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: In the US, call 888-357-7667; outside the US, call 001 978-614-4000. Phone support hours are 8 a.m. to 8 p.m. Eastern Standard Time (EST).

E-mail: support@netscout.com

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
— Type of nGenius series packet flow switch model
— nGenius 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.

Education and Training
Education and training resources including course listings, product certification, webinars, and case studies are available at:
http://www.netscout.com/education/overview

Copyright 2009-2021 NETSCOUT Systems, Inc. All rights reserved.
Table of Contents

Chapter 1  About This Document and Introduction

Related Documentation ................................................................. 1-1
Contacting NETSCOUT Customer Care ...................................... 1-1
NETSCOUT Web Site ................................................................. 1-1
PFS Fabric Manager Overview .................................................. 1-2

Chapter 2  Login and Setup PFS Fabric Manager

Starting / Login to PFS Fabric Manager ....................................... 2-1
PFS Fabric Manager (NMS) Server .............................................. 2-1
Login to PFS Fabric Manager ...................................................... 2-1
PFS Fabric Manager Session Expiration ..................................... 2-2
PFS Fabric Manager Interface Screen ........................................ 2-2
  Configure Lifecycle ............................................................... 2-3
  Deploy Lifecycle ..................................................................... 2-5
  Inline Lifecycle ...................................................................... 2-5
  Monitor Lifecycle ................................................................. 2-6
System Settings ......................................................................... 2-7
  Bringing a PFS into Central Management ................................. 2-8
    Connecting to the PFS from the NMS .................................. 2-8
    Configuring the NMS address in the PFS ....................... 2-8
Accepting Switches into Central Management ........................... 2-10
Importing the PFS Configuration into the NMS ......................... 2-10
Removing a PFS from Central Management ............................... 2-10
Viewing Events .......................................................................... 2-11
Changing the Theme .................................................................. 2-12
Documentation .......................................................................... 2-12
End User License Agreement .................................................... 2-13
Logout of PFS Fabric Manager .................................................. 2-14

Chapter 3  Configure Lifecycle

Discover Switches ........................................................................ 3-1
  Device > Switch Acceptance ............................................... 3-2
  Perspective Menus ............................................................... 3-3
Perspective > Device ................................................................. 3-4
  Active .................................................................................. 3-4
    Active Switch Sub-Menu .................................................. 3-4
    Reconnect ......................................................................... 3-4
    Delete ............................................................................... 3-5
    Line Card Display Details ............................................. 3-5
    Line Card Port Indicators .............................................. 3-6
  Discovered ........................................................................... 3-7
  Unmanaged ........................................................................... 3-7
  PFX ..................................................................................... 3-7
Configure / Update Devices ......................................................... 3-9
  Interfaces > Primary Interface ........................................... 3-10
    Profile > Default > Basic Information ............................. 3-11
    Profile > Default > Service Profile ................................. 3-12
    Profile > Default > Time Clients ...................................... 3-13
    Profile > Default > Logging ............................................ 3-15
    Profile > Default > Logging (Secure Syslog) ...................... 3-16
Profile > Default > SNMP Feature ..................................................... 3-17
Profile > Default > Features ......................................................... 3-19
Profile > Default > Authentication Order ........................................ 3-20
Profile > Default > TACACS Server ................................................ 3-21
Profile > Default > RADIUS Server ............................................... 3-22
Transceiver Details .................................................................. 3-22
Blade/Line Card Control ............................................................... 3-24
Locate Me ................................................................................. 3-24
Connect to the Device ................................................................. 3-24
MIB File Viewing .................................................................... 3-25
External PowerSafe TAPs Configuration ...................................... 3-26
PFX > Basic Information .............................................................. 3-27
Adding a PFX Device ................................................................. 3-28

Configure Search Filter ............................................................... 3-29
Port Perspective ....................................................................... 3-29

Perspective > Port ................................................................. 3-30
Basic Information .................................................................... 3-31
Port Types ................................................................................ 3-32
Tunnel Termination Port Feature Profile ..................................... 3-33
IP Tunnel Termination ............................................................... 3-33
Tunnel Termination Considerations And Limitations ..................... 3-34
VN, VLAN, VXLAN, MPLS Tag Stripping Port Feature Profile ......... 3-35
VN, VLAN, VXLAN, MPLS Tag Stripping Port Feature Profile (UI for 5000/7000 Series Platforms) .............................. 3-35
VN, VLAN Tag Stripping Port Feature Profile (UI for 6000 Series Platforms) .................................................. 3-36

Deduplication Port Feature Profile ............................................. 3-38
Monitor_Stamping ..................................................................... 3-39
Port Properties from Deploy Lifecycle ........................................ 3-40
Configure > Port on Topology Association .................................. 3-41
Configure > Inline Port ............................................................... 3-41

Perspective > Group ................................................................. 3-42
Basic ....................................................................................... 3-42
Ports ......................................................................................... 3-43
Inline Network Group Ports ......................................................... 3-44
Inline Monitor Group Ports ........................................................ 3-45
Additional Groups .................................................................... 3-45
Configuring a Destination Group as a Remote Monitor Group for pfsMesh ........................................................................ 3-46
Removing a Load Balancing Group from a Remote Monitor Group ................................................................. 3-47
Port Group Sub-Menu ................................................................. 3-47
Configure > Group on Topology Association ................................ 3-48

Perspective > Profile ................................................................. 3-49
Port Profile .............................................................................. 3-49
Creating a Port Profile ............................................................... 3-50
Port Profile Sub-Menu ............................................................... 3-51
Creating a Port Feature Profile .................................................. 3-52
Packet Deduplication ................................................................. 3-54

MPLS-L3, VLAN and VN Tag Stripping ...................................... 3-54
Generic Stripping ..................................................................... 3-54
Port and Time Stamping ............................................................. 3-55
Port Stamping .......................................................................... 3-55
Time Stamping ......................................................................... 3-55
Packet Slicing .......................................................................... 3-56
Packet Masking ....................................................................... 3-56
Group Profile .......................................................................... 3-58
Creating a Group Profile ............................................................. 3-59
Tunnel Profile .......................................................................... 3-60
Creating a Tunnel IP Interface Profile ........................................ 3-60
Creating a Tunnel VxLAN Profