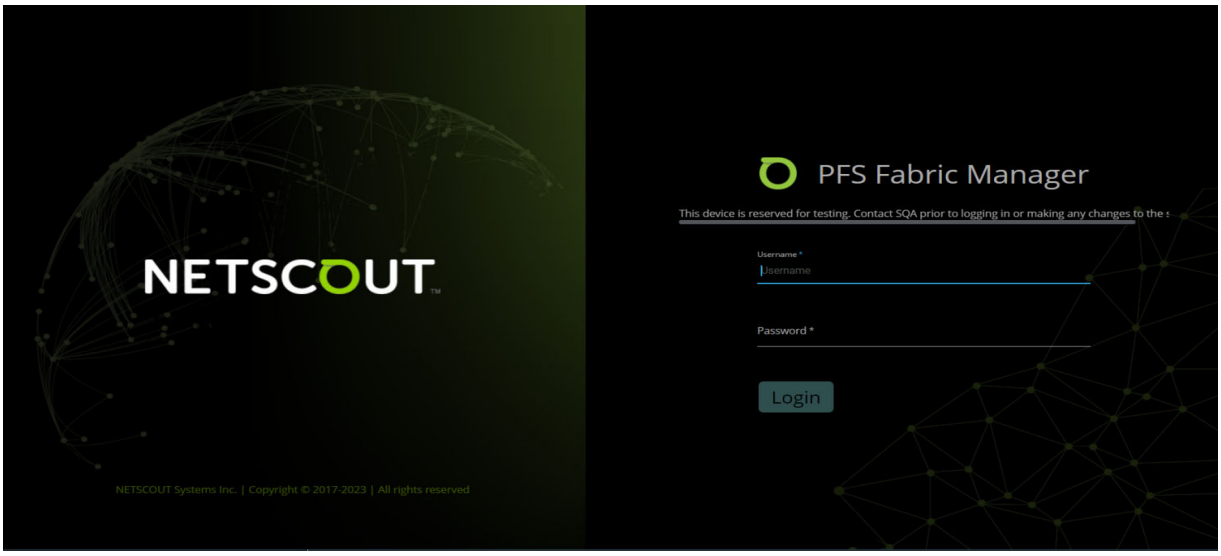
> **Note:** If Sync destination is configured, both automated jobs and manual jobs are synced to the remote destination.

Restore from Workstation

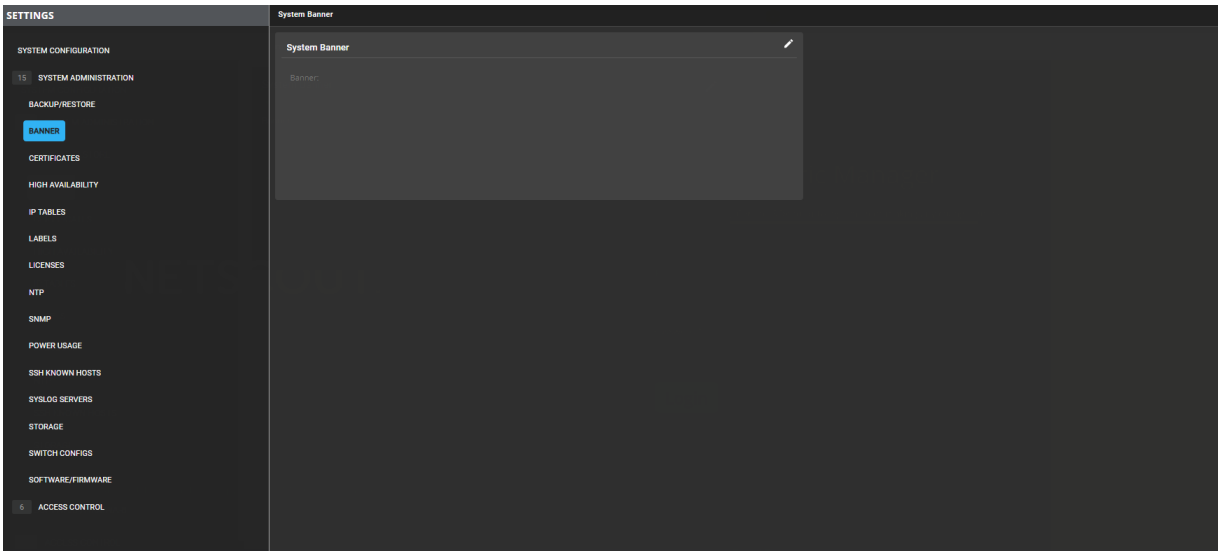
- Click the icon
- Confirmation dialog asks if they wish to restore a backup now.

Banner

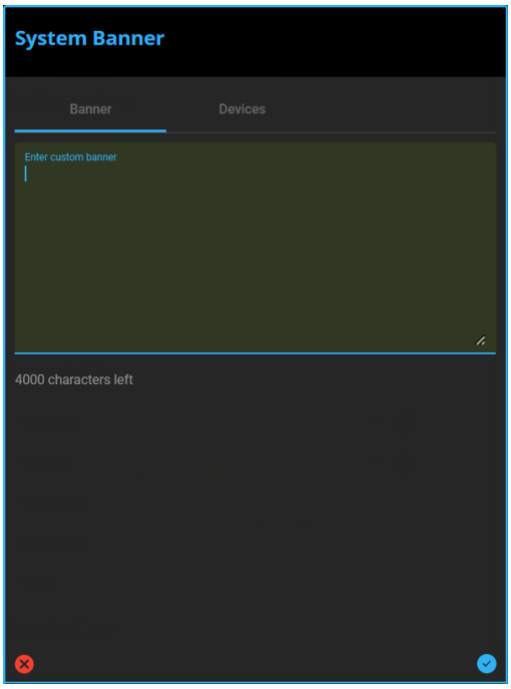
The Banner feature allows the user to create a banner message which is displayed on the login page.



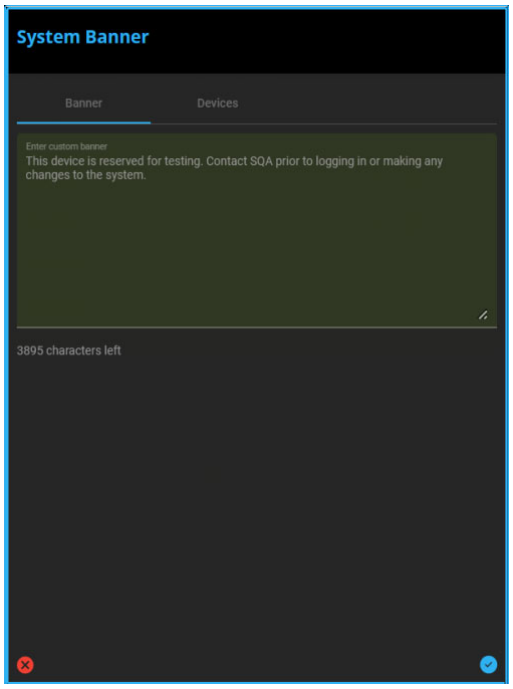
The banner is configured in System Administration under System Settings.



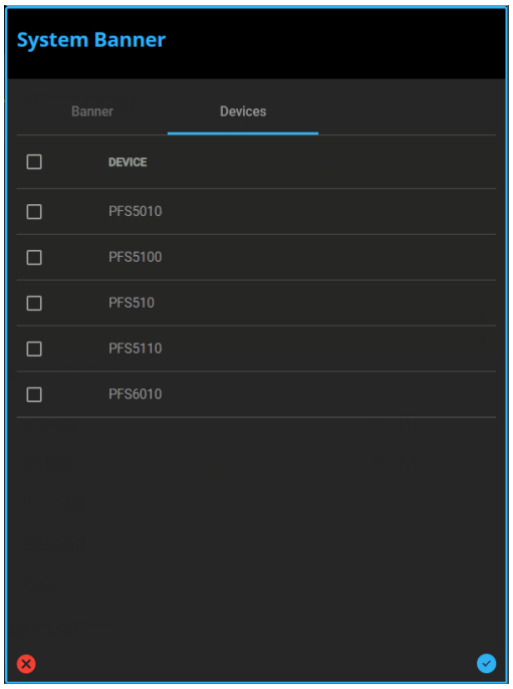
To create/update a banner, the user clicks the Edit icon to open the System Banner slideout.


System Banner
Banner
Devices
Enter custom banner
4000 characters left

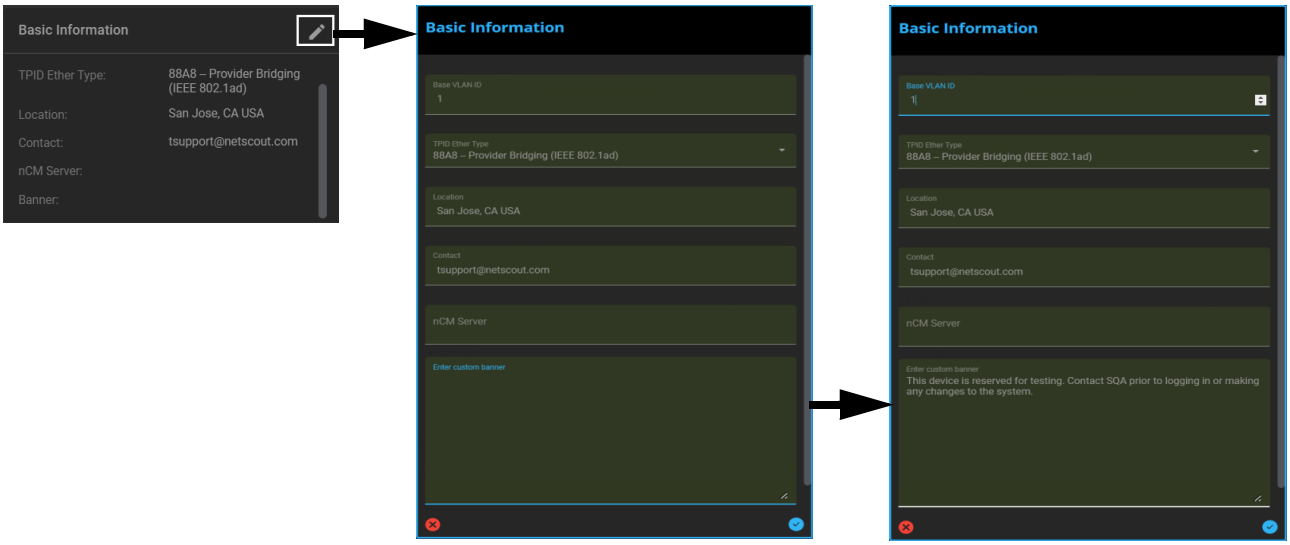
From the Banner tab, the user can enter the desired message to be displayed on the login page.



From the Devices tab the user can select a managed device or all managed devices to which the banner will be applied.



The banner can also be configured as part of the basic profile in Basic Information from Configuration lifecycle. The banner content allows for numbers, letters, and symbols (_- , . ( ) space @). A maximum of 4000 characters that can be entered.



Certificates

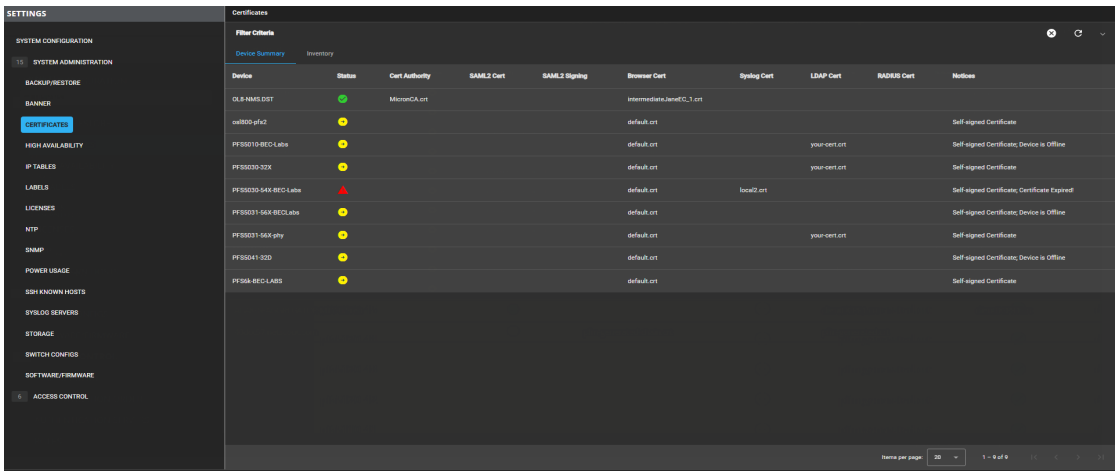
The Certificates feature allows the user to manage the certificate inventory and a device summary.

Note: PFS Fabric Manager cannot manage configuration changes of browser and syslog TLS certificates on PFS running PFOS version 6.0.3 and earlier.

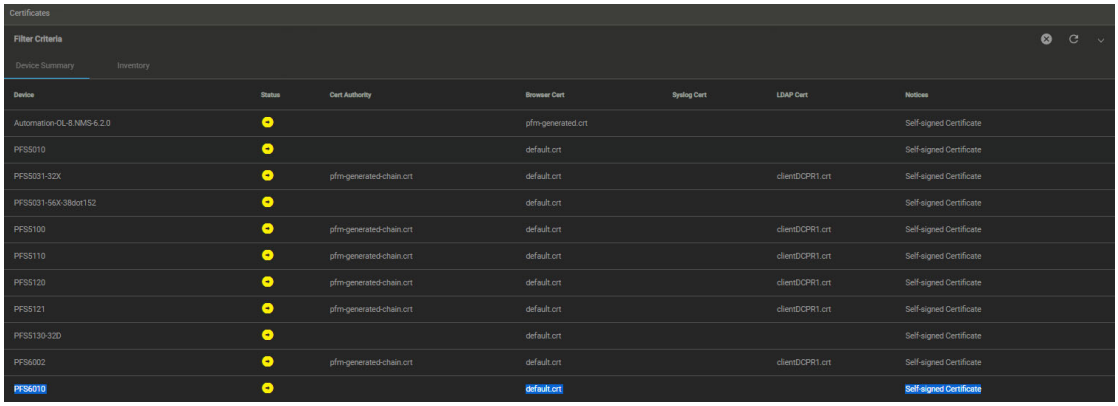
Note: All certificates must be PEM (base 64 ASCII) encoded in a file whose name ends with ".crt". DER-encoded certificates or certificates stored in PKCS#7 (.p7b) or PKCS#12 (.p12 or .pfx) containers must be converted to PEM format for use with PFS Fabric Manager. Most certificate providers can supply PEM-encoded certificates; if not free tools such as OpenSSL are available to convert or extract the certificates.

Device Summary Tab

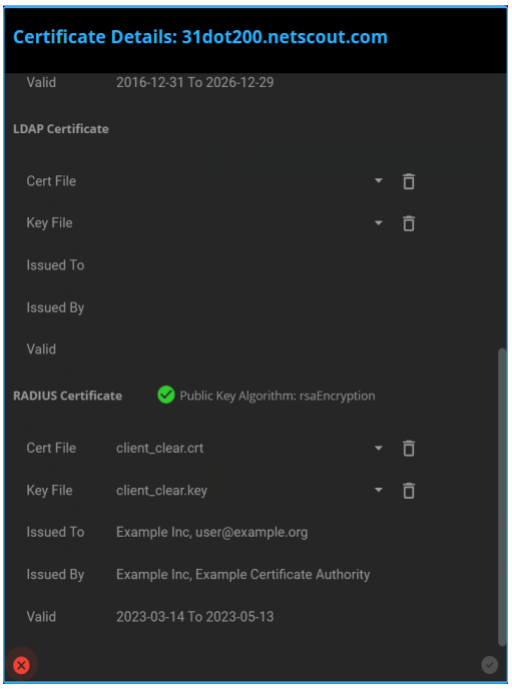
The device summary table is a searchable, pageable list that includes all managed devices and the NMS. The certificates on each device will be displayed, as well as warnings for expired or soon to be expired certificates. Self-signed certificates will also show a warning.



If different certificates are installed on both management cards of a PFS-6010 device, then comma separated details from both the cards are displayed in respective columns.



Selecting/clicking on a row in the Device Summary table displays the Certificate Details for the device. If the selected device is a PFS-6010, the Certificate Details includes an additional option: **Target CPU**, which allows the user to select which management card to update with the selected certificates.



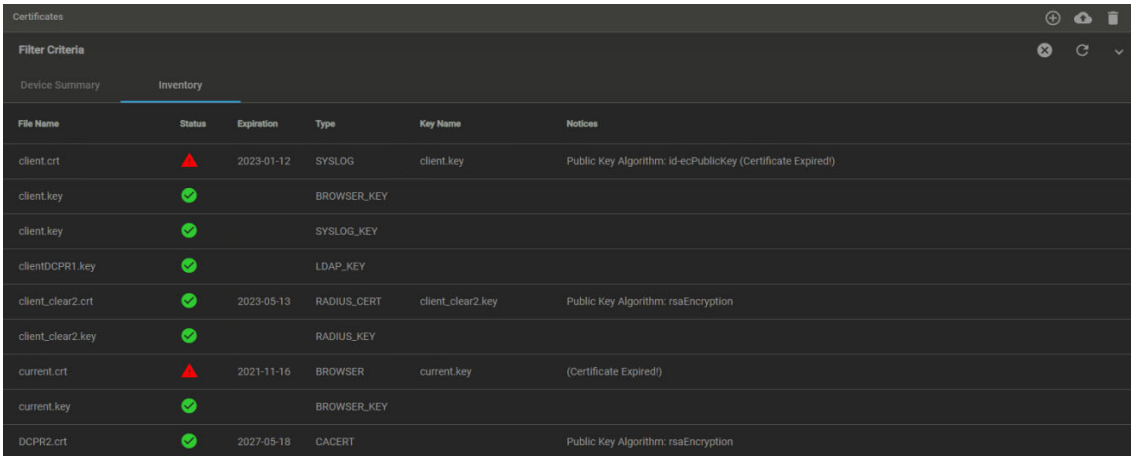
If a card is empty or invalid, that option is disabled.

Selecting a management card from the Target CPU list, updates only the certificate for that card of the PFS-6010 device.

Inventory Tab

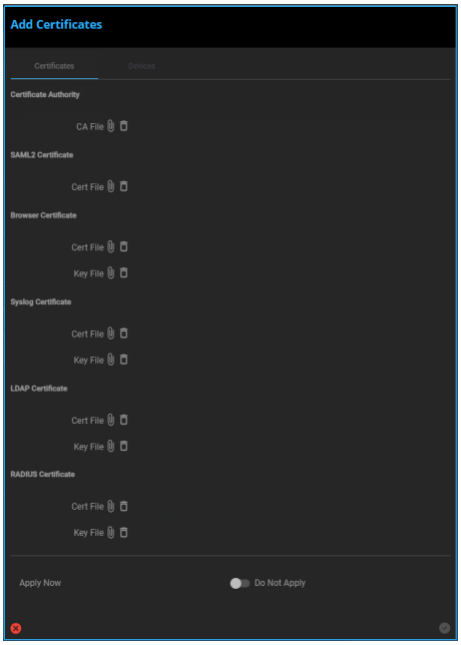
The certificate inventory table operates on certificates. Non-root certificates will have key files associated and the key files will have optional pass phrases. The inventory table is a searchable, pageable list since there could be as many certificate sets as there are devices and the user can search for a certificate or key file which is a part of a certificate set.

> **Note:** New certificates for CA, Browser, and syslog are supported in 6.0.5. Additionally, EC certificates are supported for upload to the switch and managed via NMS (for 6.0.5 switches).



By clicking the add icon, the selected certificates can be added to the selected devices.

The Certificates tab will display the devices with All and None button along with skip-apply slider to select the specific devices.



The Devices tab displays the devices, All and None buttons allowing the user to select the devices, and a Skip-Apply slider to select the specific devices.

High Availability

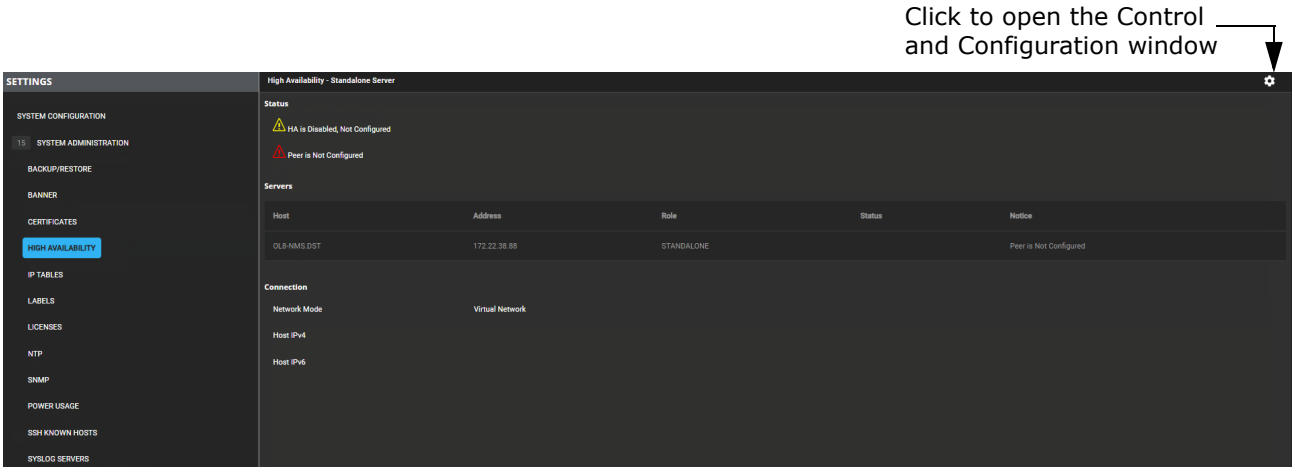
The High Avilability (HA) feature allows the user to manage the HA system and configure the HA mode and Network.

Note: The HA feature requires that the active and standby servers are time synchronized. The use of NTP on both servers is highly recommended. See NTP for information on how to configure NTP servers.

Note: The HA feature requires that both servers are running the same version of PFS Fabric Manager and the same OS (security) patch level before initially configuring/activating the HA feature.

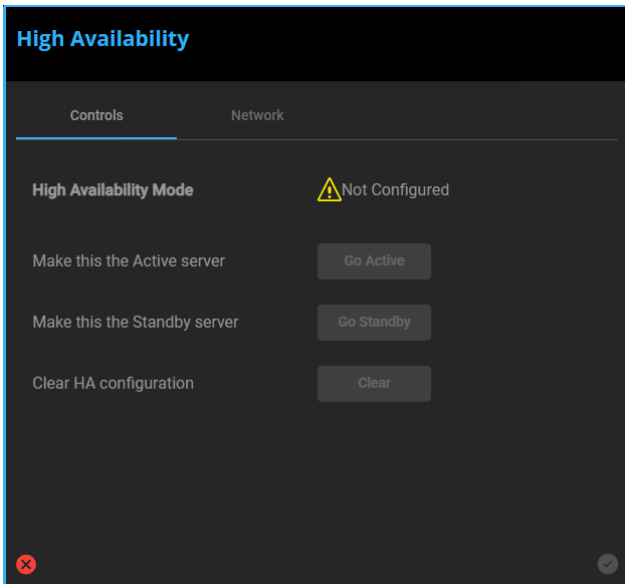
- The HA dashboard shows the status of the HA system and the synchronization state. The active and standby servers are displayed, with status and notices, in case of errors or problems. Also displayed is the currently selected network configuration and IP addresses.

  A settings icon is provided to bring up the Controls and Configuration window.



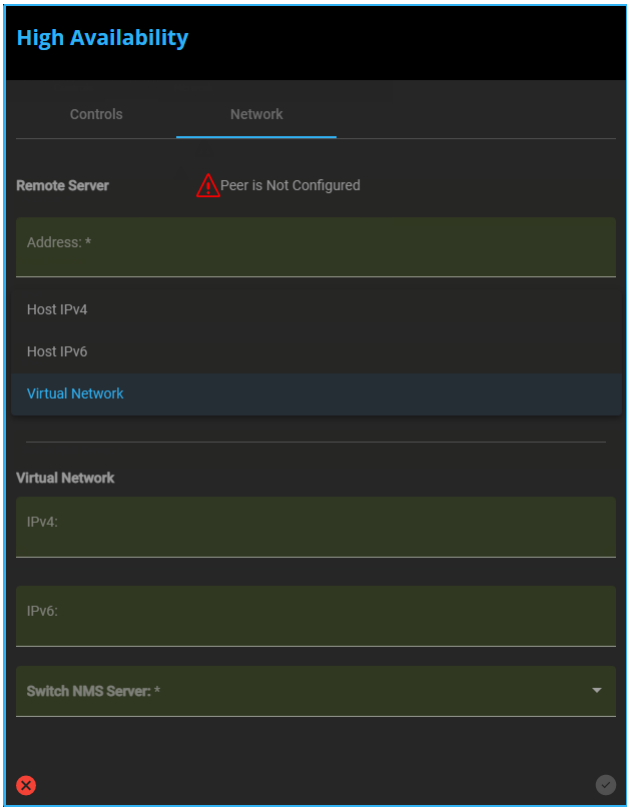
- The Controls and Configuration window provides tabs for control and configuration of the HA system.

  The Controls tab shows status and allows the user to make the current ACTIVE server the standby, or to make it go standalone.

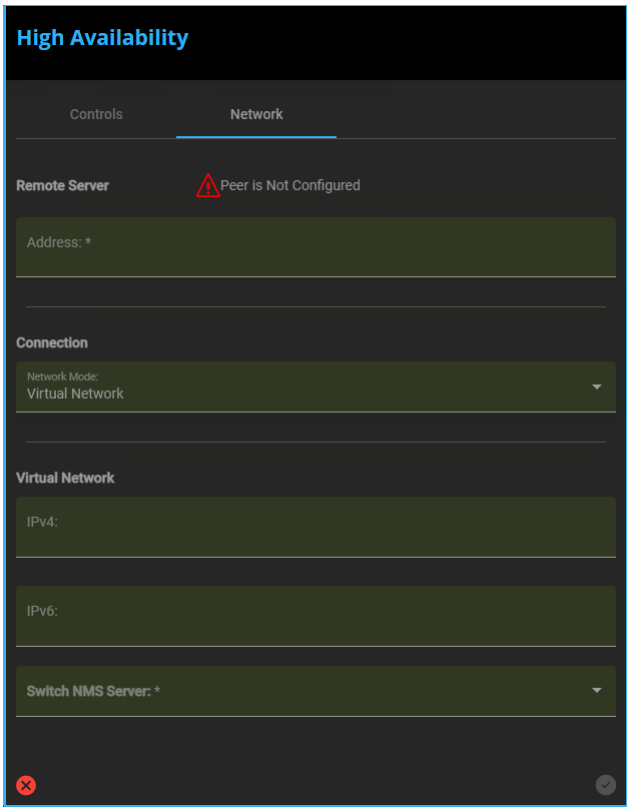


  The Network tab defines the HA peer address and any Virtual Network or Host IP Configuration (IPv4 or IPv6) that will be used for the NMS and allows for switching virtual networks or host IP configurations.

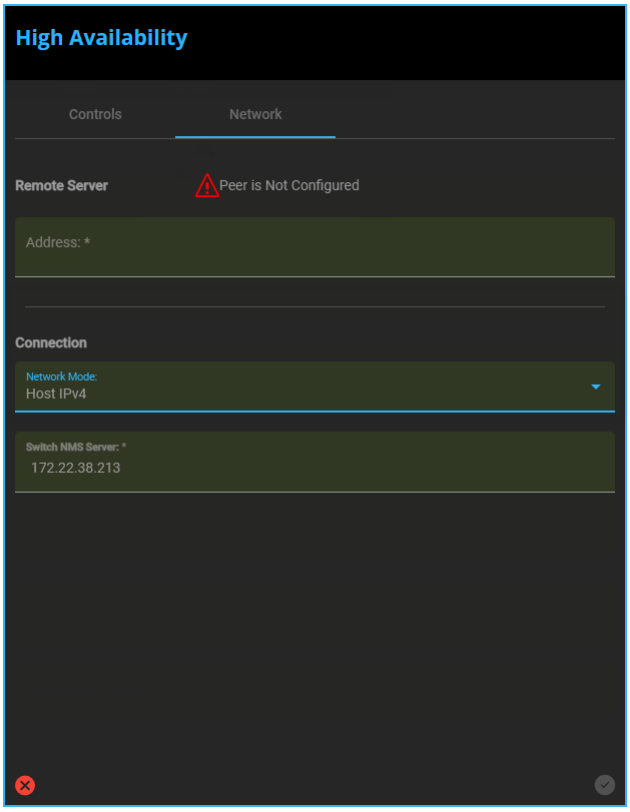
Note: Host IPv6 is only available if the NMS is configured with an IPv6 address.



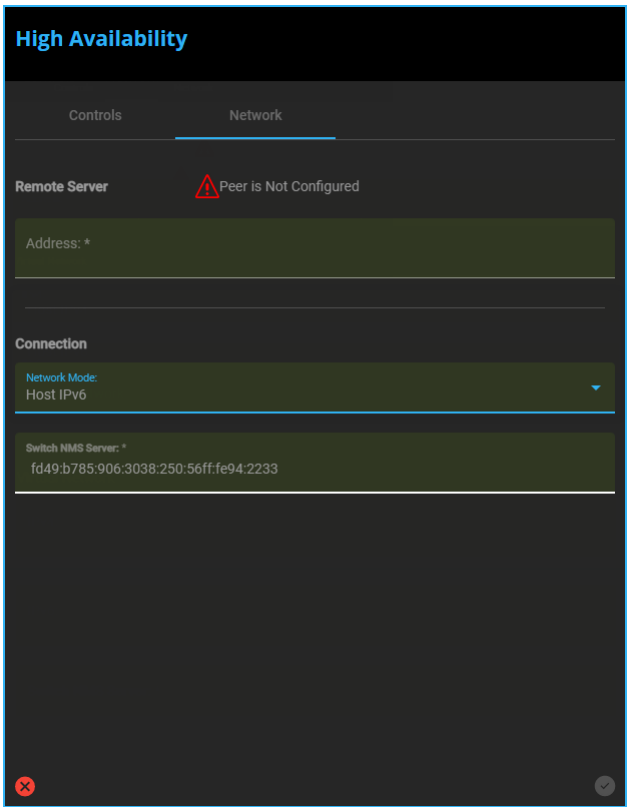
Virtual Network



Host IPv4



Host IPv6



Active/Standby Role Management

There are two roles in HA, active and standby. Active performs normal operations and mirrors its data to the standby. Standby collects data and does no active interaction/management of any switch or any other NMS regular lifecycle managements.

A third role, Standalone, is the default role for fresh installs. This is essentially *active without a standby*. There are no HA features enabled during standalone operation.

Virtual IP

A Virtual IP (VIP) should be configured for HA. This is the management IP to which users and the switches connects; users and switches accessing the VIP are always accessing the Active NMS. The VIP is on the same network as the Active/Standby. The VIP, which can be IPv4 or IPv6, can be changed from the Active NMS.

Host IP

A Host IP (IPv4 or IPv6) should be configured for HA when the active and standby servers are geographically separated. When Host IP is used, users must connect to the management IP of the Active NMS (users connecting to the Standby NMS are notified that they have connected to the Standby). Switches will also connect to the management IP of the Active NMS; when the Standby NMS becomes Active, it will notify all managed PFS to change the IP address to which they connect.

HA Role

The HA role is a persisted state that holds the current state of the HA system. It is used to determine actions in the system at startup and operation.

active - The peer is the active peer

standby - The peer is the standby peer

standalone - The peer is an active peer, but with no HA configured

Synchronization States (As seen on NMS HA Status page)

The following are the Synchronization statuses:

- Synchronized - A PFM HA system is considered synchronized when its peers are in full communication and the standby database has parity with the active.
- Synchronizing - Peers are communicating but the standby database does not have parity
- Unsynchronized - Peers are not communicating. This state will generate an alarm.

Switchover Rules

The following are the switchover rules:

- Switchover is entirely manual.
- Users can force switchover even if the system warns them against it.
- If the HA peers are in sync, users can force switchover from either peer and the peers will switch roles.
- If the peers are not in sync, users will need to follow an "out of sync switchover" procedure to avoid having two active peers.
- HA peers will remain in their roles until switchover.

Switchover from Active

Switchover from the active peer is invoked by the user from **Settings > High Availability > Controls and Configuration**.

1 To start the switchover, click on **Go Standby**.

A dialog appears showing any warnings, if any:

Examples:

- *Standby peer is not connected*
- *Database is not synchronized*

2 If the user chooses to continue, the switchover sequence begins.

Note that this switchover sequence also occurs if the active receives a *go standby* command from the standby peer.

3 Halt / wait for current transactions to finish.

4 Create a backup as a restore point in case of failure. This backup will probably be an NMS-only backup.

5 If status is synchronizing:

Wait for synchronized state (or timeout).

6 Tear down VIP.

7 Mark HA role as **standby**.

8 If peer is connected:

Send *go active* control message to peer. (Server will automatically restart)

Switchover from Standby

Switchover from the standby peer is invoked by the user from **Standby Landing Page > Controls and Configuration**.

1 To start the switchover, click on **Go Active**.

A dialog appears showing any warnings, if any:

Examples:

- *Standby peer is not connected*
- *Database is not synchronized*

2 If the user chooses to continue, the switchover sequence begins.

Note that this switchover sequence also occurs if the standby receives a *go active* command from the active peer.

3 If status is synchronizing:

Wait for synchronized state (with timeout).

4 Create an NMS backup as a restore point in case of failure.

5 If active is connected:

Send *go standby* to active.

Wait for *go active* from active (or timeout).

6 Mark HA role as **active**.

Going Standalone:

The user can decouple either peer from HA from the **Controls and Configuration** slideout.

1 Decouple either peer by clicking **Go Standalone**.

A dialog appears showing any warnings, if any:

Examples:

- *Standby peer is not connected*
- *Database is not synchronized*

The user is asked if they want to wait until synchronization is finished.

2 If the user chooses to continue, the decoupling sequence begins.

3 If status is synchronizing and user wants to wait:

Wait for synchronized state (with timeout)

4 Create an NMS backup as a restore point in case of failure.

5 If this is the active peer:

Disconnect switch connections

Tear down VIP

6 If this is the standby peer:

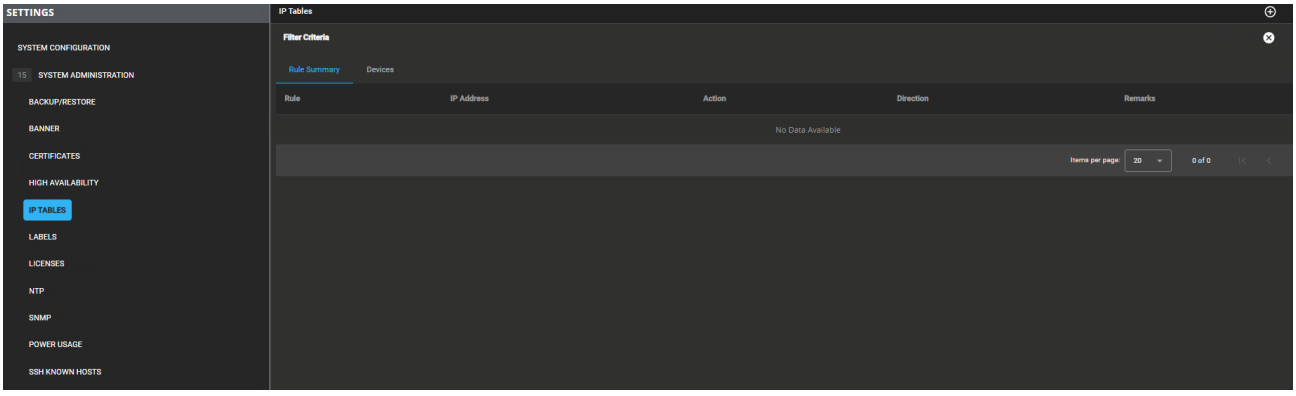
Delete switches or clear database

7 Mark HA role as **standalone**.

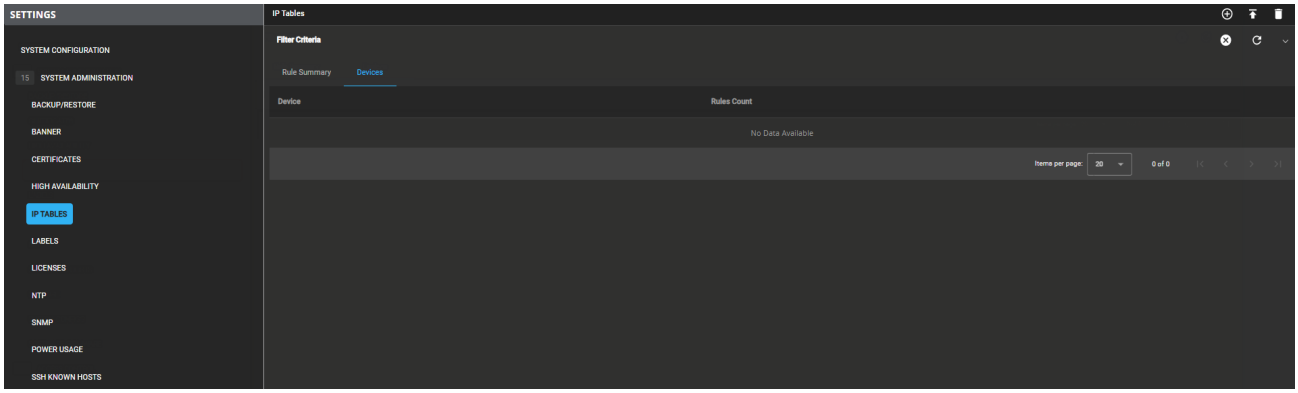
IP Tables

The IP Tables feature allows the user to view the summary and manage firewall rules.

- The Rule Summary table provides a list of rules available on the Central server for the user to push to managed devices.



- The Device table provides a list of the managed devices.



- All the rules that are created in NMS will only be displayed under the Rule Summary tab.
- Rules that are published from NMS to the switch and rules that are learned from a device will be displayed under the Device Summary tab.
  - New rules will be created in the selected devices that do not already have a rule with the same rule name.
  - If a device has an existing rule with the same rule name, which is being added, then the existing rule will be overwritten.
- If the NMS learns rules from switch, with same names and same content then, it will be overwritten
- Rule associated with device will be displayed in managed devices section.
- Existing rules in the NMS will be displayed under the Rule Summary tab.

> **Note:** If the content of a rule in the NMS and a rule in a device are the same (including remarks), then NMS and device have a common rule. This rule can be edited from the Rule Summary tab for the device as well, but if they have same rule name but different content it would be an entirely different rule.

Rules can be added by clicking on the Plus icon in the top right side of the screen. The user can also delete one or more rules by clicking on the Trash icon, also on the top right side of the screen.

The user can also apply rules in bulk by clicking on the Up Arrow icon.

Adding Rules

The following information must be included when adding a new rule:

- Rule name
- IP address
- Action - permit or deny
- Direction - ingress or egress
- Remarks

The new rule can be added to the rule inventory or can be applied to a specific device by selecting the device form the Devices tab.

> **Note:** The Devices tab will be greyed out if there are no managed devices or the rule details are not filled out or invalid.

Editing Rules

Click on a row to edit that rule.

Bulk Publishing

To perform a bulk rules publishing, click on the Up Arrow icon, then select the rules and devices and click Apply All to publish the selected rules to the specified devices. Only those devices which can accept the selected rules will be listed during a bulk publish.

Device Details

To view device details, click on a specific row for a specific device. A display will open with that devices rules information.

Device details will be displayed if there is at least one rule present on a device.

When you click on a row in the Rule Summary tab, an update action is performed. In the Devices tab, only those devices will be listed on which the current rule is applied. If the selected rule is not applied to any device, then no devices will be listed.

You can delete one or more rules by checking the boxes for the specific rules or you can select the All check box at the top and then click on the Trash icon.

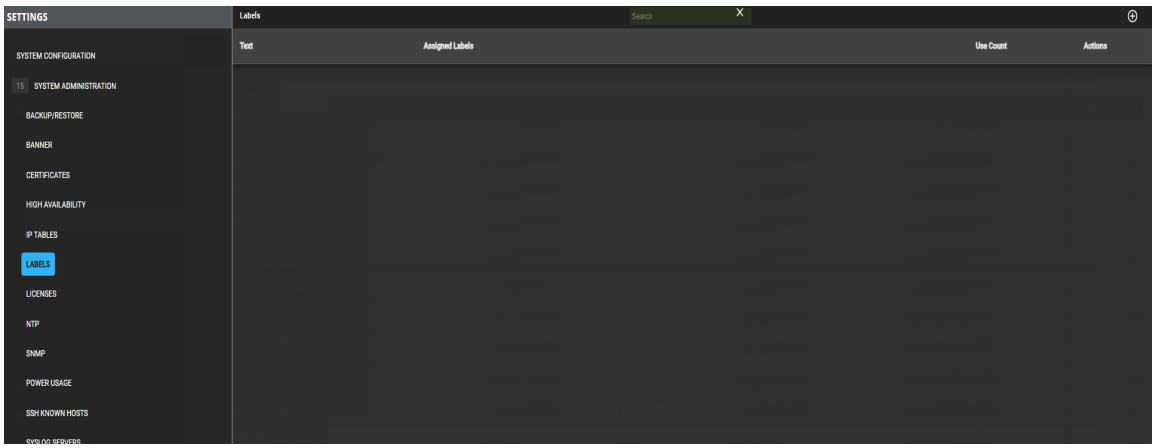
You can also edit a rule by clicking on the row for that rule. A display will open allowing you to edit the specific rule details. Click apply when you are done editing the rule.

Note: Changes made in this display will only apply to the selected device.

Labels

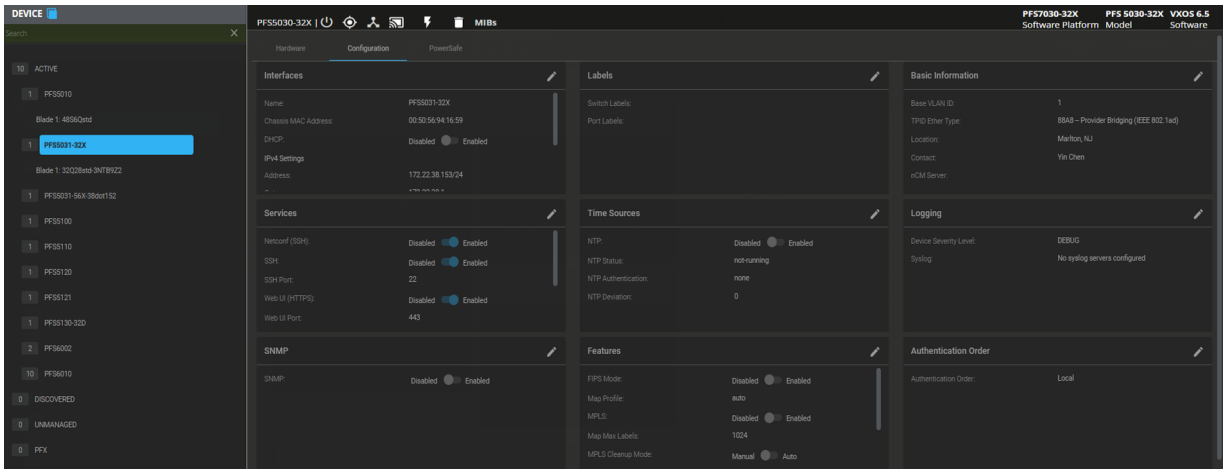
The Labels feature allows the user to focus on specific parts of their system by labeling entities, by their use case, and then filtering menus and views in the application using the labels. The labels are generic and customizable. Entities inherit labels from their parent entities (e.g., ports inherit labels from their PFS) and from their children (e.g., PFS inherit labels from their ports).

From the LABELS section in the System lifecycle the user can view a list of all the labels and search for specific labels.

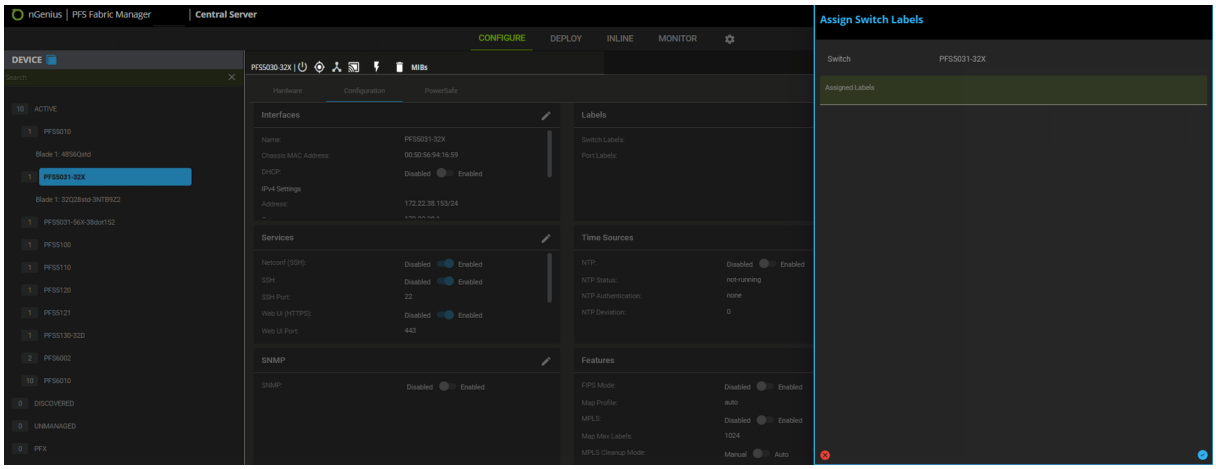


Labeling Switches

From the Configure > Device menu, select an active device and then Configuraton tab to view the labels and inherited labels for that switch.

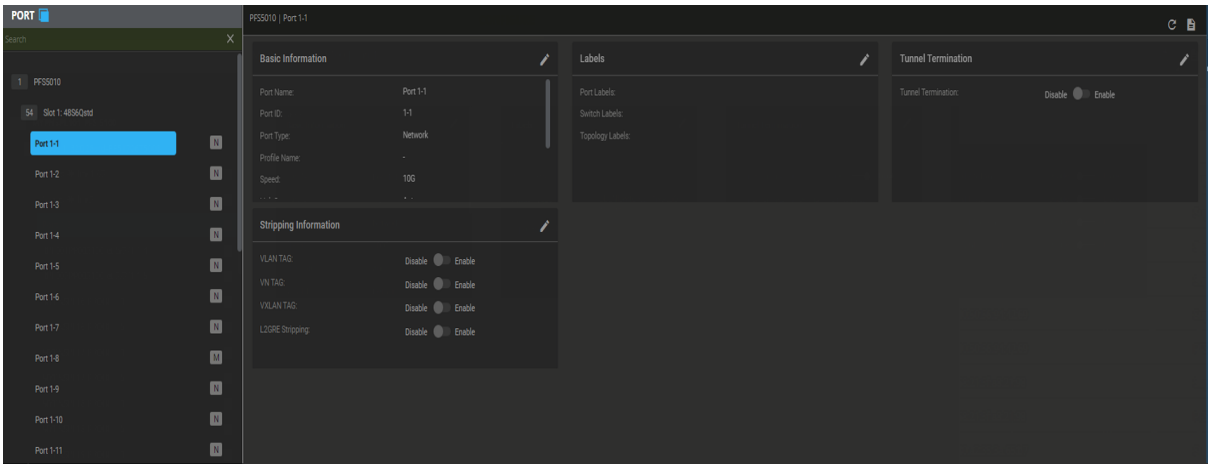


New labels can be added directly from any interface that applies labels.

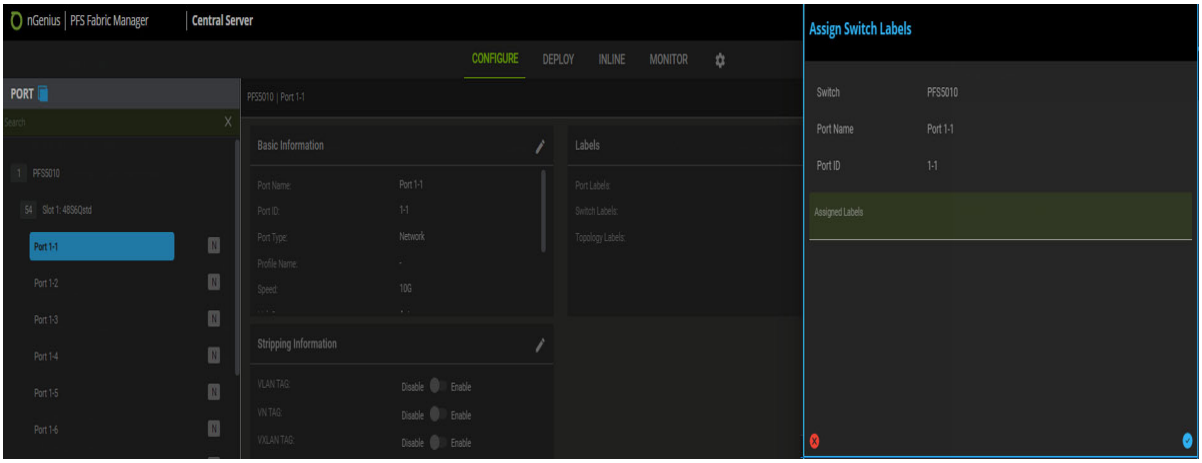


Labeling Ports

From the Configure > Port menu, select a port to view the labels and inherited labels for that port.



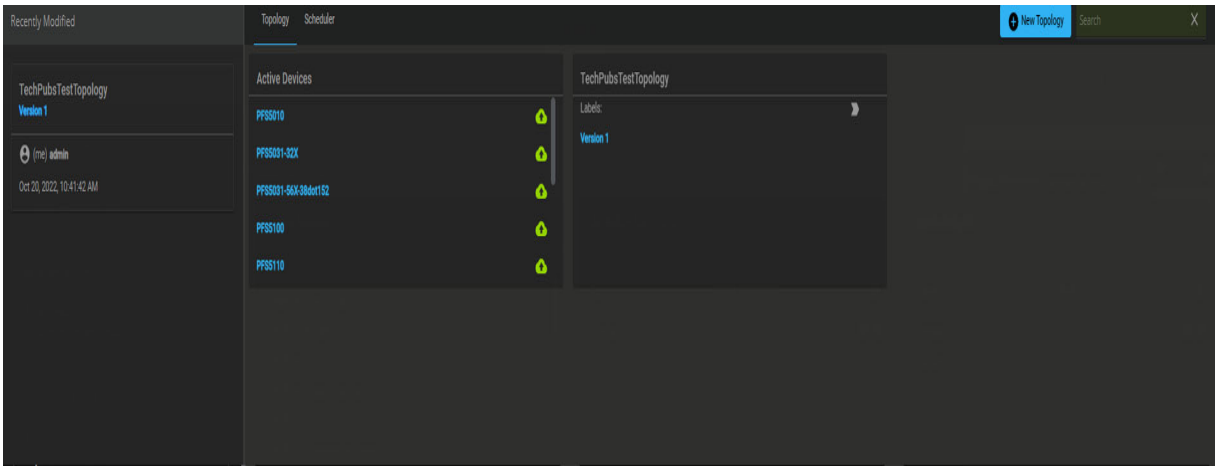
Users can assign labels to ports.



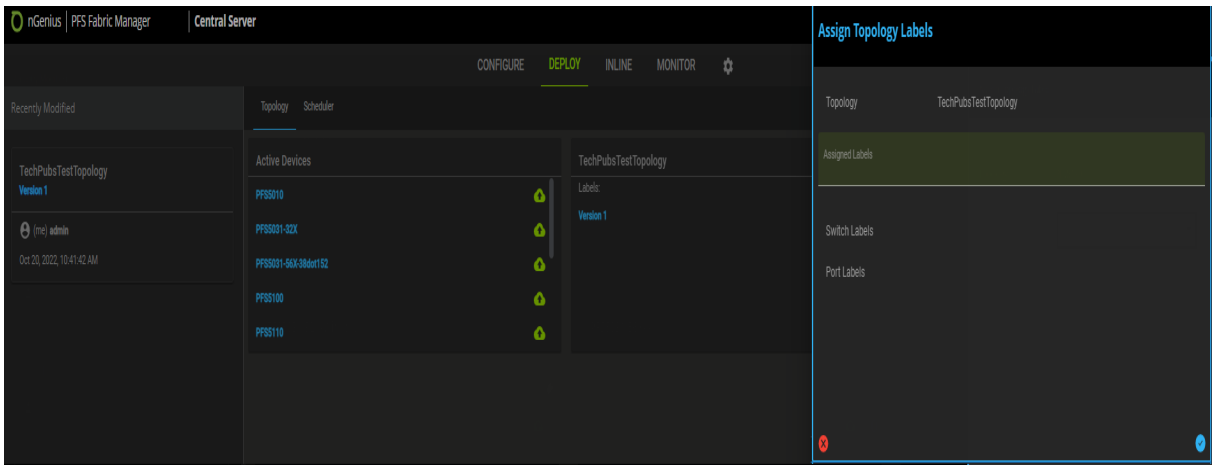
Labeling Topologies

From the Deploy> Topology tab, select a topology to view a merged list of all the labels and inherited labels for each version.

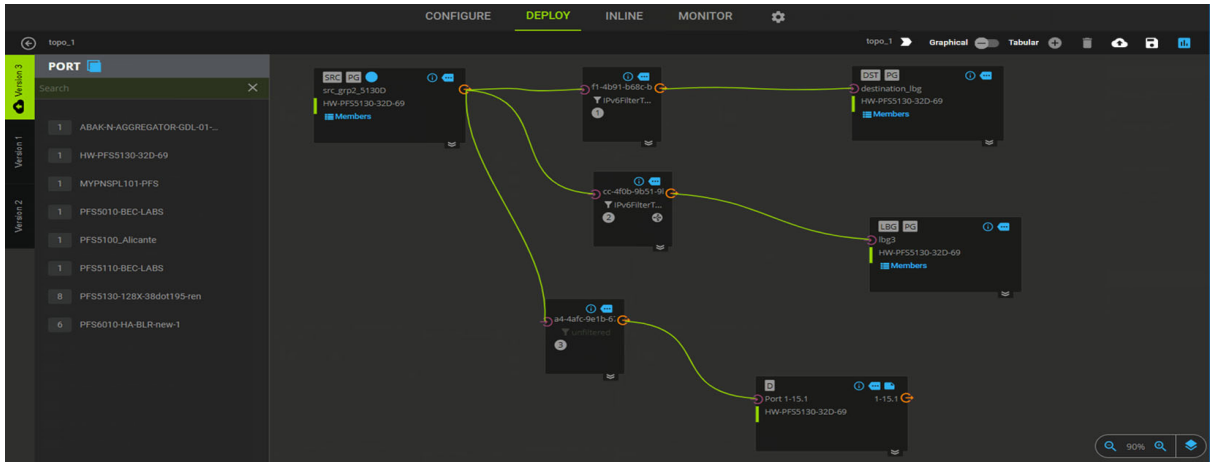
> **Note:** Topologies are labeled for all versions. Different versions of the same topology cannot have different labels applied directly, however each version can inherit different sets of labels.



Users can assign labels to topologies from the overview page.



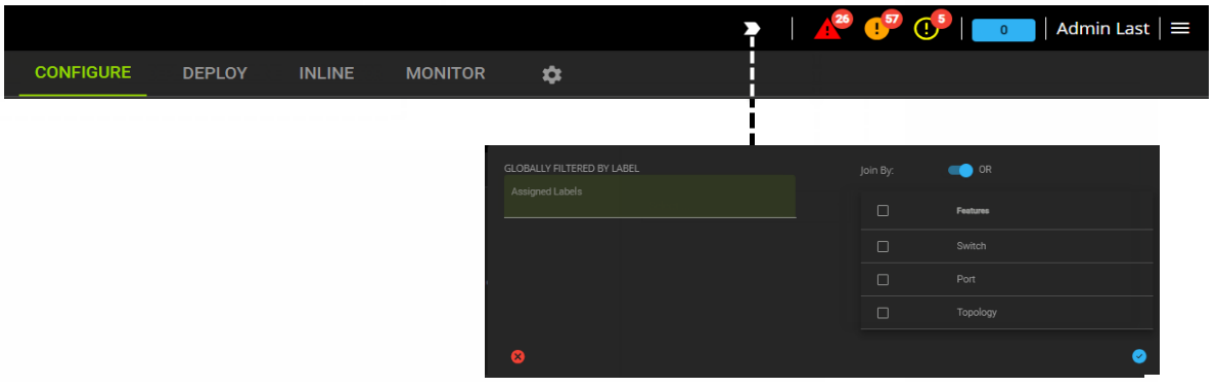
When viewing a specific topology version, users can see all the applied labels and inherited labels for that version. Users can also assign labels and can view assigned port labels from the graphical topology by clicking on the Tag icon on the port node.



Global Filtering

Users can apply one or more labels globally, which will filter the entire interface by that label. If a user selects more than one label, they can choose to use AND/OR filtering.

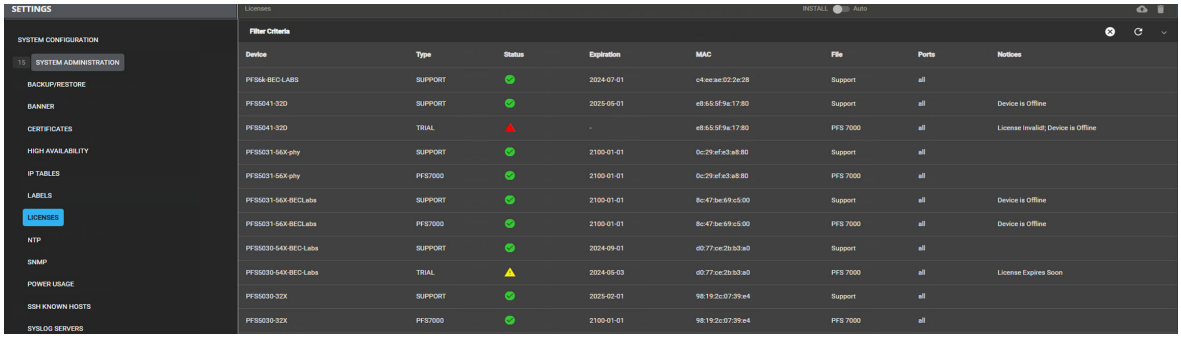
Note: If AND is selected, all entities must match all labels. If OR is selected, entities may match any label.



Licenses

The Licenses feature allows the user to manage PFOS Support and PFS 7000 licenses for all devices from a single screen; on this screen you can view the details of each license, its status and whether it is expired or soon to be expired. The user can also select automatic or manual installation of the licenses.

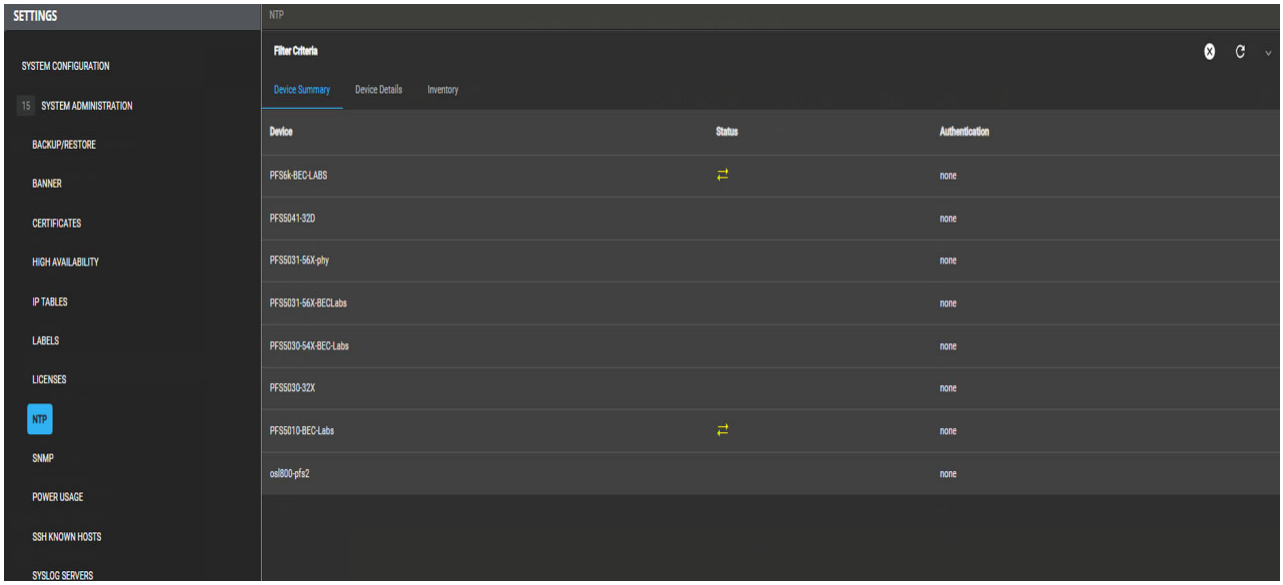
- When automatic license installation is enabled, licenses will be automatically installed when a license file is read and its license(s) are added. If the device is not on-line, the system will wait until a device with a matching MAC comes on-line and then install the license.
- License installation is a 2-step process when manual license installation is enabled. After adding a license, the user will click Install. This displays a panel with a list of all uninstalled licenses that can be installed at that time. The user then can select which license(s) to install and install them.



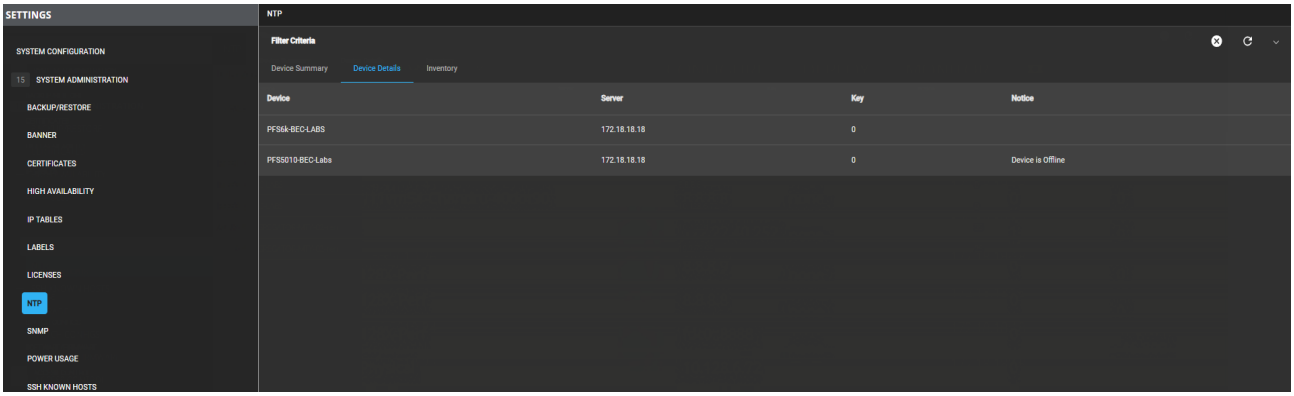
NTP

The NTP feature allows the user to specify up to three Network Time Protocol (NTP) servers to provide updated time to the system clock. After NTP synchronization is configured, up to five minutes may elapse before the first synchronization with the external server occurs. After that, the system is resynchronized once every five seconds.

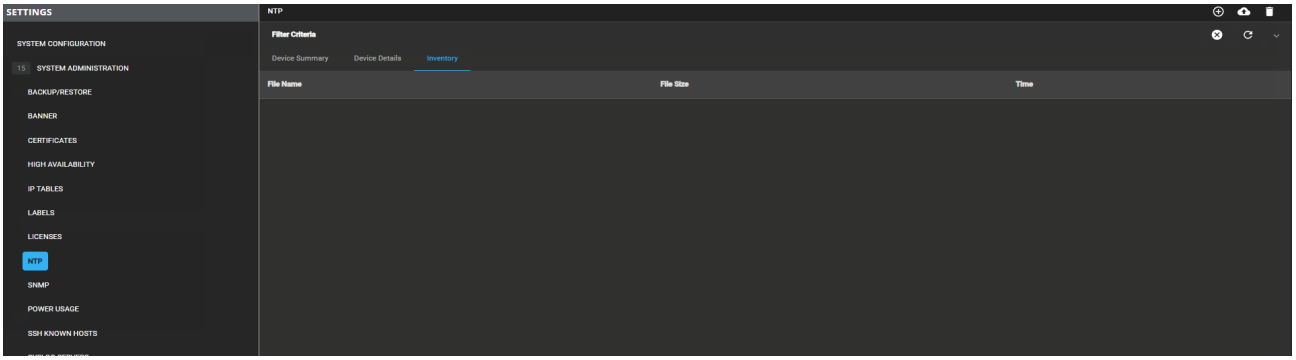
- Device Summary tab - provides the device name, status of the connection, required authentication, and the deviation of the system clock from the NTP source at the last update, and any adjustment are displayed.



- Device Details tab - provides the device name, the IP/hostname of the NTP server, the key, and displays any notices.



- Inventory tab - provides a list of the available NTP key files.

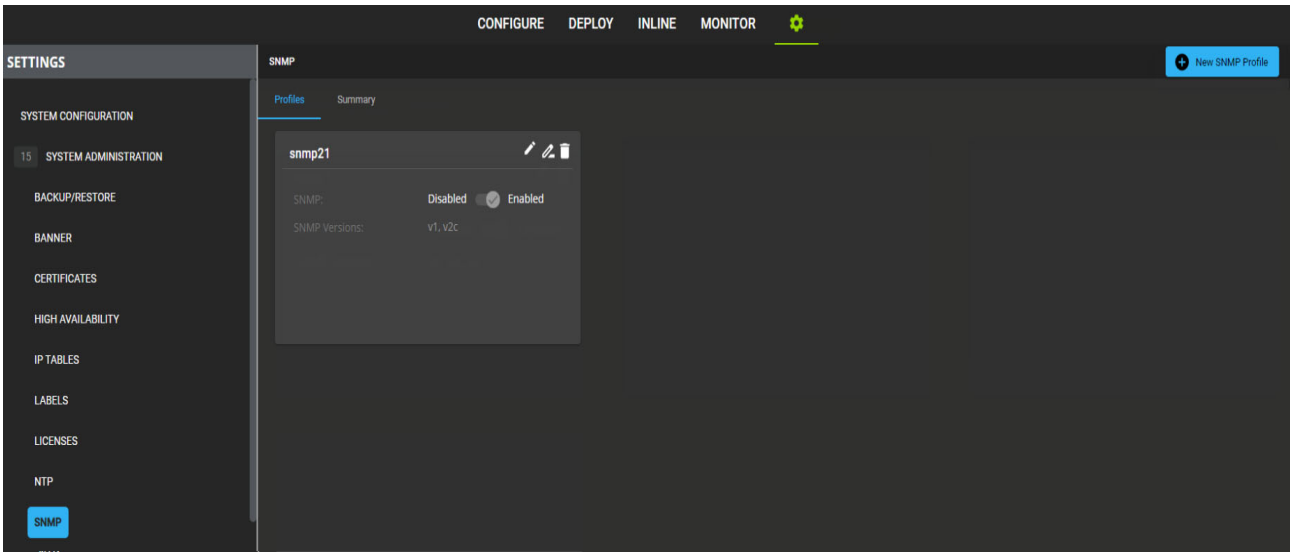


SNMP

The SNMP feature allows the user to configure SNMP information to enable the PFS-FM to accept/respond to SNMP get requests for standard MIB information and to send SNMP traps to remove SNMP agents.

> **Note:** NMS running on Oracle Linux 8 must have security update 2024-04-09 or later installed in order support SNMP. NMS running Oracle Linux 9 all have the prerequisite updates installed.

Navigate to Settings > System Administration > SNMP to create, view, and manage existing SNMP profiles and associate them with NMS and/or managed devices.

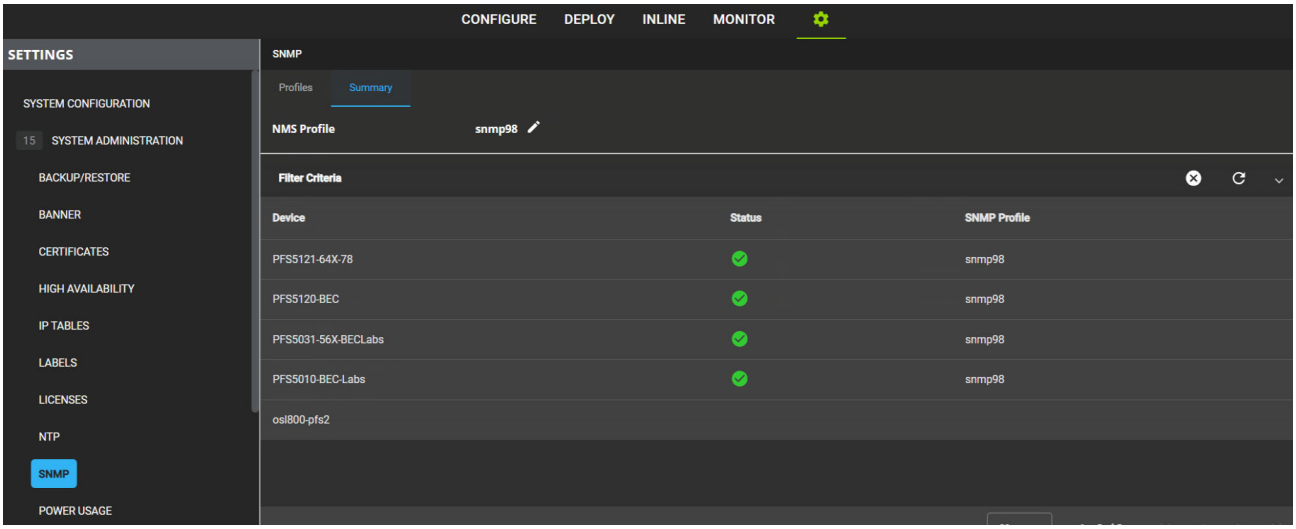


Each vCard allows the user to perform the following actions:

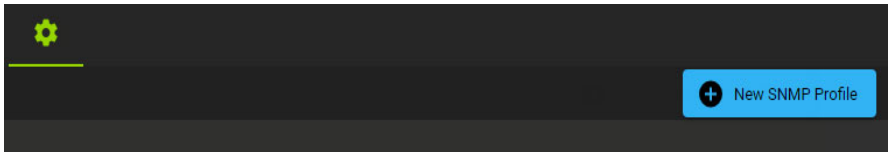
- Edit the profile by clicking on the Edit Pencil icon.
- Rename the profile by clicking on the Rename Pencil icon.
- Delete the profile by clicking on the Trash icon.

> **Note:** Deleting an SNMP profile does not remove the SNMP configuration on any devices using the profile.

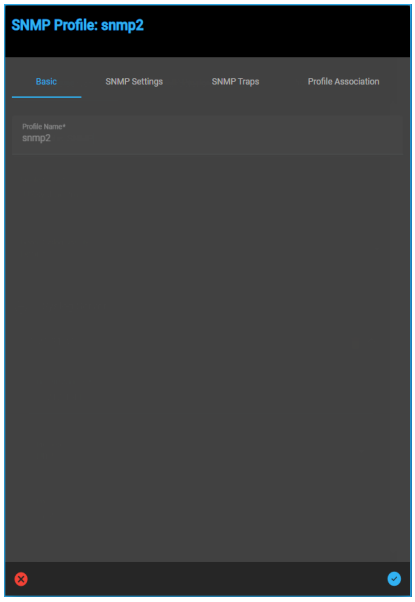
Click on the Summary tab to view existing associations between NMS and managed devices with profiles.



To configure SNMP settings for NMS and managed devices, first create a profile by clicking on '+ New SNMP Profile' button.



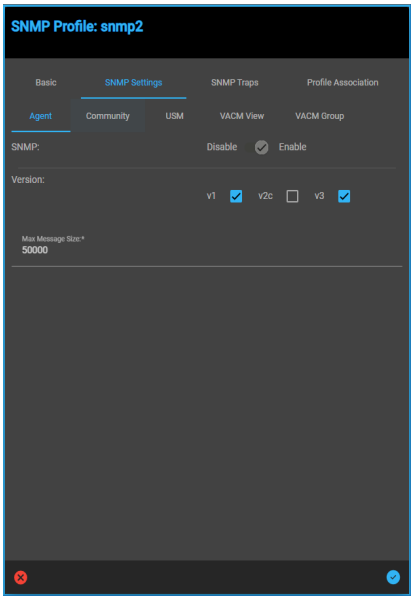
1 In the **Basic** tab, enter a profile name.

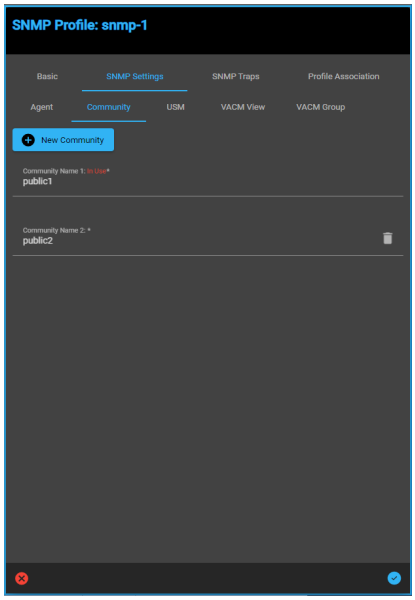


2 In the **SNMP Settings** tab, configure the following SNMP parameters: Agent, Community, USM, VACM View, and VACM Group.

3 In the Agent tab, enable/disable SNMP, select at least one version, and enter an optional message.

In the **Community** tab, enter a community name.

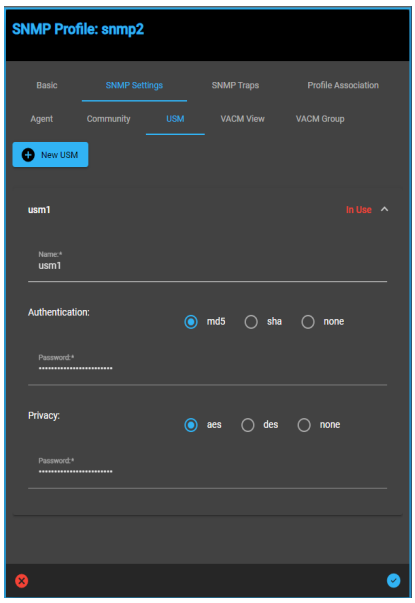


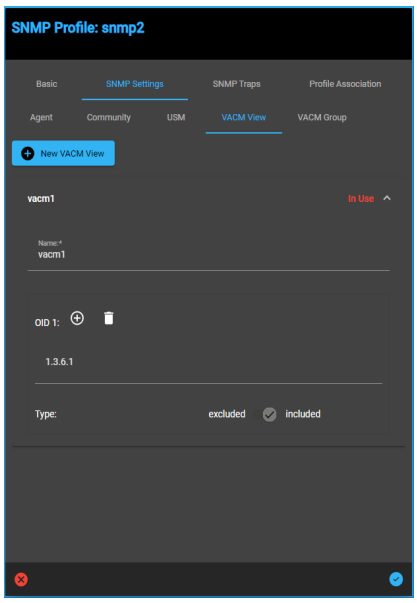


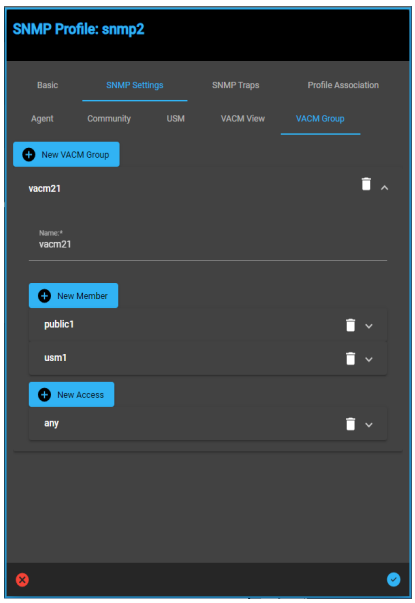
In the **USM** tab, enter a name and select the type of authentication and privacy.

In the **VACM View** tab, enter a name and the OID and then select the view type: excluded/included.

In the **VACM Group** tab, select a security option (USM/Community) and a security model (version/USM), select a security name from the drop down menu, and then configure the Access.





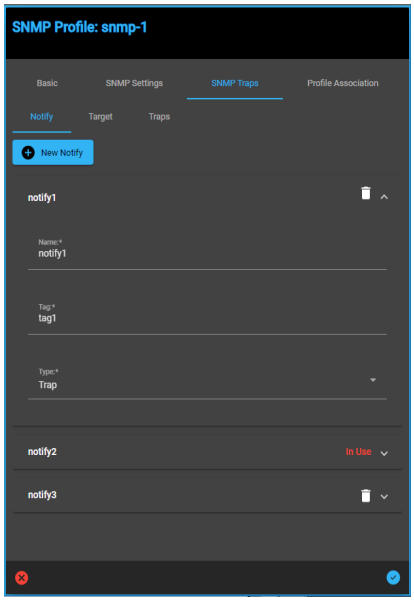


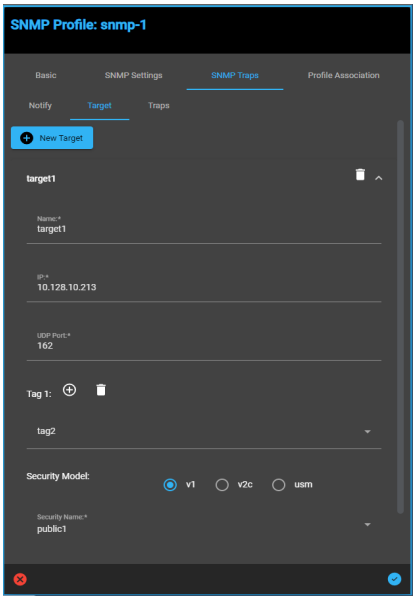
4 In the **SNMP Traps** tab, configure Notify, Target, and Traps.

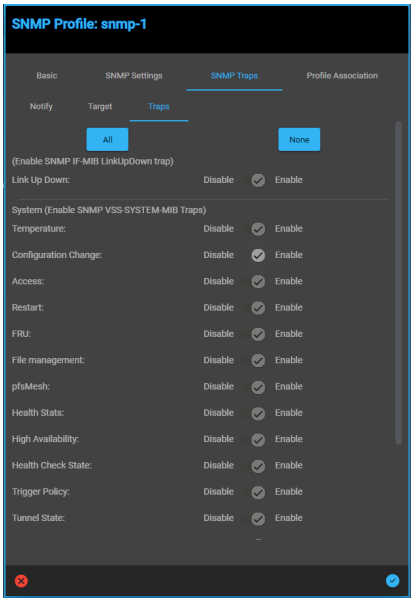
In the **Notify** tab, enter a name and tag name, and then select a notify type.

In the **Target** tab, enter a name, IP address and UDP port number; select a Tag1 from the drop down menu, and then select a security model.

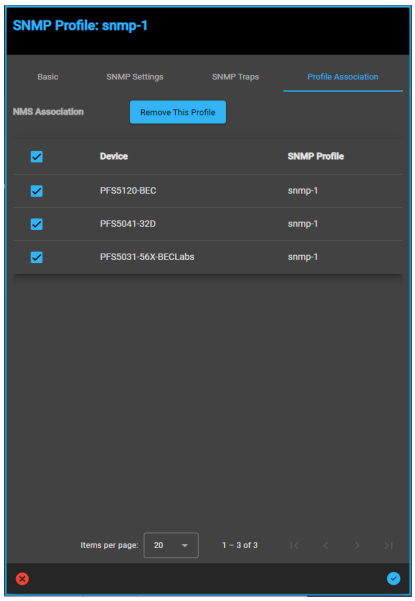
In the **Traps** tab, select to enable/disable all or none of the traps or you can select to enable/disable individual traps.







5 In the **Profile Association** tab, assign the SNMP profile to an NMS and/or managed device.



Users can associate that profile with NMS and/or managed devices in one of the following ways:

- Making the association at the same time while creating a profile
- Selecting devices while editing a profile
- Selecting a device under the 'Summary' tab by clicking on a device of interest and picking the correct SNMP profile from the drop down list

> **Note:** If an SNMP profile's association to a device is removed, the SNMP configuration on the device is not cleared (only the association to the profile is removed).

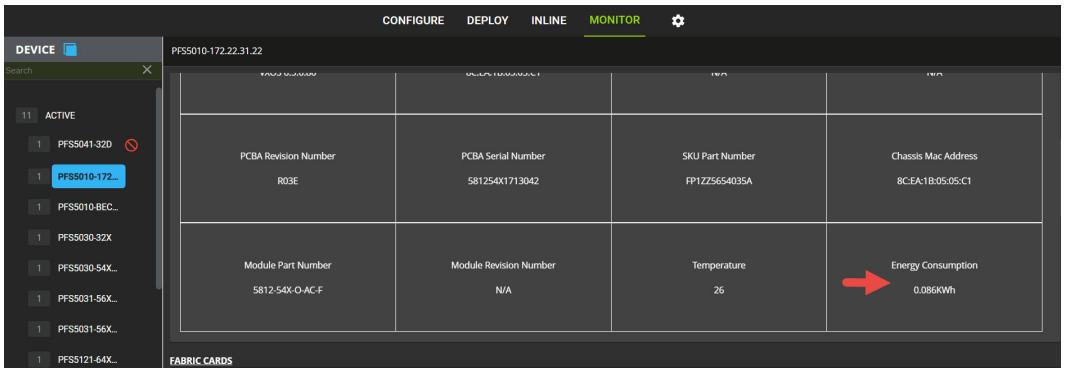
Power Usage

The Power Savings feature allows the user to view detailed power usage statistics, displayed on the existing dashboard, which allows for the easy comparison of data for multiple devices. The feature also provides for reducing some amount of power consumption of the system.

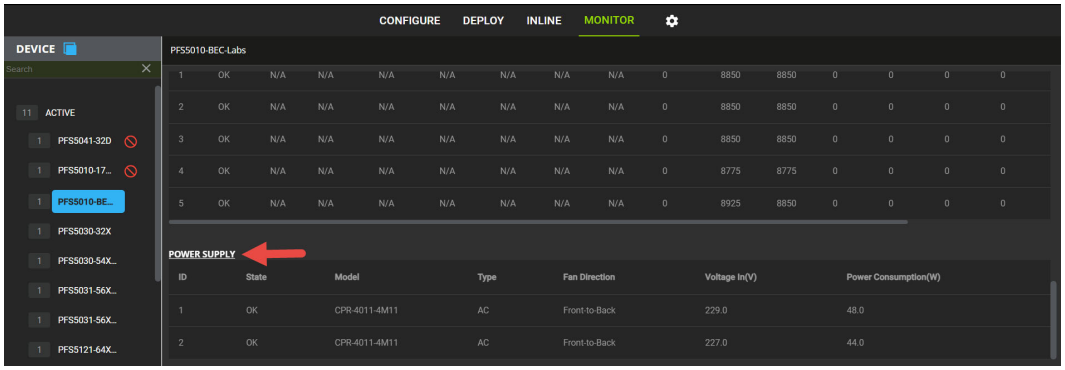
Note: The power consumption feature is not supported in PFS6000 systems.

Switch Power Consumption

To view power consumption on switch basis, navigate to Monitor Lifecycle > Device > Switch status.



To view Power Supply details on switch basis, navigate to Monitor Lifecycle > Device > Power supply.



Switch Power Consumption Real Time Statistics

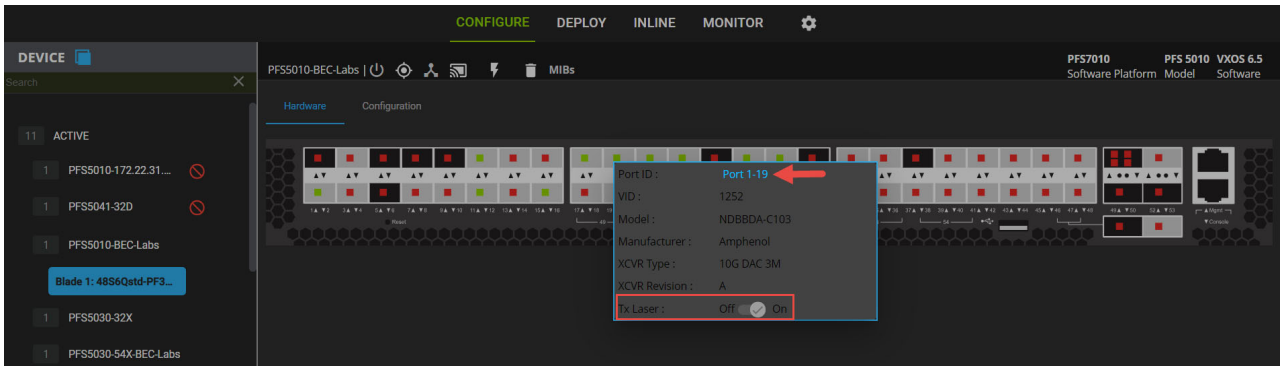
You can create a dashboard to monitor switch power consumption over time. Refer to Dashboard on page 6-14 for detailed steps to create the dashboard and use the following parameters:

- Widget Type: Device
- Name: Name for the widget
- Widget View: Tabular or Graphical
- Time Selection: Last Day, One Week or Custom
- Stats Selection: Energy Consumption (kWh)
- Device Selection: Device or devices to monitor

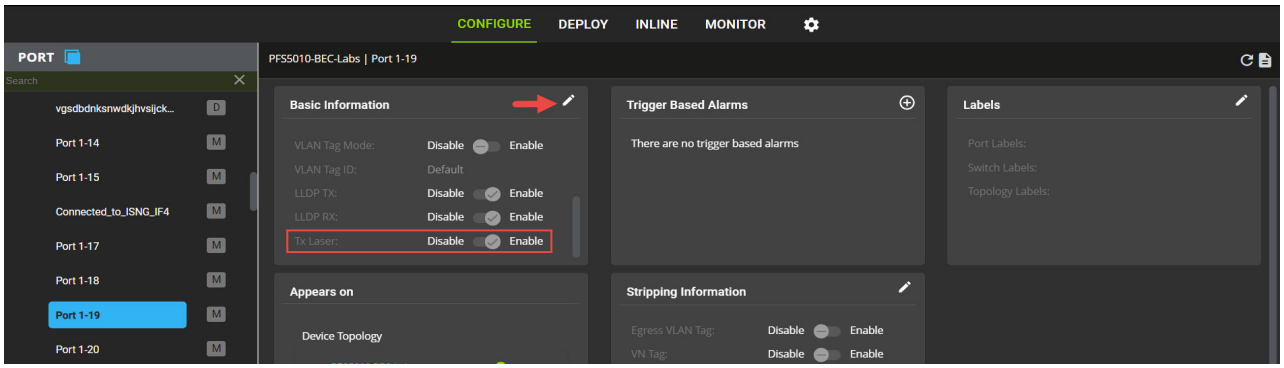
Port Laser TX Setting

You can reduce the amount of power consumption of the system by turning off the transceiver transmitter.

You can turn off the transceiver transmitter by navigating to Configure Lifecycle > Device > Hardware and clicking on a port from the switch graphic or navigating to Configure Lifecycle > Port > Port # > Basic Information and clicking on the Edit icon.

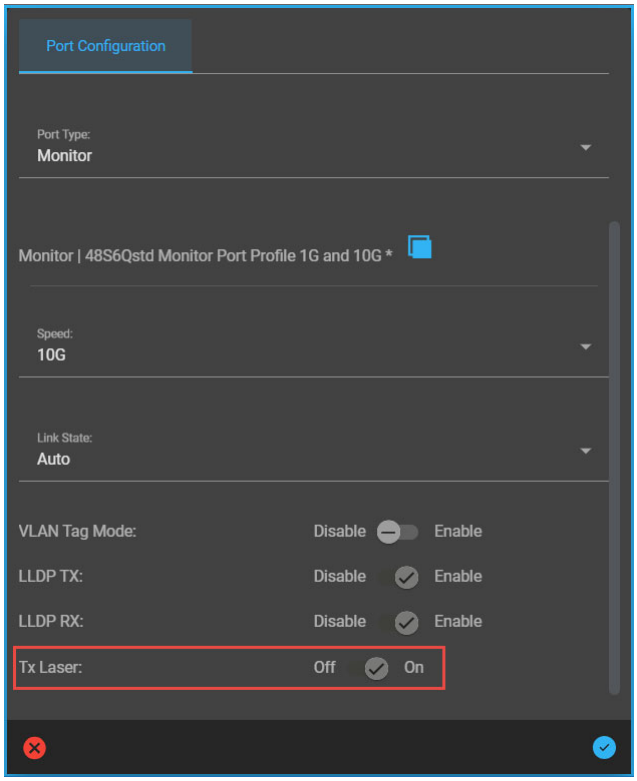


Device Perspective

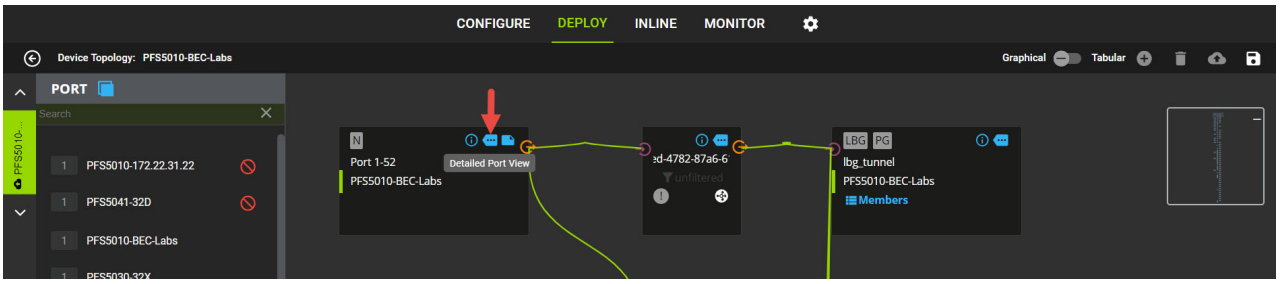


Port Perspective

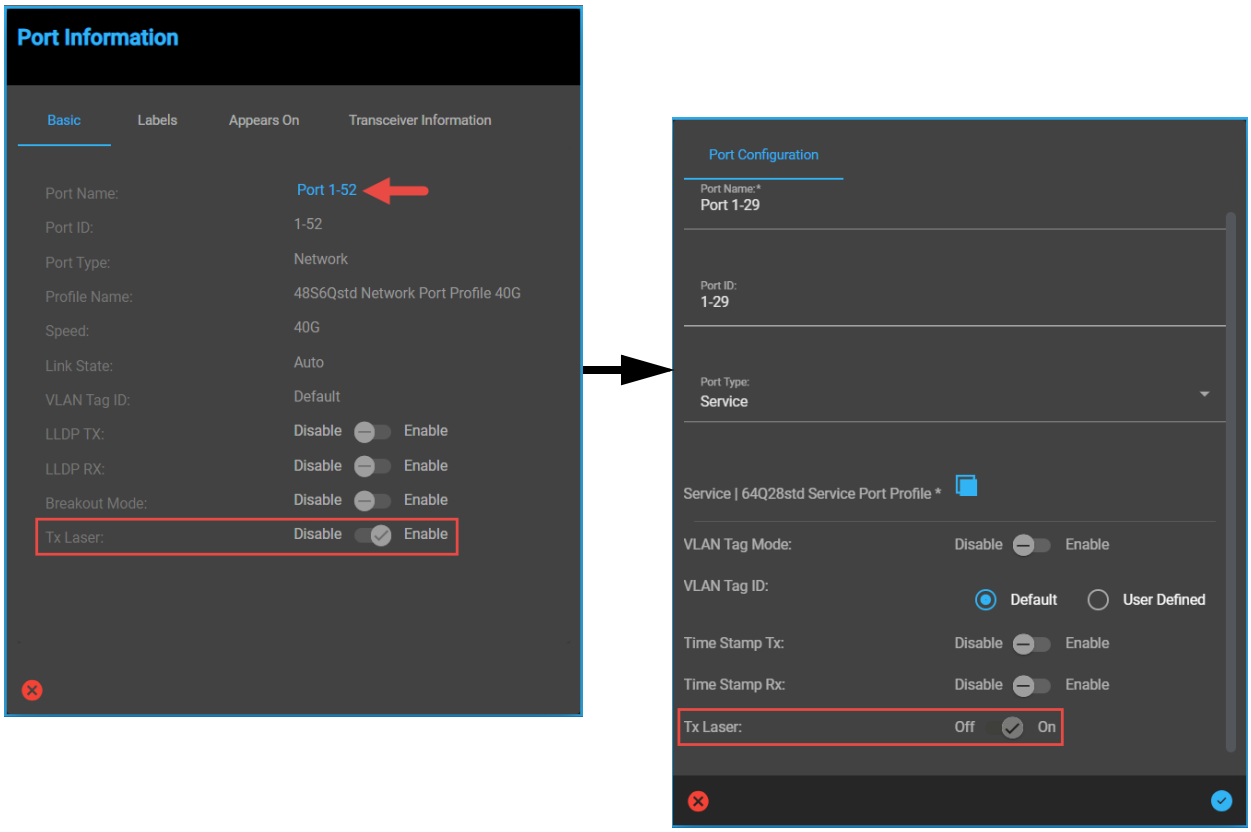
A Port Configuration pop-up is displayed where you can enable/disable the transceiver transmitter and then accept the configuration.



You can also turn off the transceiver transmitter by navigating to Deploy Lifecycle > select a Topology> select a Port Node and click on the Detailed Port View icon.

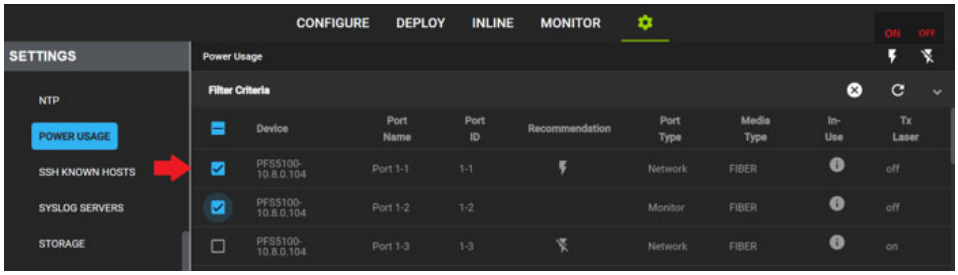


A Port Information pop-up is displayed. Click on the port name and a Port Configuration pop-up is displayed where you can enable/disable the transceiver transmitter and then accept the configuration.

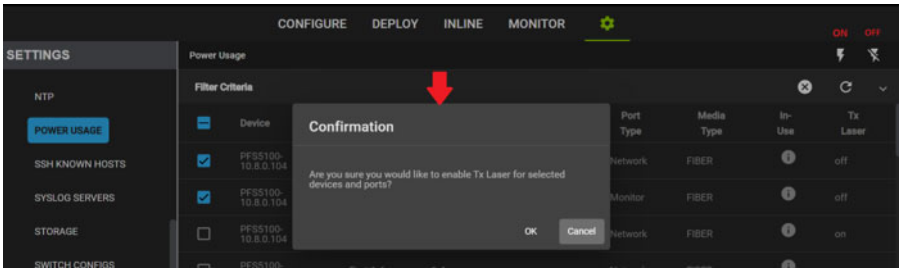


You can also enable/disable the transceiver transmitter for multiple ports at the same time. Navigate to Settings > System Administration > Power Usage.

Select the desired ports and then select On/Off from the icons on the top right corner of the screen.



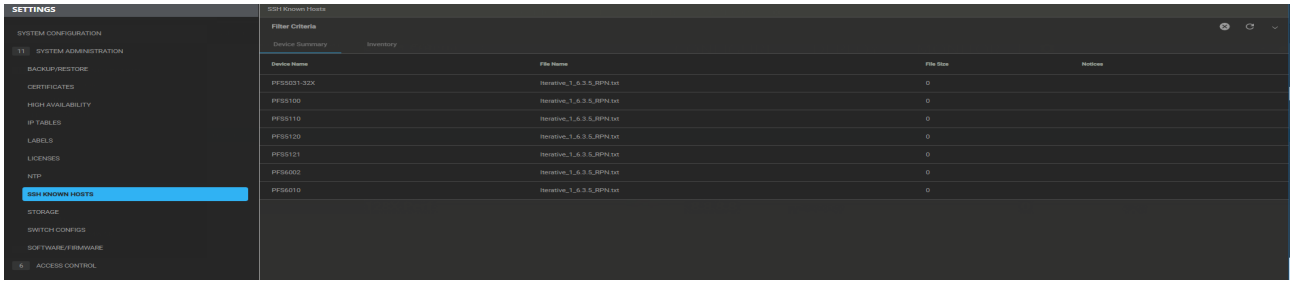
A confirmation pop-up is displayed. Click **Ok** to accept.



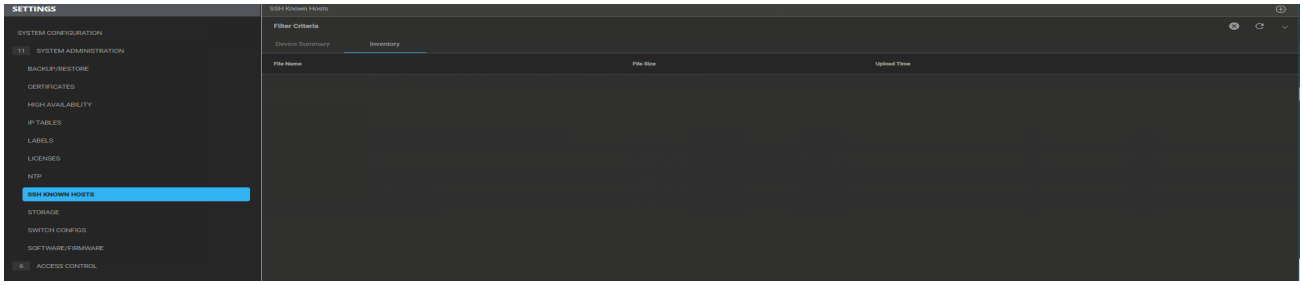
SSH Known Hosts

The SSH Known Hosts feature displays a table of devices and the names of any known hosts on each device.

- Device Summary tab - provides the device name, file name, file size, and displays any notices.



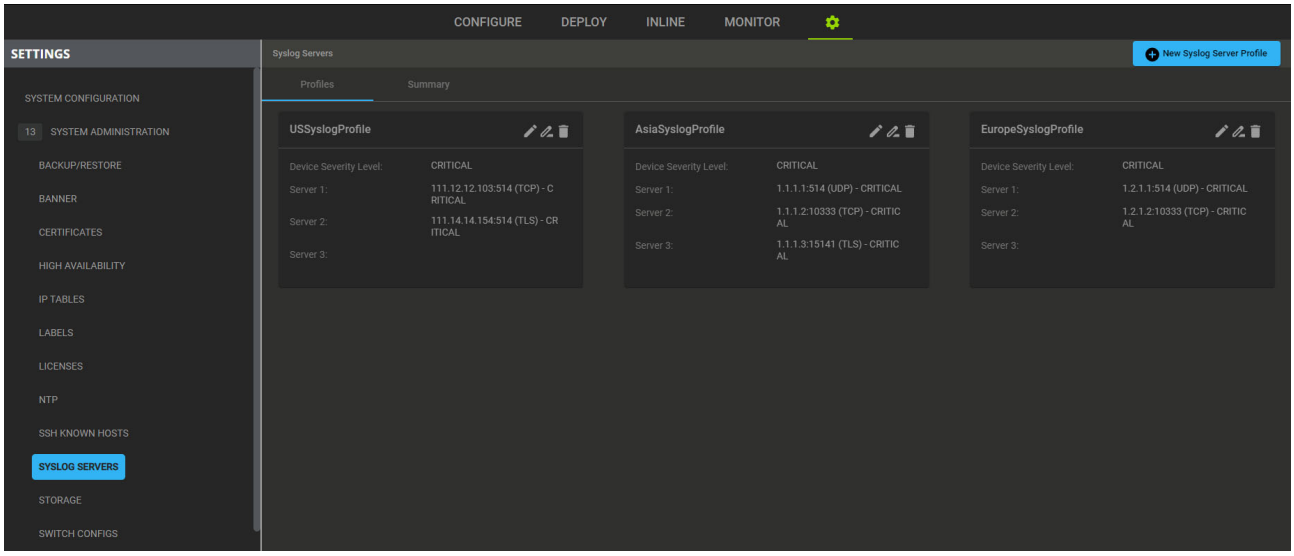
- Inventory tab - provides a list of the available SSH Known Hosts files.



Syslog Servers

The Syslog Servers feature allows the user to configure syslog parameters for NMS and, optionally, push the same configuration to managed devices (either individually or in bulk).Bulk syslog settings operate the same way as other bulk features.

Navigate to Settings > System Administration > Syslog Servers to view and manage existing syslog server profiles and associate them with NMS and/or managed devices.

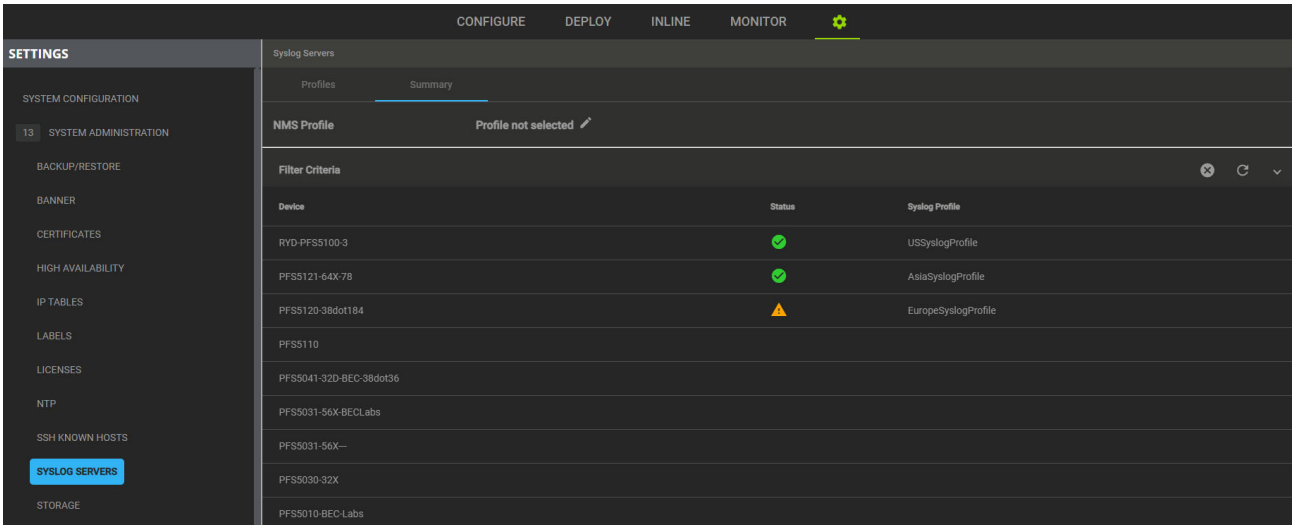


Each vCard allows the user to perform the following actions:

1. To quick view syslog servers associated with the profile.
2. Edit a profile by clicking on Pencil icon.
3. Delete a profile by clicking on Trash icon.

> **Note:** Deleting a profile removes associations with existing devices. It does not remove that device syslog servers configuration.

Click on the Summary tab to view existing associations between NMS and managed devices with profiles.

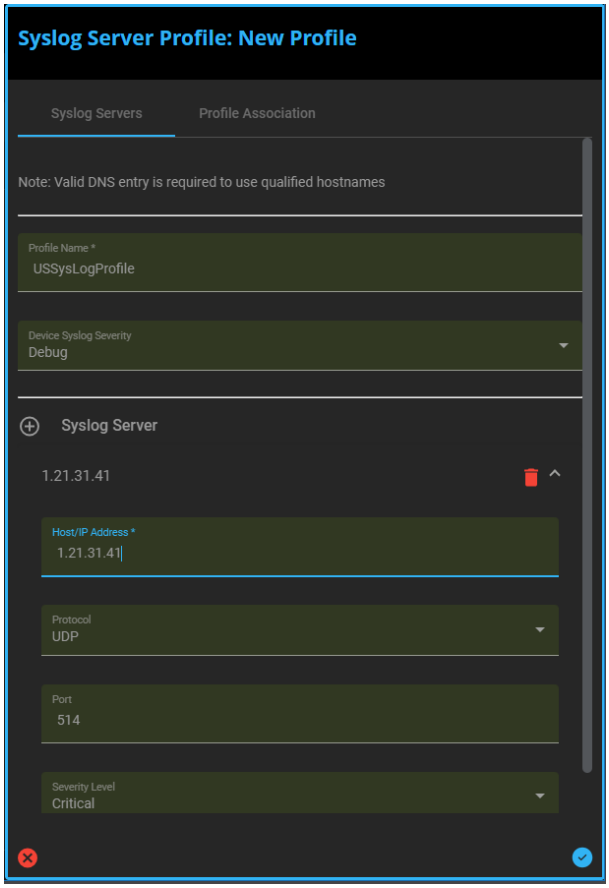


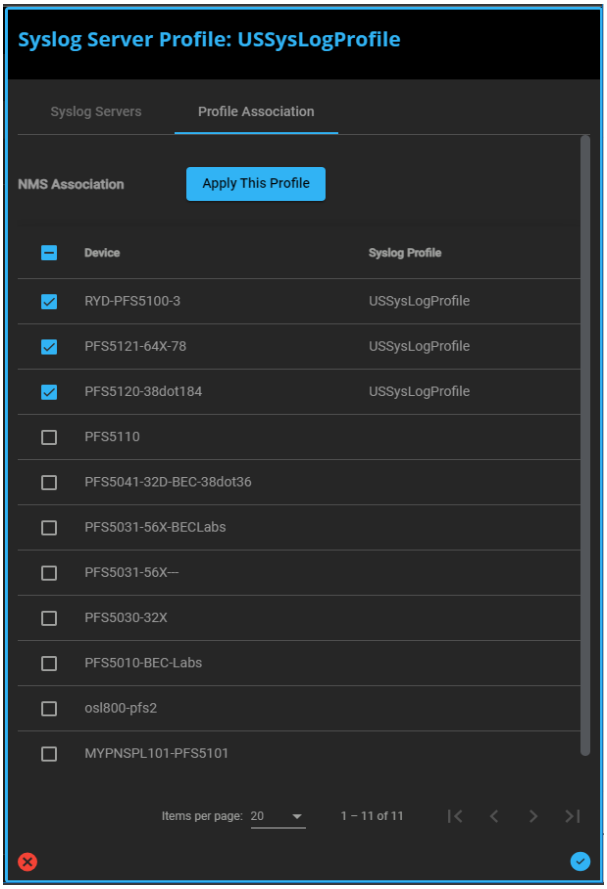
To configure syslog server settings for NMS and managed devices, first create a profile containing 1-3 syslog servers, by clicking on '+ New Syslog Server Profile' button.

Users can associate that profile with NMS and/or managed devices in one of the following ways:

- Making the association at the same time while creating a profile
- Selecting devices while editing a profile
- Selecting a device under the 'Summary' tab by clicking on a device of interest and picking the correct syslog profile from the drop down list

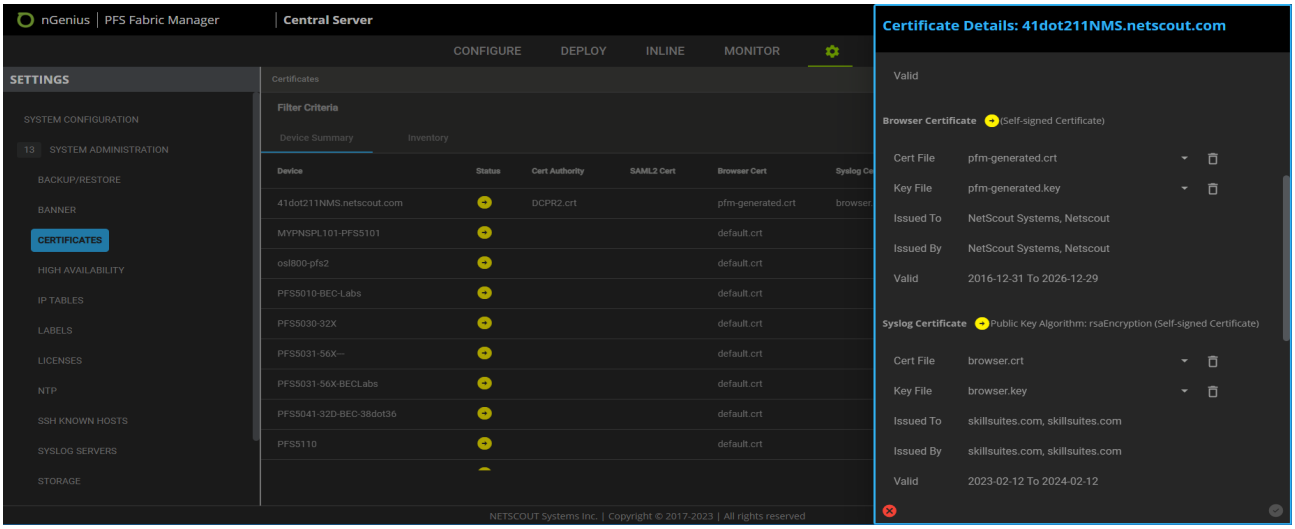
> **Note:** If a syslog profile's association to a device is removed, the syslog configuration on the device is not cleared (only the association to the profile is removed).





To associate a device with an existing Syslog profile, simply click on a device/NMS row and select or clear the associated profile.

Currently, Syslog certificates are uploaded and applied for managed devices only.



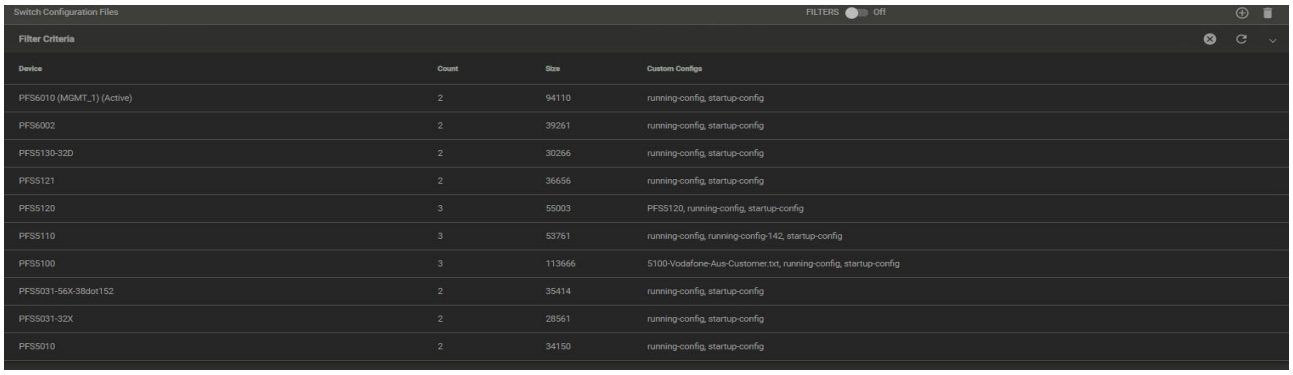
Storage

The Storage feature allows the user to monitor storage alarms for all devices to detect deviation outside of operating parameters. Alarm information is displayed as dashboard: a device summary is displayed which shows each active device's alarm status, reported disk usage for root and non-volatile partitions, and cores count.

Switch Configs

The Switch Configuration feature displays a table of devices (excluding the NMS) and the names of any installed user configurations on each device. The summary table is searchable with filter and paging controls. A detailed slide-out panel is invoked by highlighting a device row in the summary table.

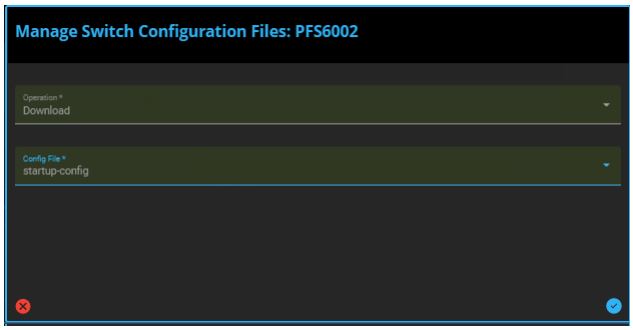
The panel shows the current full set of configuration files on the selected device and allows the files to be viewed, copied, downloaded or applied.



Selecting/clicking on a row displays the Manage Switch Configuration Files details.

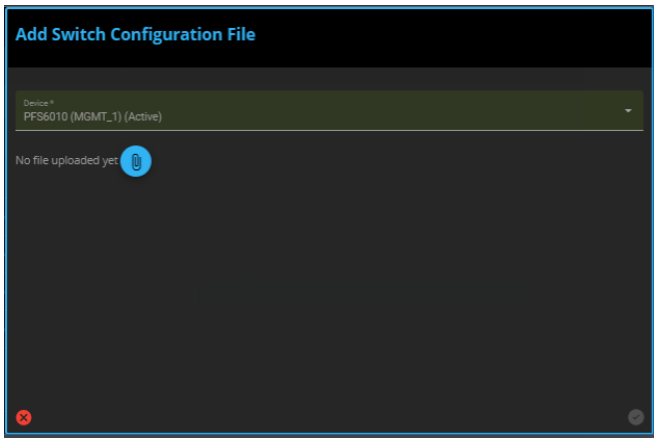
Note: If a PFS-6010 device is selected, a Target CPU drop down menu is included in the Manage Switch Configuration Files window. The user can select the target CPU of the PFS-6010 device on which to apply the selected operation and config file.

If a card is not valid (empty/disabled), the related card option of the Target CPU drop down menu is disabled.



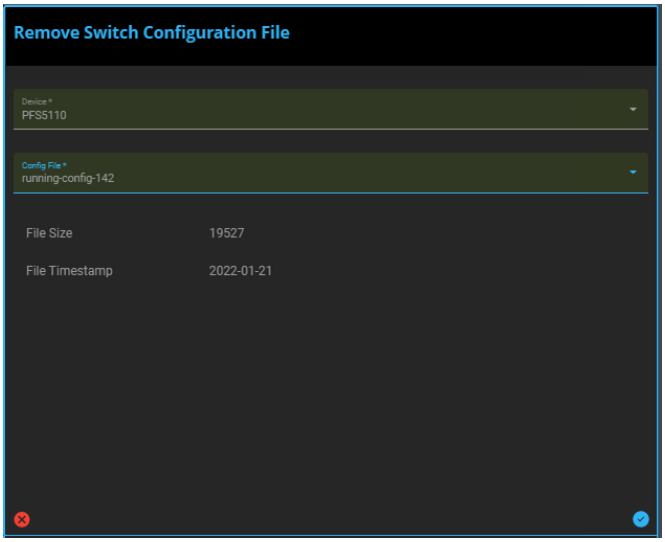
Users can add configuration files by clicking on the add icon. This displays the Add Switch Configuration File window.

Note: If the selected device is a PFS-6010 device, an additional Target CPU drop down menu is displayed. The Target CPU drop down menu is used to select the management card of the PFS-6010 device on which the selected config files are uploaded. If a card is empty or invalid that option is disabled.



Configuration files are removed by clicking on the remove icon. This displays the Remove Switch Configuration File window.

The selected configuration file will be removed from the selected device and management card (management card is applicable only for PFS-6010 devices).



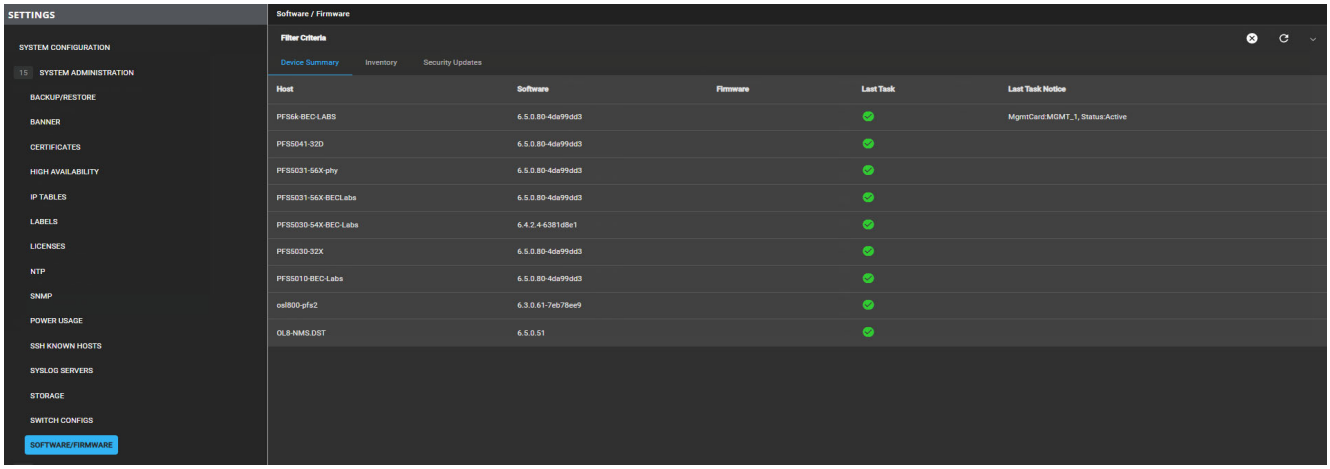
Software/Firmware

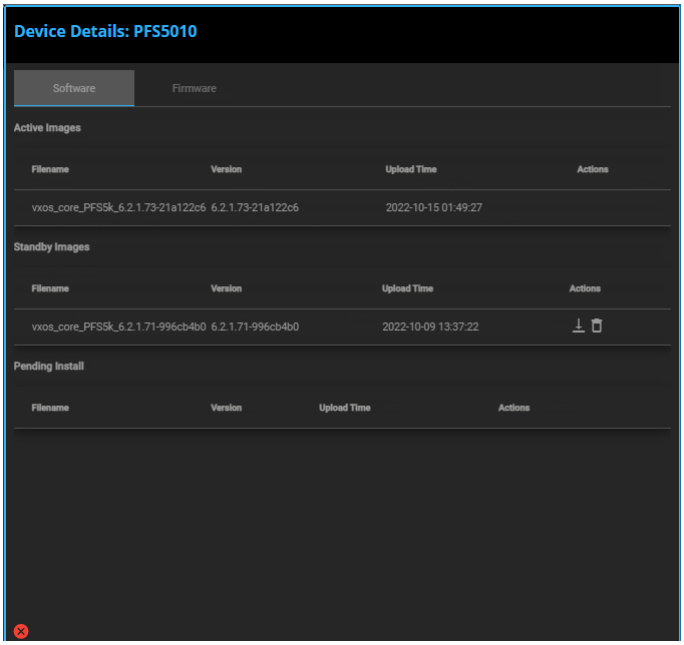
The Software/Firmware feature displays the software and firmware that is currently installed on the PFS Fabric Manager Central server and Manged devices. The user is able to add, apply, and remove software images on the PFS Manager and Managed devices and add, apply, and remove firmware images on the Managed devices.

Note: Software downgrades are not supported at this time.

Clicking on **Software/Firmware** displays the current and standby software installed on the PFS Fabric Manager server and managed devices. Clicking on the **Check Mark** icon (under Last Install) displays the current software image details of the installed software (current and all standby versions). Clicking on the **Delete** icon allows removing a standby (not-current) software version.

Clicking on **Device Summary** and then an accepted switch / device displays the software information of the PFS Fabric Manager server and the PFOS software operating on the switch / device.

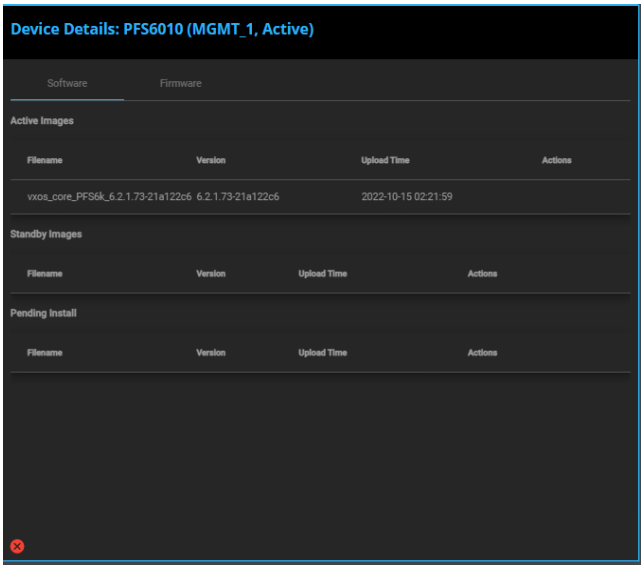




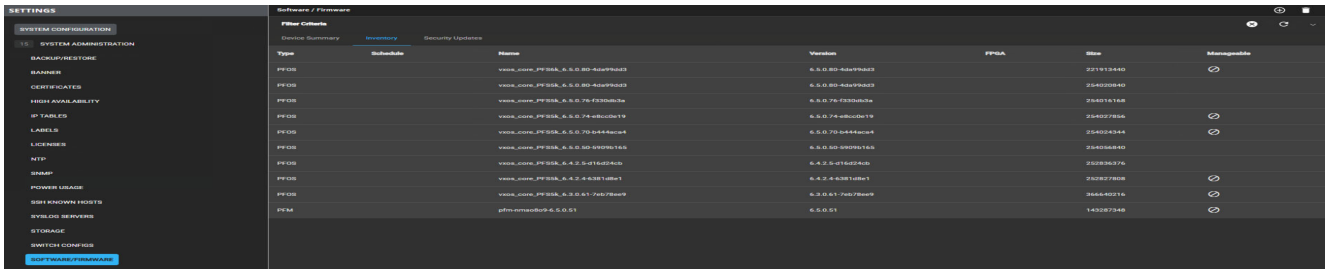
If the selected row is for a PFS-6010, the Device Details displays a segment control option. The selected Mgmt card is highlighted in blue and if there is only one management card, then other Mgmt card is disabled (grayed out).

Mgmt-1 and Mgmt-2 will show the images details on respective management cards.

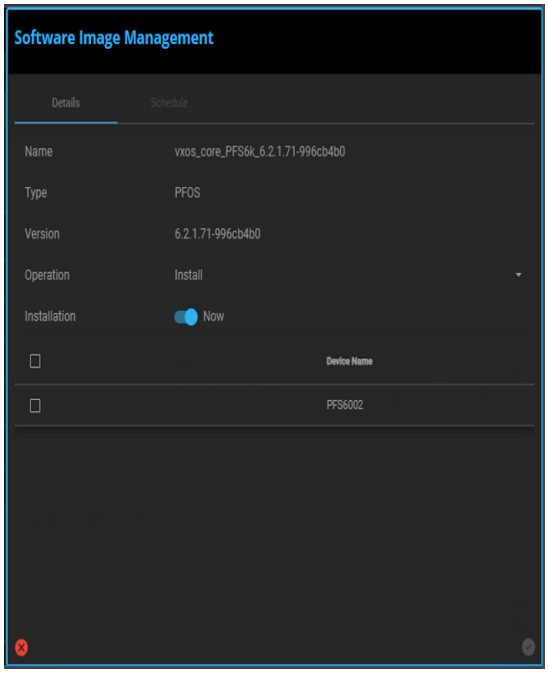
The apply image and delete image operations are applicable for images on both the cards, in their respective space.



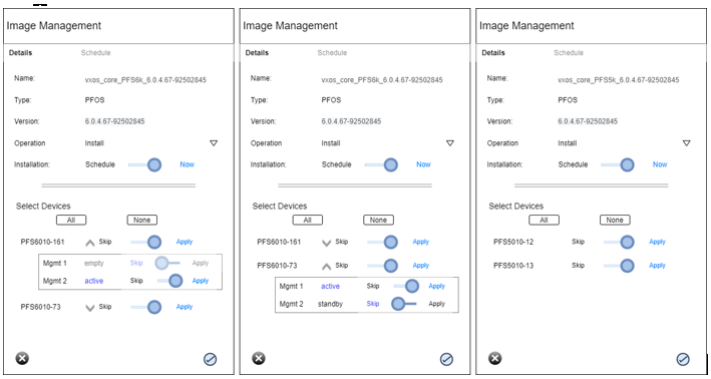
Clicking on **Inventory** displays a list of the available software loads for the PFS Fabric Manager server.



Click on a software load and the **Image Management** window is displayed. From this window you can select which device(s) to install or remove the software load.



On selection of operation, devices will be listed on which a selected operation can be applied and if there is a PFS-6010 device in the list and there are two management cards, then PFS-6010 device will give the options to select which Mgmt card the selected operation will be applied.



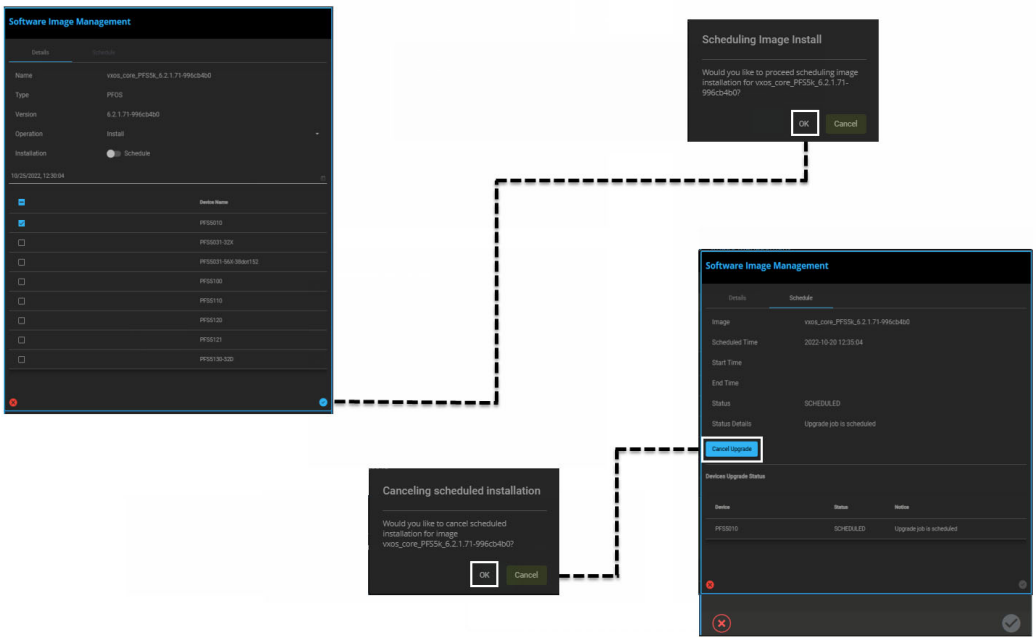
You can also schedule and cancel an install/upgrade from the **Image Management** window. Select **Schedule** and enter a time for the install/upgrade. To cancel an install/upgrade, click on **Cancel Upgrade**.

Note: The following apply to all scheduled installs/upgrades:

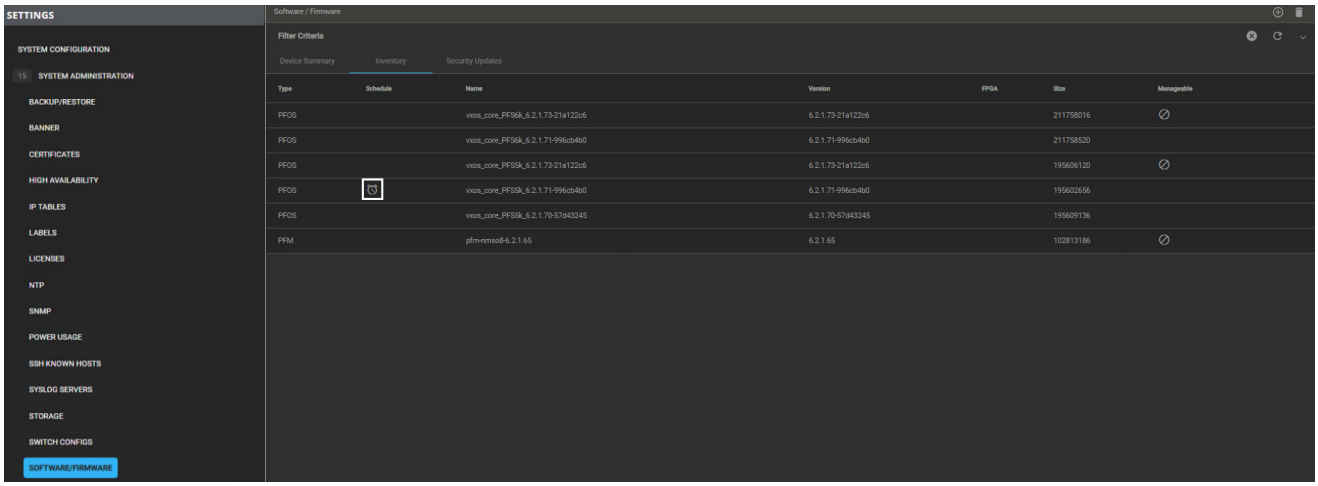
Schedule times are in the browser's local time zone.

An image cannot be scheduled for more than one schedule at a time.

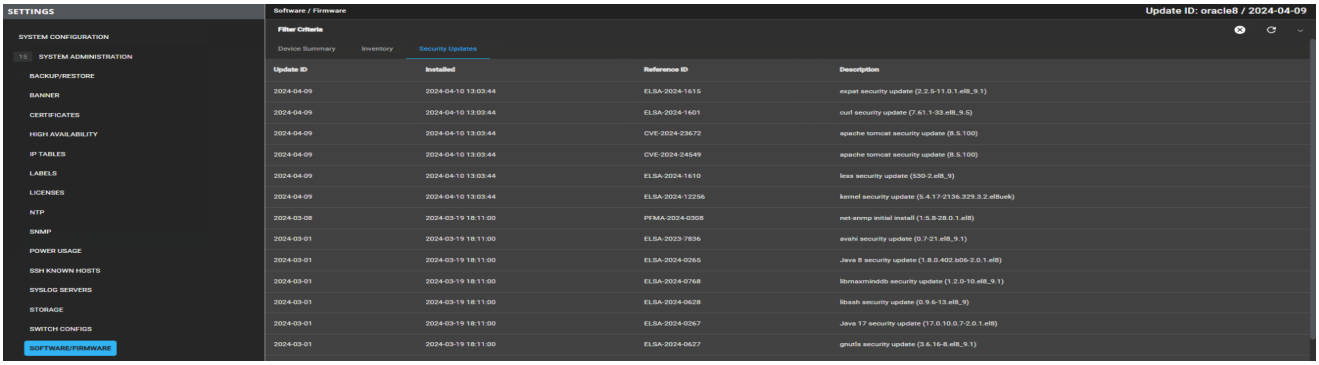
An image can be installed at the user's discretion, even if it is already scheduled for installation later.



When an install/upgrade has been scheduled, the Inventory tab will be updated with a Stopwatch icon under the **Schedule** column for the selected software load.



Clicking on **Security Updates** displays a list of the available security patches for the PFS Fabric Manager server.



From this window you can filter and sort the available security patches.

To install the security updates see *Security Updates for the PFS Fabric Manager (NMS) on a Central Server* in the PFS Fabric Manager Release Notes for details.

Note: As of 6.2.0, security updates can only be uploaded and installed from the NMS GUI.

Uploading / Upgrading PFOS Firmware

This feature allows the user to manage PFOS firmware installation - upload, delete, view and install.

Note: This feature is only supported on the PFS 6002 and 6010.

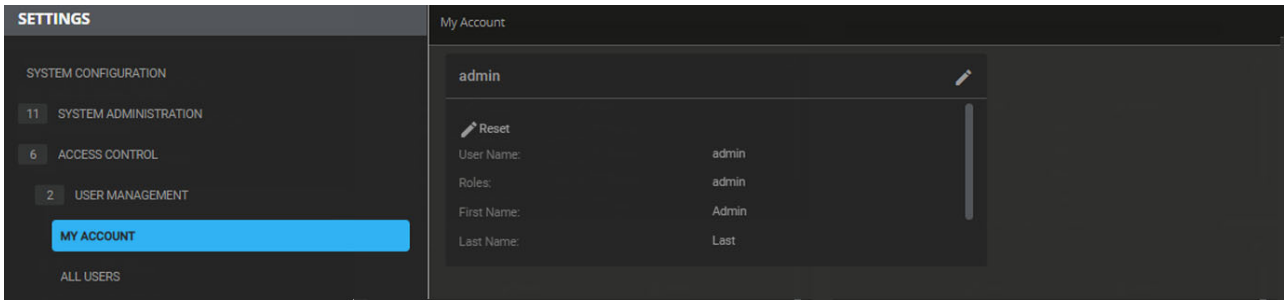
1. Select **Software Management**.
2. Select **(+) Upload**.
3. Select **Image Type > PFOS Firmware**.
4. Click **Browse** and select from the file manager, the **PFOS** firmware image (***firmware_inline-<revision>***) file.
5. Click **Open**, the file will upload to the GUI.
6. Once the upload completes, perform a refresh of the browser to display the newly uploaded firmware file (displayed in the PFOS Firmware file listing).
7. To complete the installation of the newly uploaded file, click the **Install** icon. From the Image Details screen, click **Install**; the file installation begins.
8. After the installation process completes, allow 5 minutes for internal file configuration to complete, then refresh the browser. The new firmware is now defined as Status = Current.

Access Control

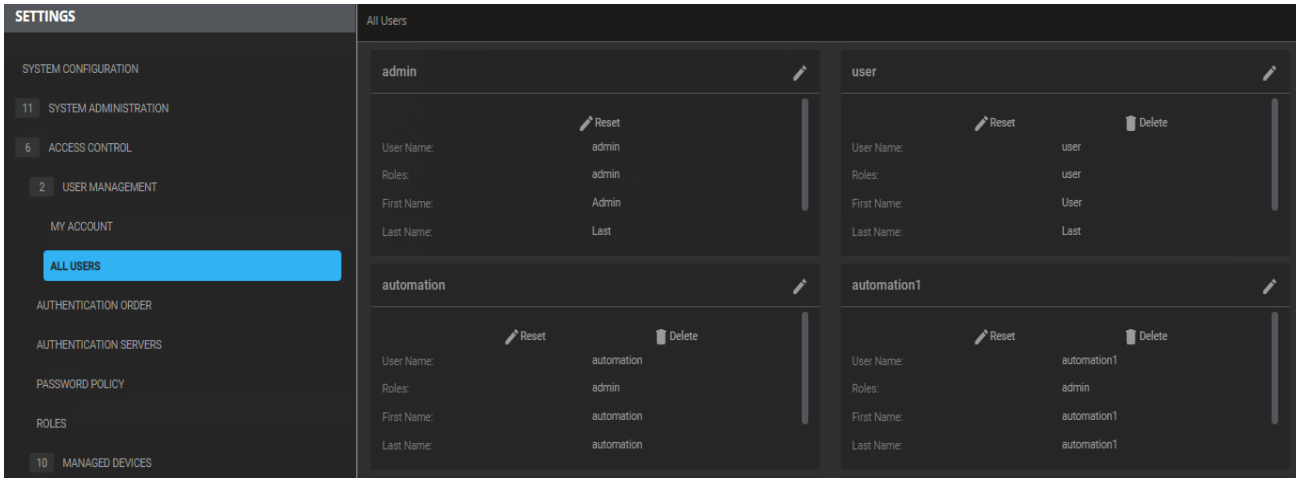
Selecting Access Control allows viewing and editing the User Management, Authentication Order, Authentication Servers, Password Policy, and Roles of the PFS Fabric Manager.

User Management

My Account

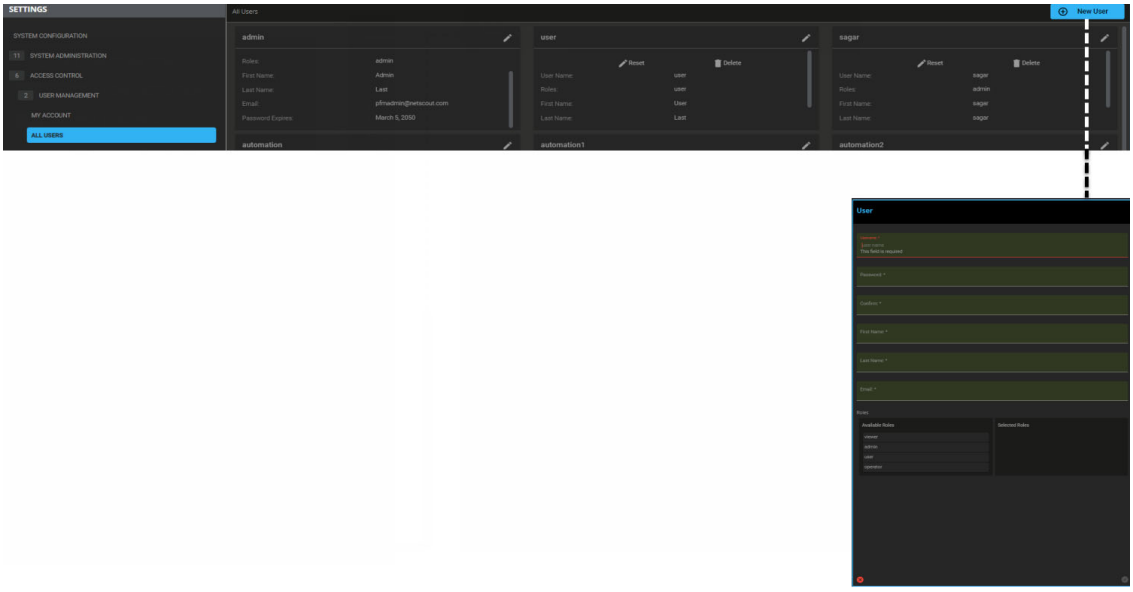


All Users



Add Users

From All Users, click on **+ Users** to add a new user to PFS Fabric Manager. Click on the **Accept** check mark to save the new user settings.



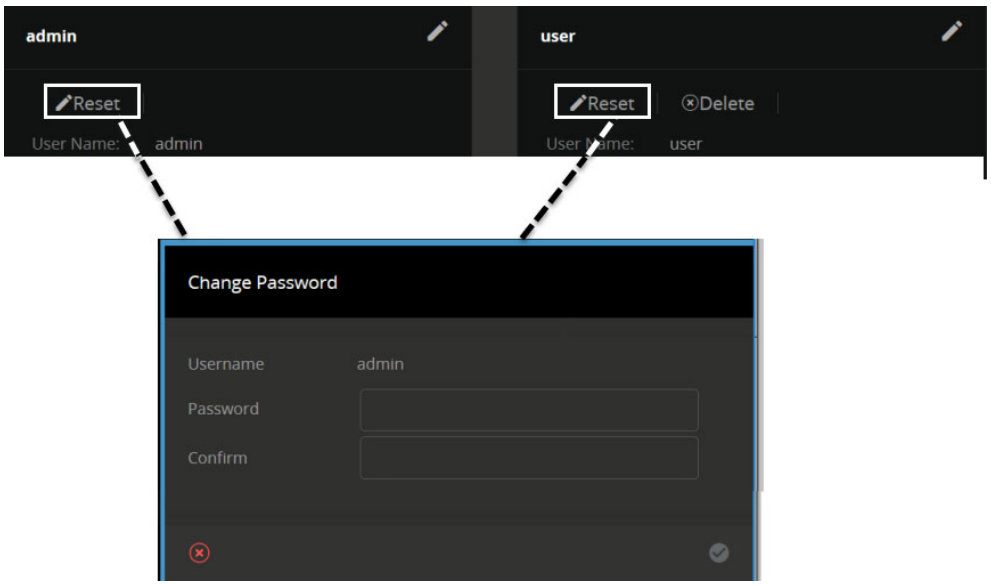
Field	Description
Username	Enter a user name (e.g., admin, admin-1, user, user-1)
Password	Assign a login password (minimum length of 8 characters and must contain at least 1 uppercase and 1 lowercase character).
Confirm	Confirm the assigned password
First Name	Enter user first name
Last Name	Enter user last name
Email	Enter users email address
Selected Roles	Role or roles to be assigned to the new user

Delete User

You can delete a user by checking the Delect User icon located on the user account window.

Reset Password

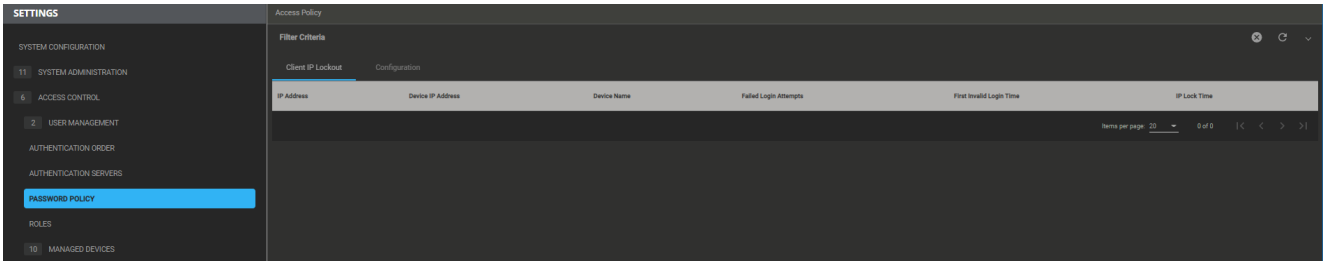
You can reset a users password by clicking on the Reset Password icon. Enter the revised password in the password text field. Click on the **Accept** check mark to save the change.



Access Policy

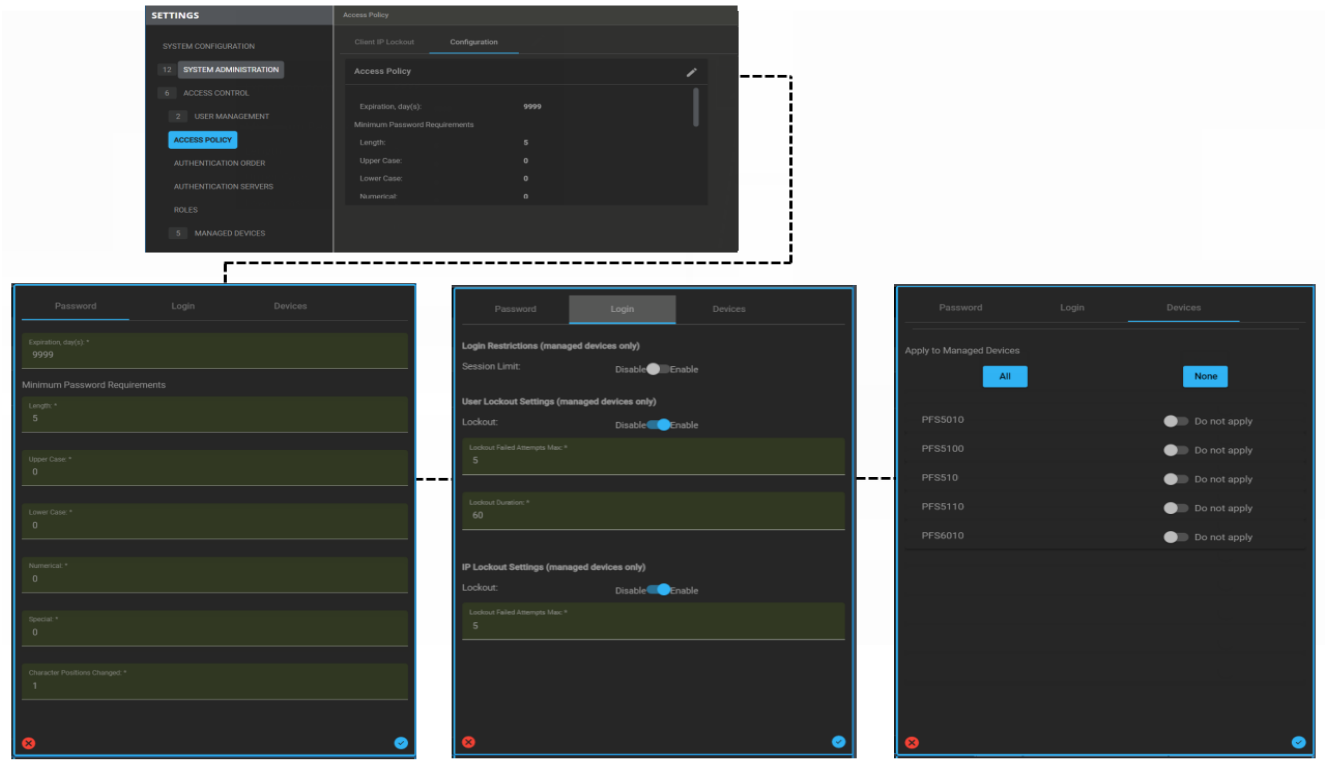
Client IP Lockout

The Client IP lockout tab lists the IP addresses that have been locked out due to excessive failed login attempts.



Configuration

To add a new Access Policy, select Settings > Access Control > Access Policy > Configuration. From the Access Policy tab, click on the Edit icon to access the Access Policy configuration screen. Specify the settings based on the users password requirements.

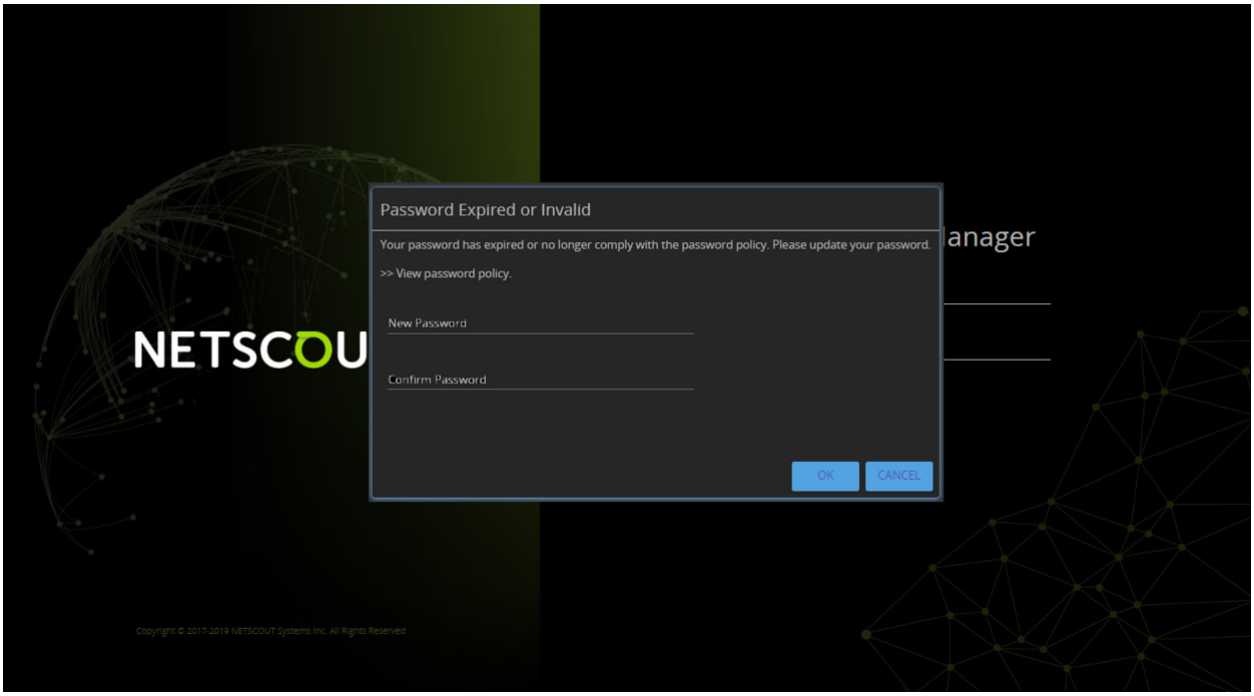


Settings	
Expiration, day(s)	Number of days in which the password will expire.
Minimum Password Requirements	
Length	Minimum password length.
Upper Case	Minimum number of upper case characters allowed.
Lower Case	Minimum number of lower case characters allowed.
Numerical	Minimum number of numerical characters allowed.
Special	Minimum number of special characters allowed.
Character Positions Changed	Minimum number of character positions changed within the new password which must be changed from the old password. Note that this setting does not require character changes, but character position changes. For example: • If the current password is "abc1234" and Positions Changed is set to 5, the new password "1234abc" is valid • If the current password is "1234abc" and Positions Changed is set to 2, the new password "1234abc56" is valid.
Login Restrictions (managed devices only)	
Session Limit	Enable / Disable the session limit.
User Lockout Settings (managed devices only)	
Lockout	Enable / Disable the lockout feature.
Lockout Failed Attempts Max.	Maximum number of lockout failed attempts.
Lockout Duration	Length of lockout duration (in minutes).

IP Lockout Settings (managed devices only)	
Lockout	Enable / Disable the lockout feature.
Lockout Failed Attempts Max.	Maximum number of lockout failed attempts.

The user will be prompted for a new password if the current password has expired or no longer complies with the password policy.

Note: Click on **View Password Policy** to view the current password policy.



Authentication Order

When a user logs in, PFS-FM and PFOS go through each configured remote authentication server. If the server that is next in line is reached but fails to authenticate, a response is returned to the client that authentication failed, and no attempt to try another server is done. If the server is not reachable, then the next server in line is tried. Authentication fails if none of the servers are reachable.

Selecting Authentication Order allows specifying which authentication types (TACACS, RADIUS, LDAP, and Local) are active and the order in which they are used.

To define the authentication order, select Access Control > Authentication Order. Click on the Edit icon to access the Authentication Order setup screen.

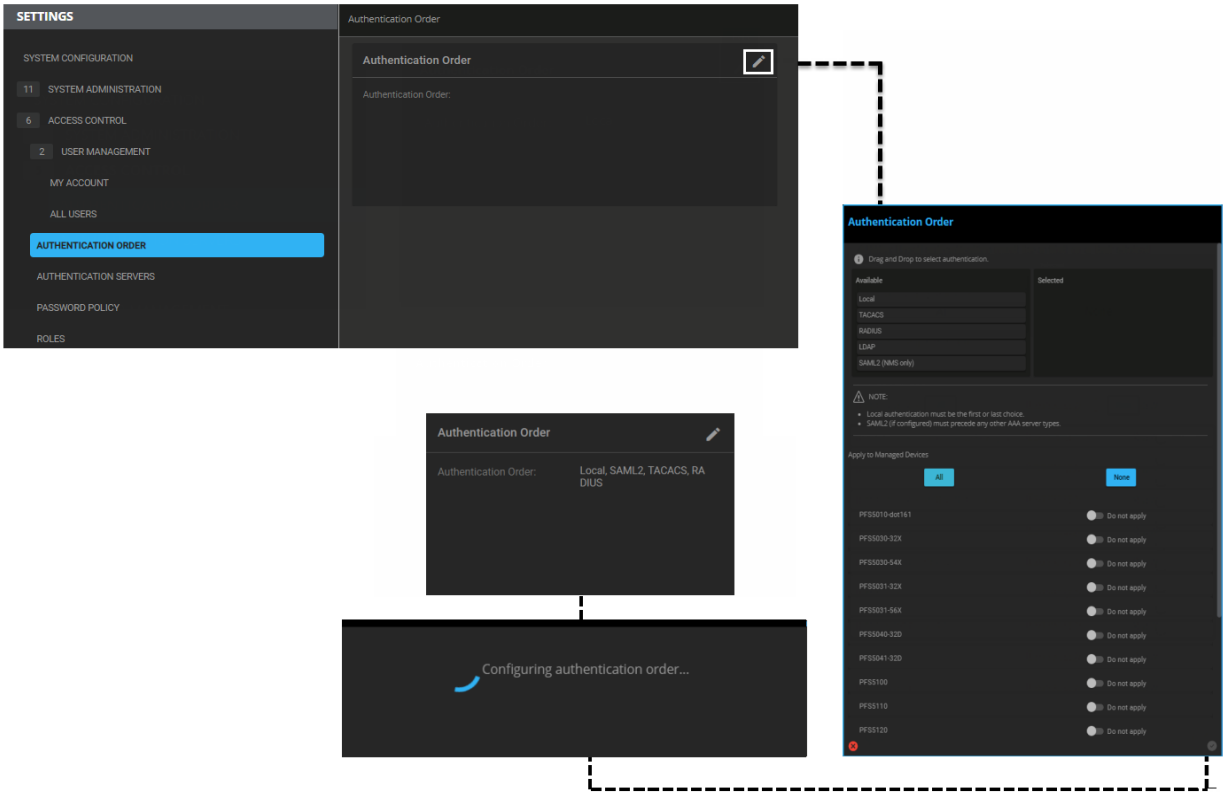
Select the authentication types [Local, TACACS, RADIUS, LDAP and SAML2(NMS only)] in the order in which they are used. The default is only Local authentication. In a list of multiple authentication types, Local must be last or no other authentication is attempted.

You can optionally assign the same authentication order to any managed devices connected to the central server. Selecting **All** sets the selected authentication order to all of the managed devices; or select one or more using the **Do Not Apply / Apply** slider controls for the individual devices. **None** unselects all managed devices.

Click the **Apply** checkmark to save the settings.

Note: When setting up external authentication for the first time, log in as administrator in one window to configure TACACS or RADIUS, then use a separate browser to test if the credentials are working.

As long as the administrator stays logged in on the first window, the user will not be locked out.



Configuring TACACS

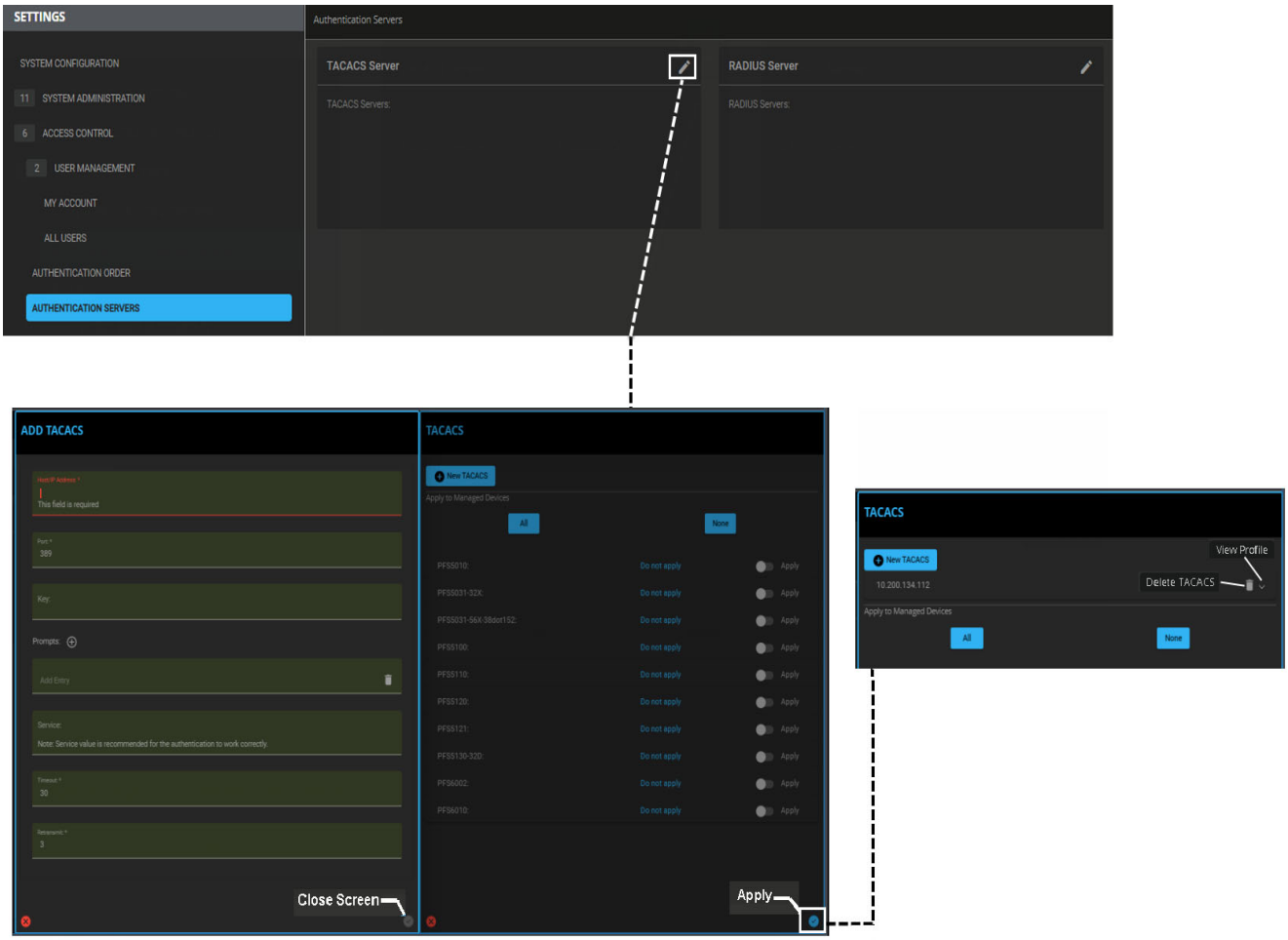
To add a new TACACS server, select Access Control > Authentication Servers. From the TACACS Server click on the Edit icon to access the TACACS setup screen. Click on the **Add More TACACS** (TACACS (+)) link to open an Add TACACS screen. Specify the settings based on the configuration of your TACACS server.

You can optionally assign the same TACACS settings to any managed devices connected to the central server. Selecting **All** sets the defined TACACS settings to all of the devices; or select one or more using the **Do Not Apply/Apply** slider controls for the individual devices. **None** unselects all managed devices.

When the new TACACS server is defined, click on the **Apply** checkmark in the Add TACACS screen to close the screen. The new TACACS server is added to the TACACS list.

Click the **Apply** checkmark in the TACACS screen to save the settings.

To view or edit a defined TACACS server settings, click on the **View Profile** icon next to the server name. To delete a TACACS server, click on the **Delete TACACS** icon next to the server name.



Settings	
Host / IP Address	IPv4/IPv6 address or a fully qualified domain name of the TACACS server.
Port	Port for access to the server (default 49).
Key	AES encrypted string to authenticate to the server.
Prompts	TACACS prompts parameter.
Service	TACACS service parameter. Note: Service value is recommended for the authentication to work correctly.
Timeout	Time after which requests to the server time out (default 30 seconds).
Retransmit	Number of times PFOS attempts to contact the TACACS server (default 3).

Note: The Service parameter needs to match what is defined in the TACACS server. It is recommended to use 'system' as the Service parameter, while configuring TACACS+ servers.

Configuring RADIUS

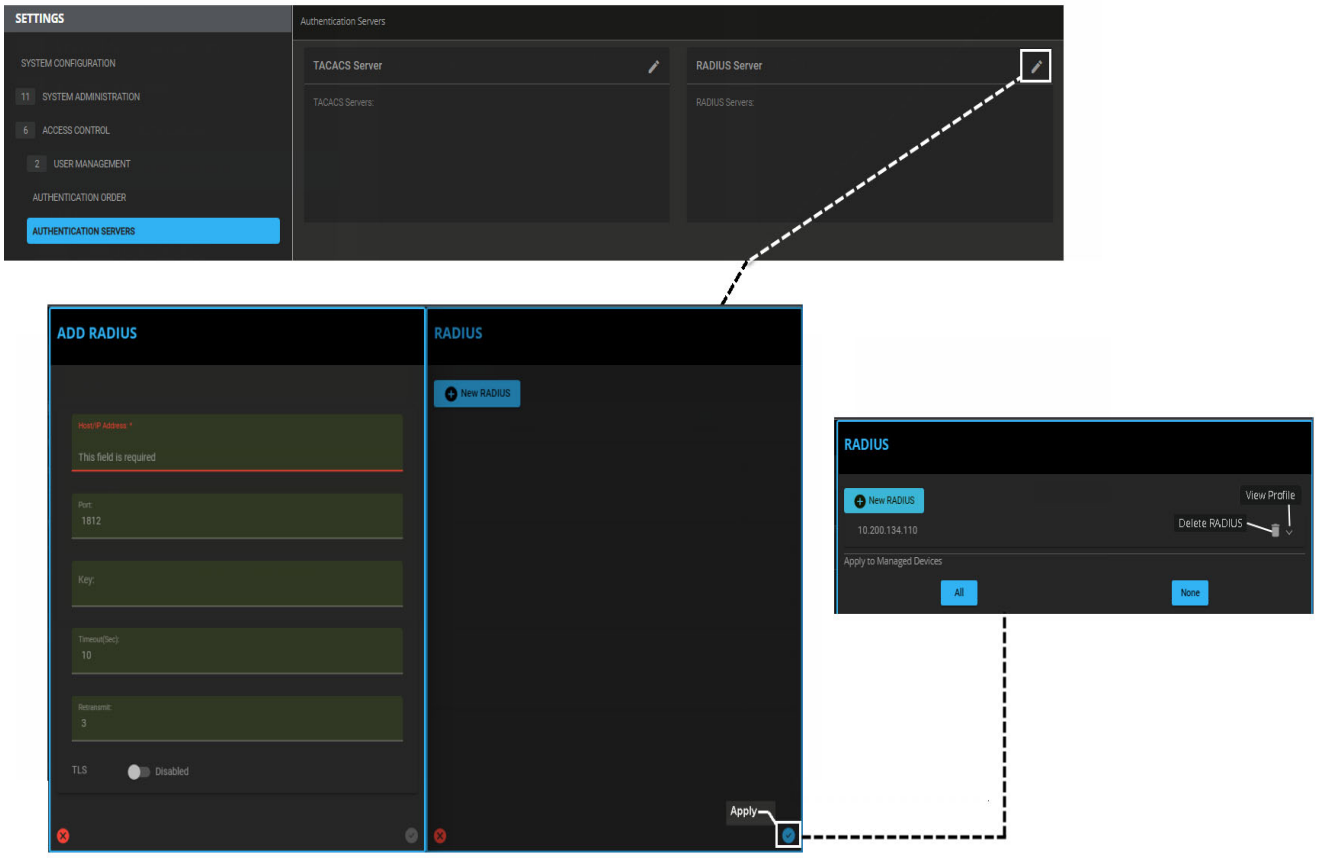
To add a new RADIUS server, select Access Control > Authentication Servers. From the RADIUS Server click on the Edit icon to access the RADIUS setup screen. Click on the **+ New RADIUS** link to open an Add RADIUS screen. Specify the settings based on the configuration of your RADIUS server.

You can optionally assign the same RADIUS settings to any managed devices connected to the central server. Selecting **All** sets the defined RADIUS settings to all of the devices; or select one or more using the **Do Not Apply/Apply** slider controls for the individual devices. **None** unselects all managed devices.

When the new RADIUS server is defined, click on the **Apply** checkmark in the Add RADIUS screen to close the screen. The new RADIUS server is added to the RADIUS list.

Click the **Apply** checkmark in the RADIUS screen to save the settings.

To view or edit a defined RADIUS server settings, click on the **View Profile** icon next to the server name. To delete a RADIUS server, click on the **Delete RADIUS** icon next to the server name.



Settings	
Host / IP Address	IPv4/IPv6 address or a fully qualified domain name of the RADIUS server.
Port	Port for access to the server (default 0).
Key	AES encrypted string to authenticate to the server.
Timeout	Time after which requests to the server time out (default 30 seconds).
Retransmit	Number of times PFOS attempts to contact the TACACS server (default 3).
TLS	If TLS is enabled for Radius (RADSEC), a Radius Certificate must be installed on the NMS. Also, ensure that the appropriate and corresponding signed CA certificate is updated and applied to Fabric Manager.

Configuring LDAP

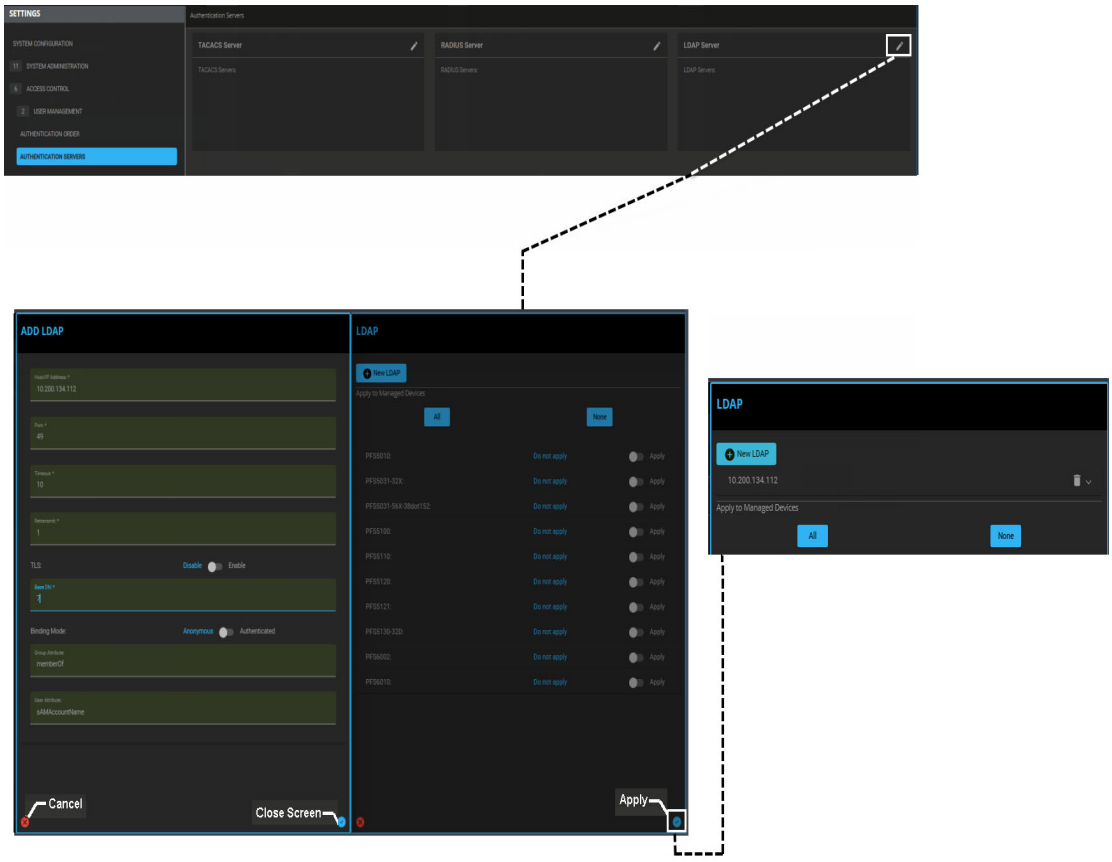
To add a new LDAP server, select Access Control > Authentication Servers. From the LDAP Server click on the Edit icon to access the LDAP setup screen. Click on the **Add More LDAP** (LDAP (+)) link to open an Add LDAP screen. Specify the settings based on the configuration of your LDAP server.

You can optionally assign the same LDAP settings to any managed devices connected to the central server. Selecting **All** sets the defined LDAP settings to all of the devices; or select one or more using the **Do Not Apply/Apply** slider controls for the individual devices. **None** unselects all managed devices.

When the new LDAP server is defined, click on the **Apply** checkmark in the Add LDAP screen to close the screen. The new LDAP server is added to the LDAP list.

Click the **Apply** checkmark in the LDAP screen to save the settings.

To view or edit a defined LDAP server settings, click on the **View Profile** icon next to the server name. To delete an LDAP server, click on the **Delete LDAP** icon next to the server name.



Settings	
Host / IP Address	IPv4/IPv6 address or a fully qualified domain name of the RADIUS server.
Port	Port for access to the server (default 389 for non_TLS/636 for TLS).
Timeout(Sec)	Time after which requests to the server time out (default 30 seconds).
Retransmit	Number of times PFOS attempts to contact the TACACS server (default 3).
TLS	Disable/Enabale TLS mode (When TLS is enabled, you can choose to validate against CA. To enable validation, enable authorize certificate.)
Base DN	Enter the distinguished name (DN) to search tokens on groups associated with that DN.

Binding Mode	Select Anonymous or Authenticated for LDAP binding. By default, Binding Mode is anonymous. If you enable authenticated mode, then the PFS-FM prompts you to enter a username and password for LDAP Binding. If binding mode is set to Authenticated, then Binding DN and Password are required. This is used when LDAP/AD mode requires a lookup user before query logged in user.
Group Attribute	Defines the group the user is a member of (typically set in LDAP AD as memberOf) and maps to one of the roles defined in the NMS (if no role mapping is found, it defaults to viewer role which has minimal rights - view only tokens).
User Attribute	Defines the lookup for the user when querying the server, for example: sAMAccountName or userPrincipalName. When logging in, the user is validated by using this lookup on the LDAP/AD server.

Upon configuring the above parameters, you can choose to apply the configuration to the NMS only or to the NMS and its managed devices. When managed devices are selected, the PFS-FM publishes the LDAP server configuration to the selected devices.

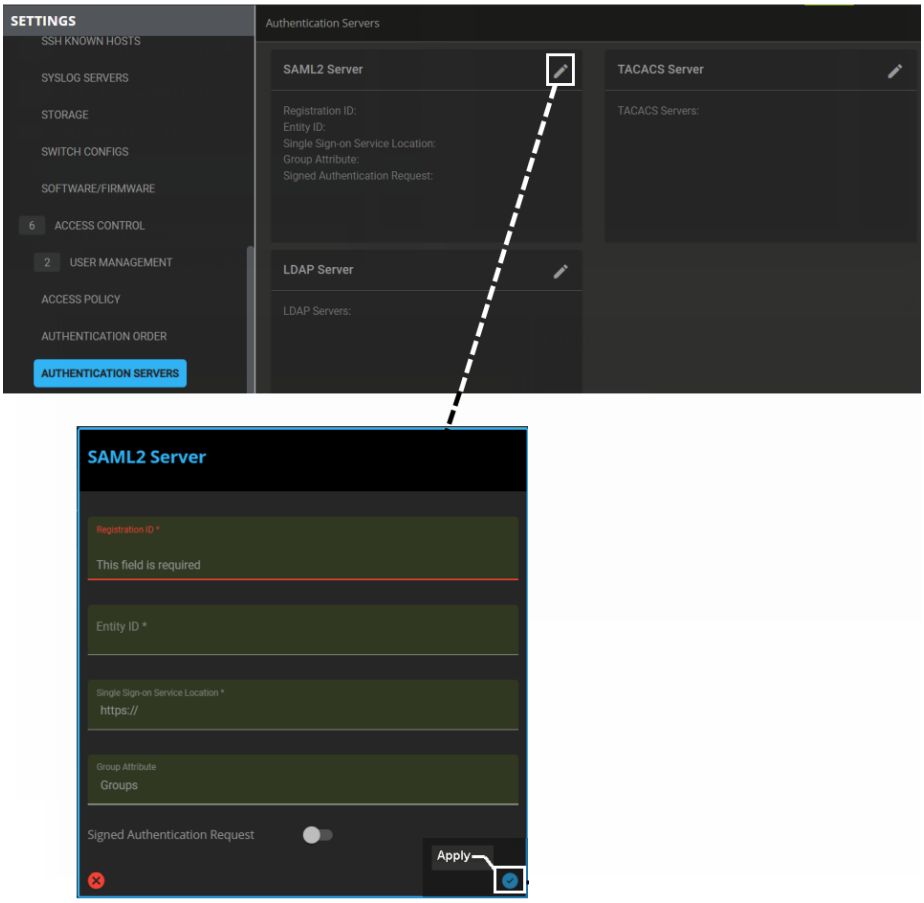
Like TACACS and RADIUS, a maximum of three LDAP Server instances can be configured and the order in which these instances are created is maintained for validation. The PFS-FM will authenticate against whichever instance is reached first.

Configuring SAML2 (NMS only)

To add a new SAML2 server, select Access Control > Authentication Servers. From the SAML2 Server click on the Edit icon to access the SAML2 setup screen. Specify the settings based on the configuration of your SAML2 server.

Note: Before adding a new SAML2 server, you must upload and apply an SAML certificate. Refer to Inventory Tab on page 7-17 to upload and apply the certificate.

When the new SAML2 server is defined, click the **Apply** checkmark to save the settings. The new SAML2 server is added to the SAML2 list.



Settings	
Registration ID	Unique RegistrationID assigned by your Identity Provider for your PFS-FM (as a Service Provider/App)
Entity ID	EntityID assigned by your Identity Provider
Single Sign-on Service Location	SSO Endpoint for the Identity Provider
Group Atttibute	Attribute maps to Role Mapping in Identity Provider (for example: the memberOf attribute maps to Group Names in Identity Provider)
Signed Authentication Request	Enable/Disable (always set to Disable)

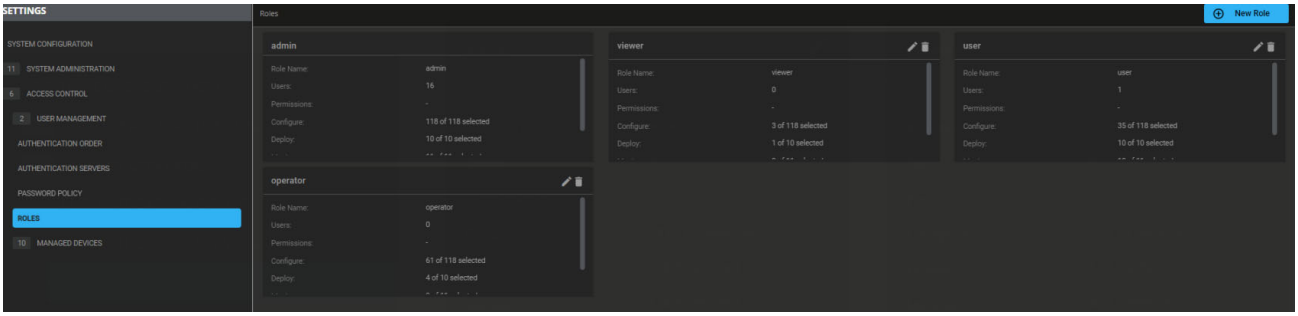
Roles Based Access Control (RBAC)

PFS Fabric Manager supports Role Based Access Control (RBAC). Roles define what a user can access, view, and change within the application. The roles are designed to represent specific job functions within the application. A user may have more than one role. Administrators can define custom roles, or change the permissions associated with default roles, except for the admin role.

PFS Fabric Manager comes with four default roles. With the exception of the admin role, each of these roles can be customized or deleted. The default roles and their permission are:

- admin – a super user with all access (permissions cannot be changed)

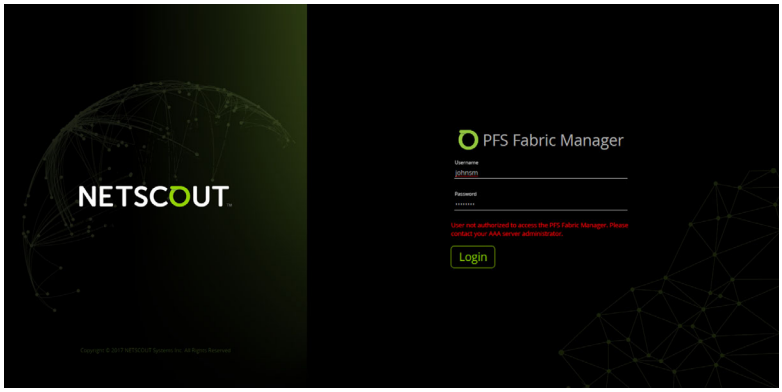
- user - a legacy role added in 4.3.1 to preserve 4.2.1 functionality, has most admin privileges (permissions can be removed or changed by an administrator)
- operator – a standard user role with a mix of read and write permissions
- viewer - a mostly read only role



Note:
Role Name:
- Role names support upper and lower case alphanumeric ASCII characters, limited special characters, and non-leading and non-trailing spaces.
- Role names used in remote authorization cannot be numerical-only (for example, a role named "1234" is not supported for remote authorization).
- Users not associated with a role will not have permission to read, write, or execute any commands after logging in. Local users without a role assigned to them only have permission to change their local password after login.

User Name:
- User names support upper and lower case alphanumeric ASCII characters and limited special characters. User names cannot contain spaces.
- The admin user cannot be deleted. The pfmadmin user (visible only in PFOS) must should not be deleted.

If a user is not assigned a role, then that user is denied access to the PFS-FM.



To assign roles via TACACS+ or RADIUS, users must be configured in the TACACS+ or RADIUS server with a Shell Attribute ACL of "groups=<rolename>" where <rolename> is the name of the role in PFS Fabric Manager. For example "groups=admin" will give the user "admin" permissions. If no group names match Fabric Manager role names, then the user will be logged in with "viewer" permissions.

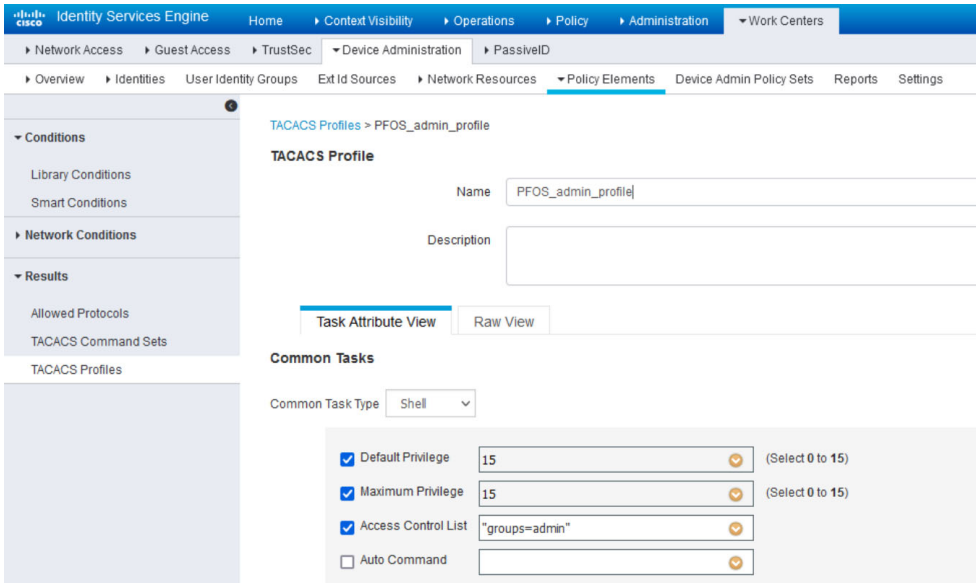
To assign roles via LDAP, the user is assigned a role if a Fabric Manager role matches the name of a group of which the user is a member. See the Group Attribute setting for details on how LDAP group membership is determined.

If no roles are provided by the AAA server (or the groups provided do not map to roles configured in PFS Fabric Manager) then the user will not be allowed to log in to PFS Fabric Manager (a notice of insufficient access will be given).

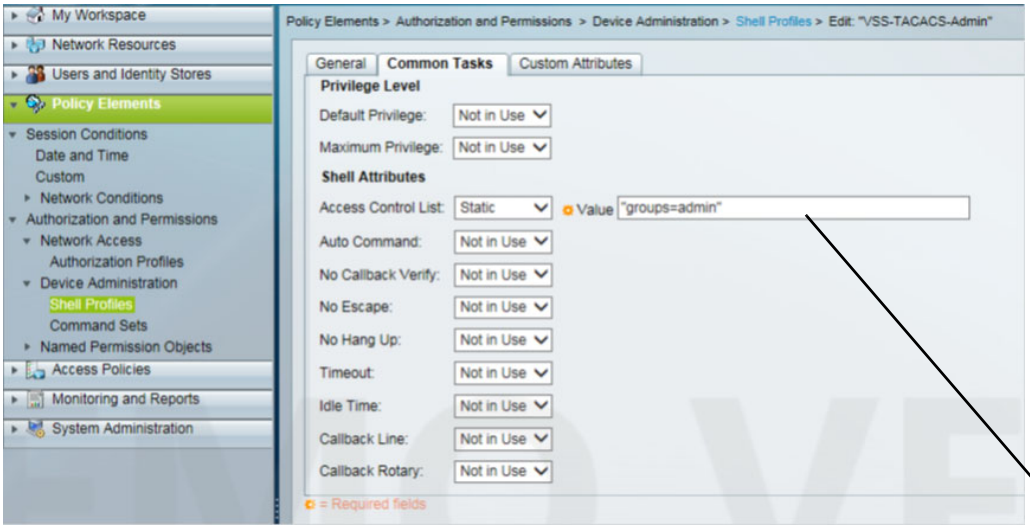
Sample Configuration for Authorization

The following example show how to configure a Shell Attribute ACL for PFS Manager authorization in a few 3rd party AAA products. These examples are provided for explanatory purposes only; these examples do not denote support of, or recommendation for, these 3rd party products.

The following example shows a Cisco ISE Server configuration of a Shell Attribute ACL.



The following example shows a Cisco ACS Server configuration of a Shell Attribute ACL.



This example shows the “admin” role being set. Change to “user” for the user role.

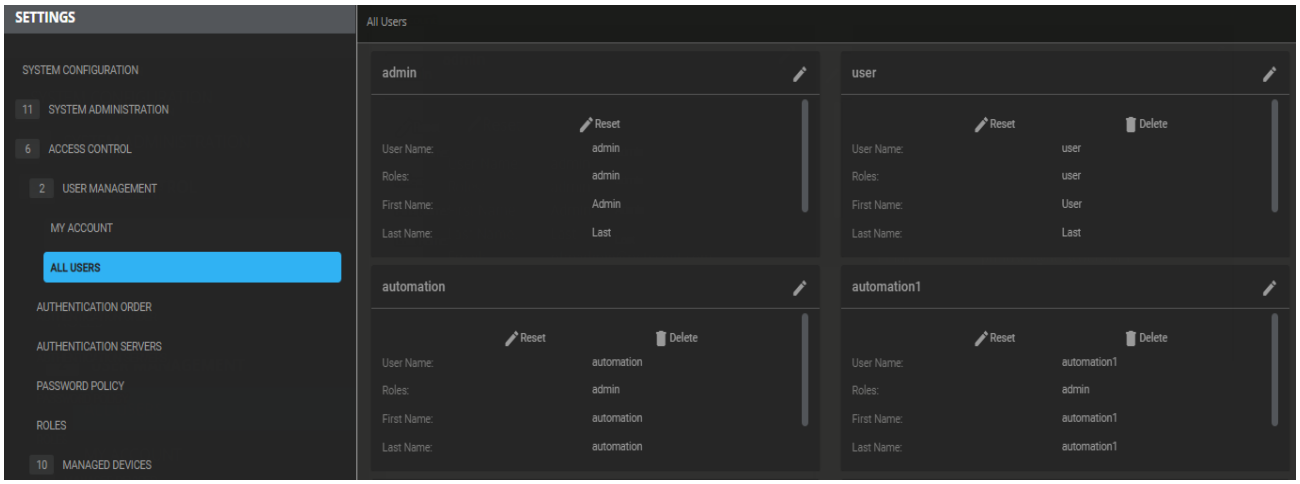
The following example shows a “tac_plus” Server configuration of a Shell Attribute ACL.

```
group = myadmin {
        default service = permit
        service = shell {
                default command = permit
                default attribute = permit
                set priv-lvl = 15
                set acl = "groups=admin"
        }
}
group = user {
        default service = permit
        service = shell {
                default command = permit
                default attribute = permit
                set priv-lvl = 1
                set acl = "groups=user"
        }
}
```

Setting Authorization for the Admin Role

Setting Authorization for the User Role

My Account

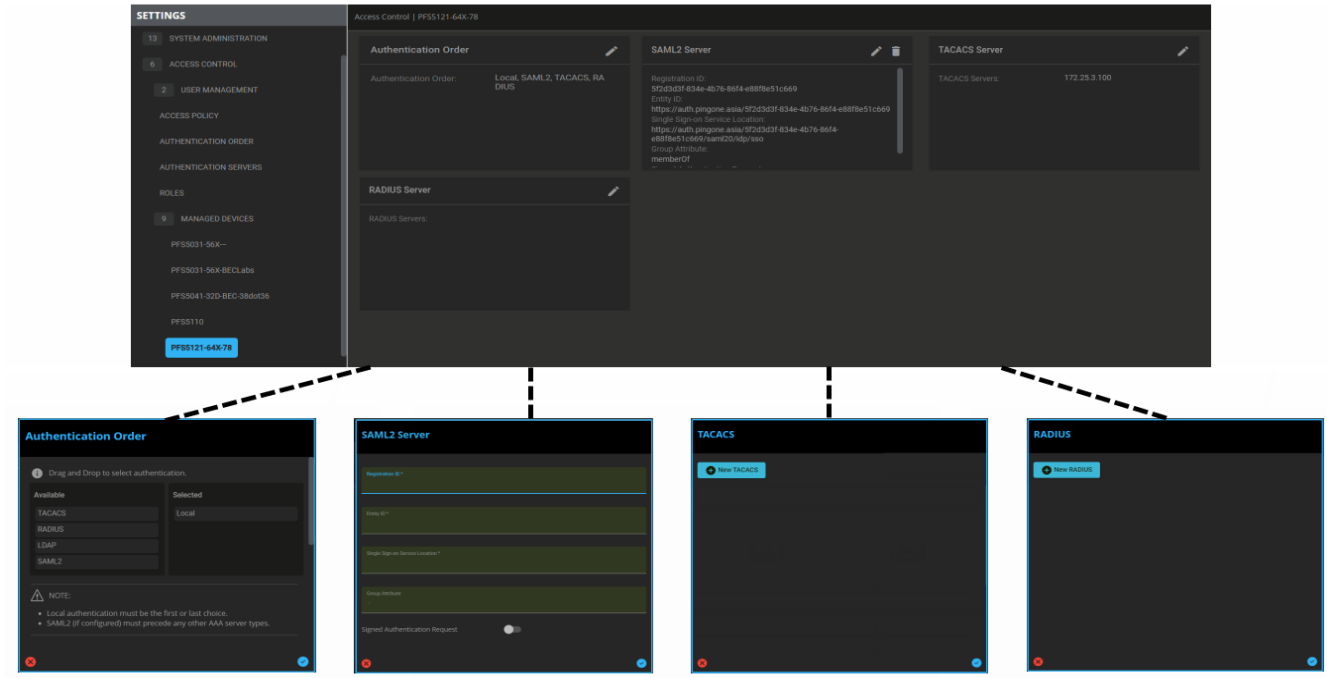


Managed Devices

The Managed Devices function is used to customize access controls for individual devices. It is also used when the server settings required on a device do not already exist or are not configured as entries in PFS Fabric Manager.

Select Access Control > Managed Devices, and click on the device to configure. You have access to the following:

- Authentication Order - Refer to Authentication Order on page 7-51
- Users - All Users on page 7-47
- TACACS Server - Refer to Configuring TACACS on page 7-52
- RADIUS Server - Refer to Configuring RADIUS on page 7-54
- LDAP Server - Refer to Configuring LDAP on page 7-55
- Password Policy - Refer to Roles Based Access Control (RBAC) on page 7-57
- Roles - Roles Based Access Control (RBAC) on page 7-57



Note: Apply to Managed Devices section is not available for managed devices.

A user cannot push the same settings to other devices, because these settings are for a specific / single device.

Appendix A
Installing PFS Fabric Manager Central Server (Software-Only Version)

This appendix details the procedures for installing the software-only version of PFS Fabric Manager NMS on a user-supplied central server or virtual machine (VM).

The software-only version of PFS Fabric Manager is distributed as an ISO file downloaded from My.NETSCOUT.com; this ISO can be installed on a VM or on a physical server.

Important:
Customers who purchased the appliance from NETSCOUT should only follow these instructions when performing an Operating System upgrade, as PFS Fabric Manager is already installed on those appliance devices, and the instructions below will remove your existing installation.

Server Requirements

PFS Fabric Manager can be installed as a central server on any user-supplied server or VM meeting at least the minimum of the following requirements.

Resource	Minimum	Recommended
RAM	16 GB	32 GB
Disk Space	1 TB (500 GB is acceptable in VMs)	2 TB
CPU	6 cores or vCPUs@ 2.1 GHz	8 cores or vCPUs @ 2.1 GHz
Network Cards	1 Gbps Ethernet	1 Gbps Ethernet

Note: System disk space should be in a single logical disk. Use of RAID for redundancy is recommended in physical servers.

Note: PFS Fabric Manager supports installation in virtual machines running in the VMware ESXi hypervisor. Other hypervisors or virtual environments are not supported.

Server Operating System

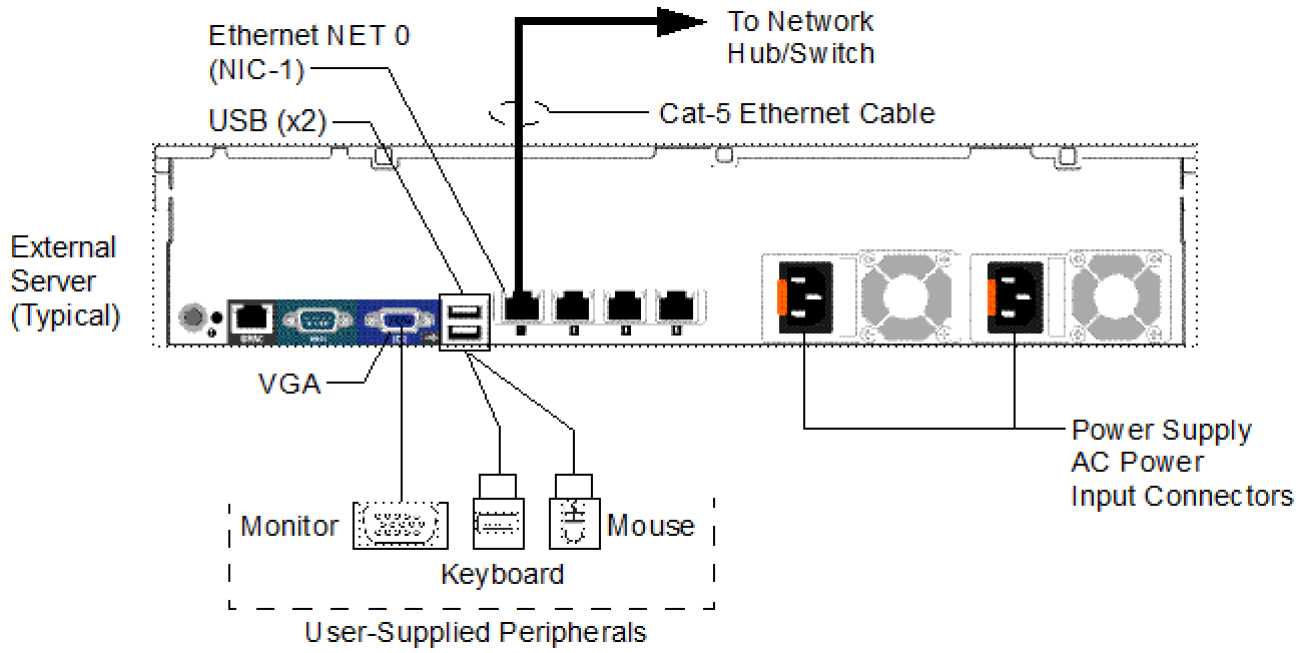
The Oracle Linux 9 operating system is installed on the server as part of the ISO re-imaging procedure.

Important:
Please be aware that any existing operating system on the server hard drive will be removed and replaced with the Oracle Linux 9 operating system.

Attaching Cables to the Physical Server

Note: Before starting the installation on a physical server, the server must be physically wired. Skip this section if installing on a VM.

1. Connect the following user-supplied peripherals to the server:
   - Keyboard: USB connector to a USB port on the server.
   - Mouse: USB connector to a USB port on the server.
   - Monitor: DB-15 video connector to the VGA port on the server.
2. Connect one end of a Category 5 Ethernet cable to the Net 0 Ethernet connector on the server. Connect the other end of the cable to a port on the network hub/switch.
3. Connect the receptacle ends of the server power cords to the server AC power input connectors. Connect the plug end of the power cords to UPS power receptacles.
4. Connect the receptacle end of the monitor power cord to the monitor's AC power input connector. Connect the plug end of the power cord to a UPS power receptacle.



Installing PFS Fabric Manager Software

Please follow these steps to install PFS Fabric Manager.

1. Download the PFS Fabric Manager Software-Only version of the product: ***OracleLinux-9.3_pfm-nmso8o9-<version>.iso*** from the **PFS Fabric Manager** or **PFS Fabric Manager Software-Only Version** download page on My.NETSCOUT to your local PC.

   Note:
   The version name of the file changes per release.

   This is a special file, used for first time installs; it is NOT to be used for subsequent upgrades.

2. Prepare the ISO for use.

a To install on a physical server: see Using Virtual Media for Software Updates on page B-11.

b To install on a VM: upload the ISO to the hypervisor so it can be used as the boot device of a new VM.

3 Boot from the ISO image in order to begin re-imaging/installing the required Linux platform.

a On a physical server: see Using Virtual Media for Software Updates on page B-11.

b On a VM: mount the ISO in the VM's DVD drive and boot the VM.

Important:
Any existing operating system on the server or VM hard drive will be removed and replaced with the Oracle Linux operating system.

4 Reboot the server after the re-imaging is complete.

5 Temporarily disconnect the server or VM from the network by removing the network cable (refer to Attaching Cables to the Physical Server, Step 2) or disconnecting the vNIC.
Reconnect the server to the PFS system network after the IP address is set.

6 Connect to the server or VM's console, using a keyboard and monitor or the hypervisor's console facility, and login as:
username: **root**
password: **r00tme**

7 From the root directory type **`cd /opt/install`**
then type **`./nGApplianceConfig.plx`** and follow the instructions in the script to configure your PFS Fabric Manager server:

At the prompt to configure ETH 0, enter **y** and press **Enter** to continue. Follow the prompts to enter the following information for ETH 0:

- IP Addresses
- Netmask
- Default gateway
- Hostname
- Domain name
- Name server(s)
- NTP Time Server(s)
- Time Zone

8 When your settings are displayed, verify that the settings are correct.

- If your settings are correct, enter **y** and press **Enter** to continue.
- To update any information, enter **n** and press **Enter**.
  You can now reenter your settings.

9 When prompted to reboot, enter **y** and press **Enter**.

10 After the server reboots, reconnect the network cable or vNIC (disconnected in step 5) and then SSH to the server's new IP address using port number 22 (default) and re-login as:
username: **root**
password: **r00tme**

11 Type the following:
`cd /opt/install`
To install PFS Fabric Manager, type: **`./hzinstall.plx`**

12 When prompted to reboot, enter **y** and press **Enter**.

At this point, you can now access PFS Fabric Manager from your server.

13 Using a supported web browser, enter the assigned IP address of the nGenius PFS Fabric Manager Server (e.g., *https://nnn.nn.nn.nnn).*

14 From the PFS Fabric Manager login screen, enter your assigned user ID and password or use the default (admin / admin) and click Login.

Note: Once PFS Fabric Manager is installed on your own server or VM for the first time, subsequent upgrades to the software follow in the same manner as if you have purchased the appliance directly from NETSCOUT. The software upgrade instructions should then be used when upgrading your PFS Fabric Manager software.

Important: If you have any issues installing PFS Fabric Manager, contact NETSCOUT Customer Care (refer to Contacting NETSCOUT Customer Care on page 1-1).

Upgrading the Operating System on the PFS Fabric Manager NMS (CentOS 6/8 to Oracle Linux 9)

Please follow these steps to upgrade the Operating System on the PFS Fabric Manager NMS.

1. Upgrade the NMS to 6.5.0, refer to *Upgrading PFS Fabric Manager (NMS) on a Central Server* in the nGenius® PFS Fabric Manager Software 6.5.0 Release Notes.
2. Verify that the NMS and managed switches are Active.
3. Take a backup of the NMS (refer to Backup/Restore on page 7-7 for more information).
4. Using the PFS-FM installation disk/ISO, install Oracle Linux 9 on the NMS following the directions in Installing PFS Fabric Manager Software on page A-2.
5. Reboot the system.

Note: The managed switches will not be connected to the NMS before the restore operation is completed.

6. Restore the backup taken in step 4 (refer to Backup/Restore on page 7-7 for more information).
7. Verify that the system is up/running with all Topologies, Port Config, Features and Device Config from the earlier release.

Appendix B
Configuring and Troubleshooting the Server Remotely

This appendix provides a summary of common tasks you can perform using the Dell Integrated Remote Access Controller for remote administration and troubleshooting of PFS Fabric Manager servers. The version of iDRAC varies based on the server model, as indicated below. This document provides an overview of the general functionality available from the iDRAC service.

For complete details on the controller's features and functions, refer to the Dell Remote Access Controller Documentation on the Dell website.

- Dell R760 (iDRAC9)
  https://www.dell.com/support/article/us/en/19/sln311300/idrac9-home
- Dell R730 (iDRAC8)
  https://www.dell.com/support/article/us/en/19/sln310710/idrac8-home

Using the Dell™ Remote Access Controller

The PFS Fabric Manager Server Hardware includes the Integrated Dell Remote Access Controller (iDRAC). The iDRAC is a systems management hardware and software solution for NETSCOUT hardware based on the Dell platform. The iDRAC provides remote management capabilities, crashed system recovery, and power control functions. By connecting the iDRAC's onboard Ethernet port to an out-of-band management network, you can then connect to these servers from a remote computer using the built-in web-based user interface (UI).

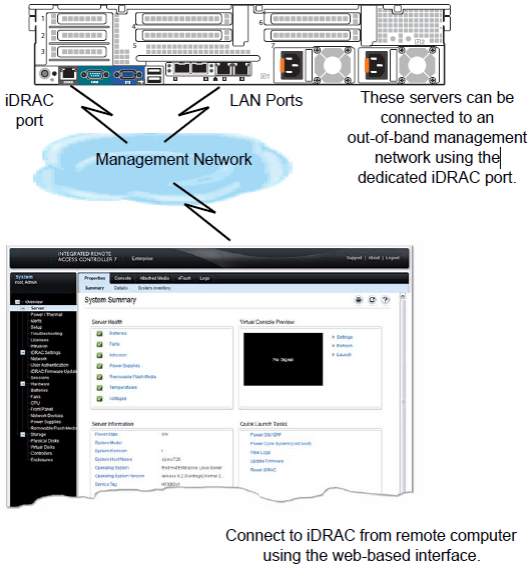


Figure B-1 Using iDRAC for Remote Management

iDRAC Requirements

This section provides details on supported browser configurations, required ports, and supported physical connections for iDRAC usage. Details are provided in the following sections.

- NETSCOUT recommends that you set your monitor resolution to 1280x1024 pixels or higher.
- Browsers must be configured to allow pop-ups in order to launch the Virtual Console.
- The iDRAC connection does not use a certificate so you will be prompted each time to approve the connection. To bypass these prompts:
  - For FireFox users, select the option I Understand the Risks and then select the button to Add Exception for that IP Address. In the dialog that displays, ensure the checkbox is enabled to Permanently store this exception, then click Confirm Security Exception.
  - For Internet Explorer users, click the link to Continue to this website. To permanently add the iDRAC address as a trusted site, perform the following steps:
    - **a** Go to Internet Explorer Options or Settings and select Tools > Internet Options >Security >Trusted sites > Sites.
    - **b** Enter the iDRAC IP address in the Add this website to the zone field.
    - **c** Click Add, click OK, and then click Close.
    - **d** Click OK and then refresh your browser.

Additional Notes for Internet Explorer Users

- Browsers must have SSL 3.0 enabled.
- Ensure that the browser is enabled to download encrypted content:
  - **a** Go to Internet Explorer Options or Settings and select Tools > Internet Options>Advanced.
  - **b** Scroll to Security and uncheck this option:
    Do not save encrypted pages to disk

- If you prefer not to use the Java plugin with Internet Explorer and instead use the (Native) ActiveX plug-in, ensure that you have added the iDRAC IP or hostname to the Trusted Sites list. Refer to "Configuring Supported Web Browsers" in the iDRAC User's Guide for a detailed list of settings to modify in Internet Explorer's Internet Options >Security tab:

  iDRAC8 User's Guide
- The 64-bit ActiveX plug-in is not supported to launch the Virtual Console session.

Firefox Users – Preventing Multiple Plugin Installations

By default, Firefox installs a separate version of the Virtual Console plugin for each separate iDRAC you visit, even though the plugin is identical for each site. You can avoid this "whitelist" feature and prevent multiple plugin installations by performing the following steps:

1. Open a Firefox Web browser window.
2. In the address field, enter **about:config** and press **Enter**.
3. In the **Preference Name** column, locate and double-click **xpinstall.whitelist.required**.

   The values for **Preference Name**, **Status**, **Type**, and **Value** change to bold text. The **Status** value changes to user set and the **Value** changes to **false**.
4. In the **Preferences Name** column, locate **xpinstall.enabled**.

   Make sure that **Value** is true. If not, double-click **xpinstall.enabled** to set **Value** to **true**.

Network Requirements for Using iDRAC

Use the information in this section to understand the environmental conditions required to use the iDRAC interface.

Physical Connections

When making physical connections for the dedicated iDRAC port, keep in mind the following:

- The iDRAC port speed is 10/100/1000 Mbps.
- The iDRAC port has a default IP address of 192.168.0.120.
- You can directly connect the iDRAC port to the Ethernet port of a PC using an Ethernet crossover cable.
- DHCP is supported, but not recommended.

If you directly connect the iDRAC port to a Cisco switch, be sure to enable Spanning Tree PortFast and disable the negotiation of the Dynamic Trunking Protocol on the Cisco switch port to which you connect the iDRAC port.

Required Network Listener Ports

The iDRAC interface uses specific network ports that you may need to open in your firewall for successful communications. Table B–1 lists the ports used by the iDRAC that listen for a server connection. Table B–2 lists the ports that the iDRAC uses as a client.

Note: Ports marked with an asterisk (*) are configurable on the iDRAC.

Table B–1 iDRAC Server Connection Ports

Port Number	Function
22*	Secure Shell (SSH)
23*	Telnet
80*	HTTP
443*	HTTPS
623*	RMCP/RMCP+
5900*	Virtual Console keyboard/mouse, Virtual Media Service, Virtual Media Secure Service, and Virtual Console video

Table B–2 iDRAC Client Ports

Port Number	Function
25	SMTP
53	DNS
68	DHCP-assigned IP address
69	TFTP
162	SNMP trap
636	LDAPS
3269	LDAPS for global catalog (GC)

User Account Requirements

For the activities described in this document, you will need login credentials for an iDRAC account with Administrator or Operator group privileges. The root user has Administrator privileges by default. The default iDRAC user group privileges are:

- Administrator —Login, Configure, Configure Users, Logs, System Control, Access Virtual Console, Access Virtual Media, System Operations, and Debug
- Operator —Login, Configure, System Control, Access Virtual Console, Access Virtual Media, System Operations, and Debug
- Read Only —Login
- None —No assigned permissions

User accounts are accessible from the following location:

- In the Web UI Overview > iDRAC Settings > User Authentication > Local Users tab and in BIOS under iDRAC Settings > User Configuration. For more information refer to the iDRAC pages on Dell’s website (noted at the beginning of this chapter).

iDRAC Settings in System BIOS

You can use BIOS to verify some important settings that can be changed if the iDRAC firmware is reset. Under most circumstances, you should use the iDRAC web interface. The default iDRAC password can be found on the pull-out Information Tag, located on the front of the chassis (near the server asset tag). The procedure below includes steps to change the password in BIOS and to configure the IP address of the iDRAC port.

- Accessing iDRAC Settings in BIOS
- Changing the iDRAC Password
- Configuring iDRAC Network Settings
- Restoring iDRAC Defaults

Important: NETSCOUT recommends that you not use the web-based iDRAC interface to reconfigure the iDRAC IP settings. Doing so runs the risk of losing connectivity during the IP reconfiguration, resulting in an unreachable system. Instead, use system BIOS in the event of an operating system failure.

Accessing iDRAC Settings in BIOS

You can use the Virtual Console to access BIOS when you are monitoring a system. However, there are cases where you may lose connectivity if you are connected remotely. Use these instructions to log in directly to the appliance.

1. Establish a direct physical connection to the PFS Fabric Manager Server Hardware, either using a keyboard and monitor or a laptop connected to the serial port.
2. Turn on or restart the server hardware.
3. Press **F2** during the boot sequence to enter the system BIOS. If the operating system begins to load before you press **F2**, wait for the system to boot completely before restarting the system and trying again. When BIOS has booted, the System Setup Main Menu displays with options for System BIOS, iDRAC Settings, and Device Settings.

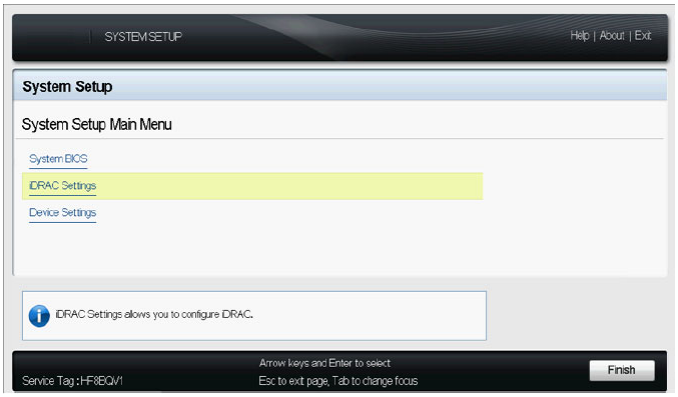


Figure B-2 System Setup Main Menu

4. Within this utility, use the following for navigation and selection:
   - **Arrow keys**—move up and down within a menu or list; left or right to toggle an alternative selection
   - E**nter key**—apply a typed or selected value; display options in a selector list (use arrow keys to navigate to a desired selection; **Enter** again to pick the entry)
   - **Tab key**—navigate between the upper banner of the screen (Help/About/Exit), the editable area of the screen, and the lower banner (Exit/Back/Finish); navigate between options for Yes/No in a dialogue
   - **Space bar**—display the options in a selector list (use the arrow keys to navigate the list and the Enter key to pick an entry)

5 Use arrow keys to navigate to the **iDRAC Settings** link and press **Enter**. The iDRAC Settings pane displays.

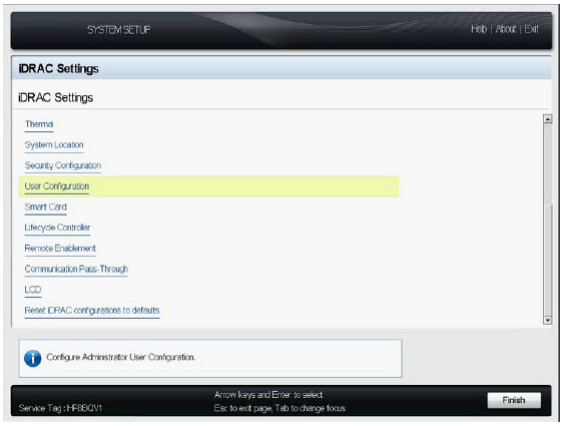


Figure B-3 iDRAC BIOS Level Configuration

Changing the iDRAC Password

If you cannot connect with your password, refer to Restoring iDRAC Defaults and then reconfigure iDRAC Settings. Otherwise, if you know your password and want to change it:

1 If you have not already, perform the steps under Accessing iDRAC Settings in BIOS on page 3-5.

2 Navigate to **User Configuration** and press **Enter** to open display the settings for the default iDRAC user.

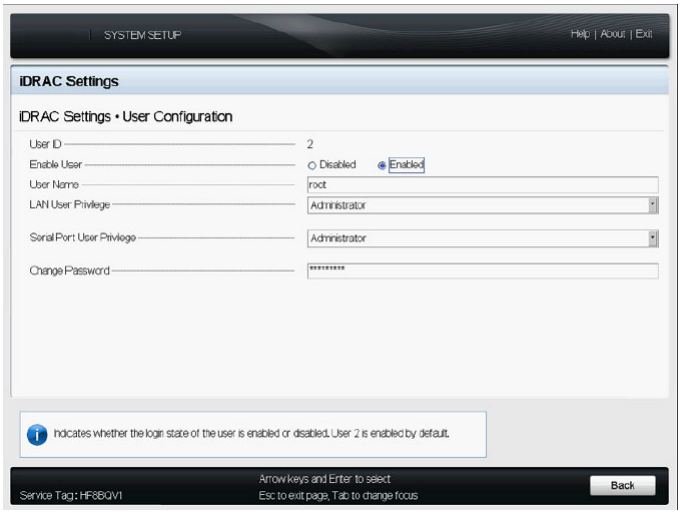


Figure B-4 Change the iDRAC Password

3 Use the down arrow key to select the Change password field.

4 Type the new password and press **Enter**.

5 When prompted to re-enter the password, type it again and press **Enter**, or tab to the **OK** button and press **Enter**.

6 Press **ESC** to exit the User Configuration screen. Your changes are not applied until you completely exit BIOS. The iDRAC Setting screen is displayed.

7 If you have no other changes, press **ESC** again to exit iDRAC Settings. A dialog box prompts you to confirm that you want to save your changes. Tab to and select **Yes**.

Note: If you press **ESC** on this dialog box, the effect is the same as a No response—the previous settings are restored.) A dialogue displays a confirmation that your settings are saved if you selected Yes or restored if you pressed **ESC** or selected **No**.

8 From the System Setup Menu you are now ready to exit the utility and apply your saved values to the system. Press **ESC** or tab to and select **Finish**. A dialogue displays asking you to confirm that you want to exit BIOS.

9 Select **Yes**.

10 The system automatically reboots with your new settings in place.

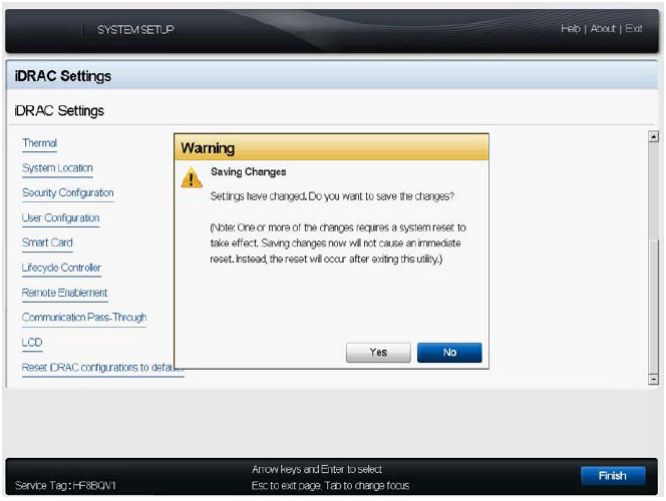


Figure B-5 iDRAC Confirm Changes Dialogue

Configuring iDRAC Network Settings

Use the procedure in this section to configure the iDRAC's 10/100/1000BASE-T port.

1 Access DRAC Settings in BIOS.

2 Navigate to **Network** and press **Enter**.

3 Use arrow keys to navigate to **Network**, then press **Enter**. The menu that displays allows you to configure the network parameters. Use arrow and tab keys to navigate the list of configuration options. Of the several options you are provided for customization, be sure to review and adjust the following:

- **Enable NIC**—Ensure the NIC for the iDRAC port is **Enabled**.
- **NIC Selection**—If this is set to any of the LOM options, change it to **Dedicated**.
- **Auto Negotiation**—Ideally, leave this On so that the port speed is ensured to match the connected network.
- **Register DRAC on DNS**—optional.
- **DNS DRAC Name**—optional; if not set, the users must know the IP address to access the web DRAC UI.
- **Auto Config Domain Name**—optional.
- **Static DNS Domain Name**—if auto config is not set, then type the domain name here
- **IPv4 Settings**—If the appliance resides in an IPv4 environment, set the following:
  - Enable IPv4—Enabled (default)
  - Enable DHCP—Disabled (default). NETSCOUT recommends using a static address, not DHCP.
  - Static IP Address—192.168.0.120 (default)
  - Static Gateway: Default is 0.0.0.0 (default)
  - Static Subnet Mask—255.255.255.0
  - Static Preferred DNS Server—0.0.0.0 (default)
  - Static Alternate DNS Server—0.0.0.0 (default)
- **IPv6 Settings**—If appropriate for your environment, you can also configure IPv6:
  - Enable IPv6—Disabled (default)
  - Enable Auto-configuration—Disabled (default). NETSCOUT recommends using a static address, not DHCP.
  - Static IP Address 1— :: (default)
  - Static Prefix Length— 1
  - Static Gateway— :: (default)
- **IPMI Settings:**
  - Enable IPMI Over LAN: Enabled (default)
  - Channel Privilege Level Limit: Administrator (default)
  - Encryption Key: All zeros (default)
- **VLAN Settings:**
  - Enable VLAN ID: Disabled (default). If this option is enabled, only traffic matching the VLAN ID specified in the VLAN ID field below is accepted

4 Press **Esc** to exit the Network menu and return to the main BIOS menu for iDRAC Settings.

5 (Optional) Set the default behavior for virtual media connections here rather than using the web iDRAC UI.

a Tab to the **Media and USB Port Settings** entry and press **Enter**.

b Tab to the desired setting and modify as desired:

- Detach—Virtual media are not allowed to be mapped to the server.
- Attach—Virtual media can be attached to the server but are not automatically mapped
- Auto attach (default)—Virtual media are automatically attached to the server and mapped as virtual drives.

c Press Esc to return to the iDRAC BIOS menu.

6 Press **Esc** when you are finished configuring iDRAC Settings. The BIOS menu displays.

7 If you have no other changes, press **Esc** again. A dialog displays, asking you to confirm that you want to exit BIOS.

8 Select **Yes**. The system automatically reboots with your new settings in place.

Restoring iDRAC Defaults

If you forget your iDRAC password, or some other condition necessitates a BIOS reset, you can revert the iDRAC firmware to factory default settings.

1 Establish a direct physical connection to the server hardware either using a keyboard and monitor or a laptop connected to the serial port.

2 Turn on or restart the server hardware.

3 Press **F2** to boot the system into BIOS. If the operating system begins to load before you press **F2**, wait for the system to boot completely before restarting the system and trying again. When BIOS has booted, the System Setup Main Menu displays with options for System BIOS, iDRAC Settings, and Device Settings.

4 Use arrow keys to navigate to the **iDRAC Settings** link and press **Enter**.

5 Use arrow keys to scroll through the iDRAC Settings list of options to the **Reset iDRAC configurations to defaults**.

6 Press **Enter** to select the item. The following warning message is displayed:

Resetting to factory defaults restores from non-volatile storage

settings. Do you want to continue?

< NO >

< YES >

7 Navigate to the Yes option and press **Enter**.

Note: This action will reset the iDRAC password to the Dell default: “calvin.” It will also reset any configuration changes you had previously made, such as setting IPMI over LAN and the IP Address, Subnet Mask, and Gateway.

Connecting to the iDRAC Interface

After you configure the iDRAC settings, you can remotely access the server hardware using the web-based interface.

1 Open a supported web browser.

2 In the **Address** field, type **https://*<iDRAC IP Address>*** and press **Enter**.

The iDRAC Login screen displays.

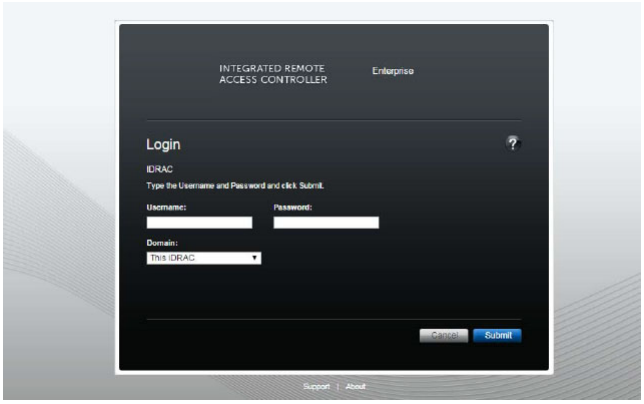


Figure B-6 iDRAC Login Screen

3 Enter a valid User name and password.

The iDRAC default User name is “root”. The default password depends on the hardware generation:

- Dell R740 and earlier: “netscout1” (the Dell default is “calvin”)
- Dell R760 uses a factory-generated random password; this password is located on the pull-out Information Tag located on the front of the chassis, near the server asset tag.

NETSCOUT strongly recommends changing these defaults as soon as possible. You can also reset this password in BIOS.

After you have successfully logged in, the main web-based interface displays.

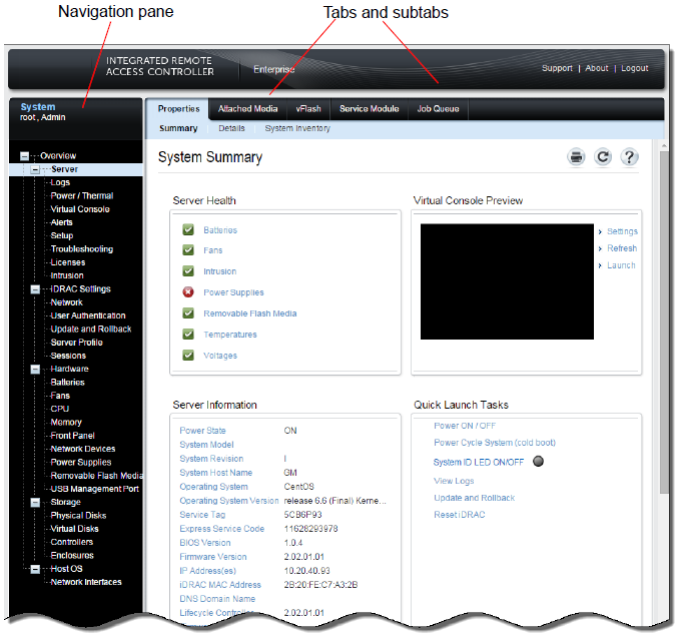


Figure B-7 Main Menu of the iDRAC Web Interface

From here you can perform a variety of remote management tasks in the tabs at the top of the user interface. Common tasks in these tabs are described in the following sections:

- Launching the iDRAC Virtual Console
- Using Virtual Media for Software Updates
- Using the Virtual Console for Software Updates
- Other iDRAC Features

Important: NETSCOUT recommends that you do not use the web-based iDRAC7 user interface to reconfigure the iDRAC IP settings. Doing so runs the risk of losing connectivity during the IP reconfiguration, resulting in an unreachable system. Instead, use the system BIOS in the event of an operating system failure.

Launching the iDRAC Virtual Console

You can use the iDRAC web-based interface to open a virtual console to the server hardware. This allows you to interact with the server hardware as if you had a directly connected keyboard and monitor. Common uses for the Virtual Console feature are:

- Reimage or upgrade the server hardware.
- Watch and interact with a boot sequence in real time, or use the Boot Capture feature from the System >Logs tab of the web interface to play back boot sequences.
- Use the Virtual Console File > Capture to File menu option to take screen shots of the Console display for use by Support.

You may use some of these features together with NETSCOUT SYST Support specialists.

To open a Virtual Console to the server hardware, perform the following steps:

1. Open a supported web browser.
2. In the **Address** field, type **https://*<iDRAC IP Address>*** and press **Enter**.
3. Log in to the iDRAC user interface with an account that includes Administrator or Operator privileges. The default login account "root" has Administrator privileges. For more information working with iDRAC user accounts refer to the iDRAC User Guides—
   - iDRAC8 User's Guide
4. You can launch the Virtual Console from either of the following pane locations:
   - **Overview > Server**: Click the **Launch** link in the **Virtual Console Preview** panel.
   - **Overview > Virtual Console**: Click the **Launch Virtual Console** link at the top of the page.

A Java applet or ActiveX plugin launches and installs. A dialog indicates the status of the connection to the Virtual Console Server. After the connection is complete, the dialog closes and the Virtual Console window displays a login prompt to the PFS Fabric Manager Server Hardware. You can use this display to interact with the server hardware as though you were directly connected.

Note: If you are accessing the iDRAC interface from a Linux operating system, an X11 console may not be viewable on the local monitor. Press Ctrl-Alt-F1 at the iDRAC Virtual Console to switch Linux to a text console. You may need to disable your browser pop-up blocker for the iDRAC IP address.

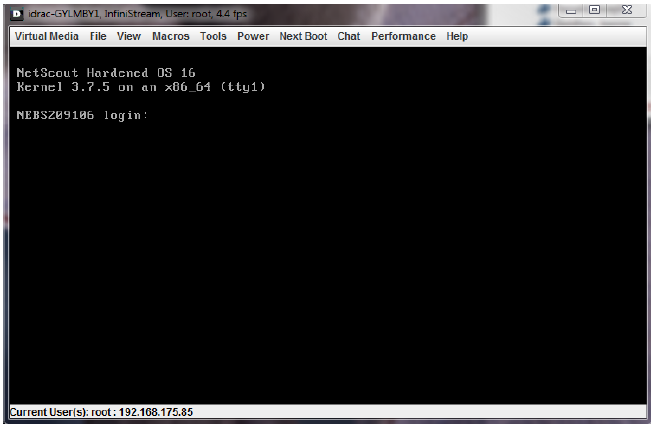


Figure B-8 Virtual Console Login (Java client depicted)

Using Virtual Media for Software Updates

You can use the iDRAC Virtual Console's Virtual Media option to upgrade the application software or reimage the PFS Fabric Manager Server Hardware altogether. This section describes how to make media available from your local client system to the server hardware for either activity. This section covers the following steps:

- Preparing Software for Use as Virtual Media
- Verifying That Virtual Media Settings Are Enabled
- Map Drives and Install from Virtual Media
- Using the Virtual Console for Software Updates

Preparing Software for Use as Virtual Media

Have the software for upgrade or re-imaging present on your local client machine:

- **ISO Image** – Download these files from the MasterCare Portal and mount to your local client machine; interact with them as you would a DVD.
- **Restore DVD** – Insert the Restore DVD in an external DVD drive connected to the local client machine.

- **Application CD, Bin Files or RPM files** - For these file types, you do not need to use the Virtual Media method. Instead, follow the directions in Using the Virtual Console for Software Updates.

Verifying That Virtual Media Settings Are Enabled

The following steps are required for use of a local ISO or local CD/DVD. You can also verify or configure Virtual Media in BIOS, but the same steps are easily done using the user interface:

1. Click on the **Server** link in the left navigation pane of the user interface.
2. Click on the **Attached Media** tab in the main body of the user interface.
3. Examine the setting for **Attach Mode**. If it is set to **Attach** or **Auto Attach**, you can proceed to Map Drives and Install from Virtual Media. If it is not, perform these steps to enable Virtual Media features—
   a. Set the **Attach Mode** dropdown to either **Attach** or **Auto Attach**.
   b. Click **Apply**.

Map Drives and Install from Virtual Media

In this procedure, you map an external CD/DVD drive or ISO to function as a Virtual Medium on the remote PFS Fabric Manager Server Hardware.

1. Launch the Virtual Console from either of the following navigation pane locations:

• **Overview > Server:** Click the **Launch** link in **Virtual Console Preview** panel.

• **Overview > Virtual Console:** Click the **Launch Virtual Console** link at the top of the page.

This triggers a Java applet to launch and install. A dialog indicates that the applet is connecting to the Virtual Console Server. After the connection is complete, the dialog closes and the Virtual Console window display an appliance login prompt.

   a. Close the applet window.
   b. Navigate to the **Server > Virtual Console** tab in the iDRAC UI.
   c. Locate the row for Plug-in Type and change the menu option from **Native** to **Java**.
   d. Click **Apply**.
   e. Relaunch the Virtual Console.

The Java plugin version of the console loads.

> **Note:** If you are using the ActiveX plugin with Internet Explorer, instead of the Java plugin, the Virtual Drive mapping may not display properly. For this reason, NETSCOUT recommends using the Java plugin version of the Virtual Console. If an ActiveX plugin tries to install, complete these steps to switch to using a Java plugin.

2. Press **Enter**, if needed, to display a login prompt, then log into the server hardware with appropriate credentials.
3. From the Virtual Console window, click the **Virtual Media** menu and select the entry to **Connect Virtual Media** (iDRAC8, Fig. 4-9).

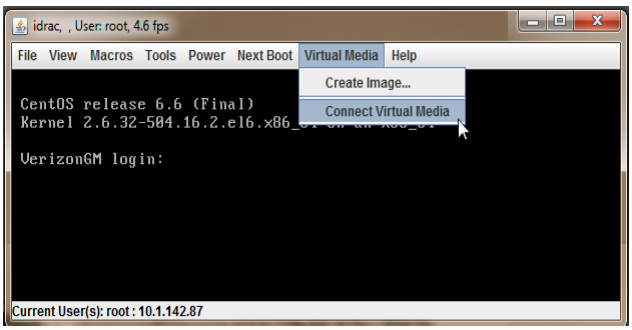


Figure B-9 Connect Virtual Media (iDRAC 8)

4 Select the **Virtual Media > Map CD/DVD** option. This command lets you map either a CD/DVD drive or a local image file (.iso or .img).

A mapping dialog appears where you can browse to the drive or image file to be mapped.

- If you are using a CD or DVD and have not already inserted it to your system, do so now.
- If you are using an ISO image, click the **Browse** button (iDRAC8, Figure B-10) and use the navigation dialog to locate and **Open** the ISO located on your client system.

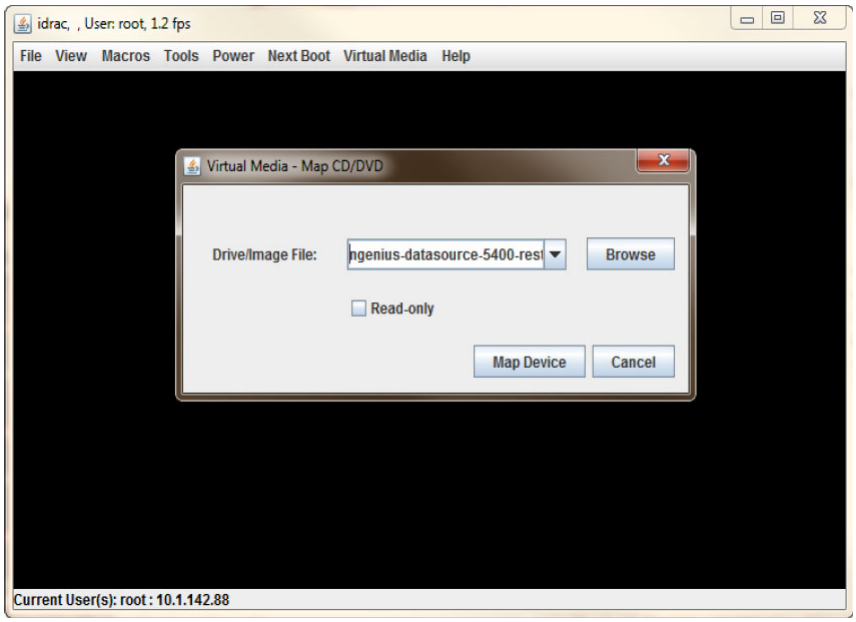


Figure B-10 Mapping Virtual Media to PFS Fabric Manager Server in iDRAC8

Next Steps: iDRAC8

1 Once you have navigated to the drive or image file to be mapped, click the **Map Device** button (Figure B-11).

2 Enable the **Next Boot > Virtual CD/DVD/ISO** option. This ensures that the system will boot from the image file or drive you just mapped in the previous steps, allowing you to reimage the target server from the drive or image file located on your local machine.

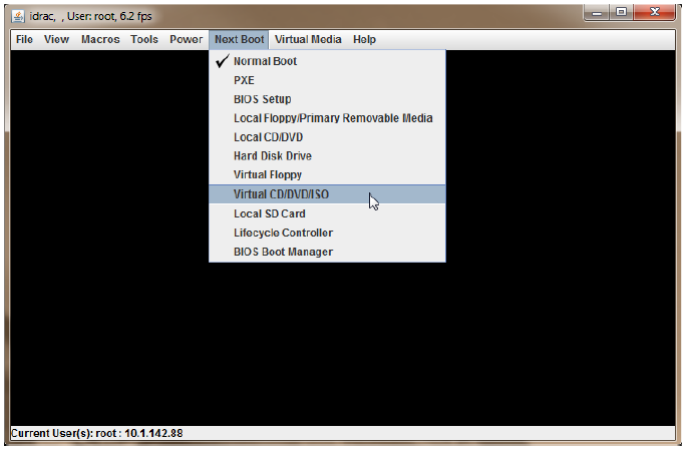


Figure B-11 Selecting the Image File or Drive as the Next Boot Drive

3 Click OK on the warning regarding the next boot device selection.

4 Return to the iDRAC8 web browser, refresh the **Server > Attached Media** tab, and check the block for **Virtual Media**.

The **Connection Status** is now **Connected**.

After the selected drive/image is mapped to the server hardware, you can boot from it as though the drive/ISO were located in the server hardware itself.

5 From the Virtual Console Power menu, select **Reset System (warm boot)**.

The system reboots and begins to install the new image.

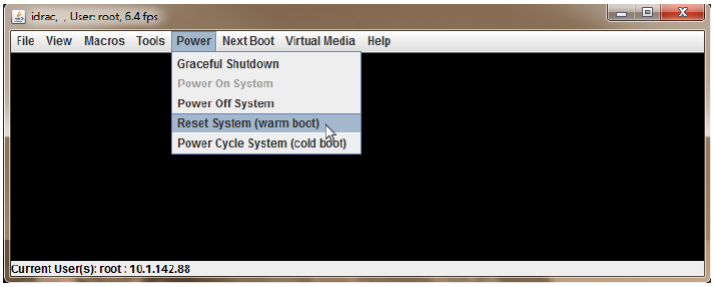


Figure B-12 Reset PFS Fabric Manager Server Hardware from Virtual Console

When the server hardware boots from the Restore DVD, the Console briefly displays "**No Signal**."

6 When the option to **Reimage an existing system** is highlighted, press **Enter** (after a brief delay, the reimage will continue automatically).

7 When prompted, select either a static or DHCP addressing model to be used. After a brief delay, the default of static will be set and the reimage will continue automatically.

8 At the end of the reimage, a Complete screen opens and displays a Reboot button. Do not click the Reboot button yet because your installation will begin again.

9 Return to the Virtual Console and enable **Next Boot > Normal Boot**. This ensures that the system will use its normal boot sequence for future boots.

10 Use the **Virtual Media > Disconnect Virtual Media** option to disconnect your local image/drive.

11 Return to the Virtual Console screen and press **Enter** on the Complete screen. The system reboots.

Using the Virtual Console for Software Updates

You can use the iDRAC Virtual Console like a local console to run the installers. Copy the software install files to the remote server hardware, then run installers from within the Virtual Console. The instructions below assume you are copying the files from a local system to the remote system.

1 Obtain the software from the NETSCOUT Customer Support site.

2 Copy the file to your local client system and then use WinSCP or another method to copy the file to the /opt directory of the remote server hardware.

3 Log into the web-based iDRAC interface.

4 Click the **Server** link in the left navigation pane of the web interface.

5 Click the **Console** tab in the main body of the interface.

6 Click the link to **Launch Virtual Console**.

7 Log into the server hardware with appropriate credentials.

Other iDRAC Features

You can monitor the system and perform a variety of tasks directly from the default landing page of the iDRAC web interface.

You may also find the following additional iDRAC features useful for troubleshooting your server hardware.

Server > Alerts

Use the **Alerts** tab to configure traps and/or Email notifications based on a wide variety of system conditions and platform events.

Server > Logs

You can use the web-based interface's **Logs** tab to view a System Event Log for the server hardware. This log can be saved to a file for submission to Technical Support personnel, if requested. You can also use this tab to replay the last three boot cycles.

Server > Power/Thermal

Use the **Power** tab to view the server hardware's current power status or to power cycle, power up, or shut down the server hardware. Power cycling operations are available in the **Server >Power/Thermal > Power Configuration > Power Control** sub-tab.

Monitoring Server Health

The **Server > Properties** tab includes a **Summary** sub-tab with Server Health status indicators for all sensors with a link to drill down to more detail on each. You can also access the system event logs and perform a collection of common operational tasks, including launching the Virtual Console.

Appendix C
Switch RMA Replacement

This appendix provides a summary of the steps required to replace a switch RMA when Fabric Manger is being used to manage PFOS devices.

Fabric Manager Switch RMA Replacement

Fabric Manager Versions earlier than 6.0.3 will require an upgrade to 6.0.3 or later to ensure that the replacement switch is detected as an RMA. If you are attempting to replace an RMA'd switch that is not running 6.0.3 or later, you will need to upgrade your switch(s) and Central Server environment first.

Note: Refer to *Upgrading PFS Fabric Manager and PFOS* in the PFS Fabric Manager Release Notes.

Fabric Manager Switch RMA Replacement Prerequisites

Do NOT attempt to connect your RMA'd switch to your Fabric Manager until you have performed the following:

1. PFOS config backup is taken from the RMA switch (either via PFOS WebUI or via NMS Backup)
2. Configure the IP address to the same IP as was previously set on the former switch. This assumes that the RMA switch is down at this point and hence only the "new" recovered switch is on network.
3. Restore the PFOS Configuration via PFOS Web UI.

Note: It's recommended to restore the configuration to the same OS version it was saved from.

4. Upgrade your RMA'd switch to 6.0.3 or later version.

Fabric Manager Switch RMA Replacement Verification

Verify the new switch by performing the following:

1. Ensure the steps in the previous section are complete.
2. Log into the PFOS Web UI for the newly RMA'd switch and navigate to the **Global Settings->System** page. Select the **NMS** Tab.
3. Enter the Fabric Manager Server IP Address or Host Name.
4. The Fabric manager should now detect the RMA'd switch as the original. It is expected that the new switch will show as **Auth Fail** state, reconnect to the switch using admin credentials.
5. All configurations will be learned from the switch again and the switch and it's configuration will reflect correctly in the NMS, as from the previous switch.

Possible issues and workarounds:

- In case the PFOS backup is not available, the NMS backup also has the running-config from each switch. This can be used to restore the config backup. If the PFOS or NMS backups are not avialable, contact NETSCOUT Support to help recover the NMS backup from the active switch.
- In some cases, at the final step, after the recovered switch is restored, it might appear as Auth Fail or Disconnected. This is expected and a reconnect will learn the switch config again. It is not necessary to disturb the topologies by unpublishing prior to connecting the RMA'd switch

- In case the NMS and RMA recovered switch are not in same release version, it is recommended that they be on same release version before attempting the procedure.

NETSCOUT SYSTEMS, INC.
310 Littleton Road
Westford, MA 01886-4105

Tel. 978 614-4000
888-999-5946
Fax 978-614-4004
E-mail info@netscout.com
Web www.netscout.com

733-1957 Rev. B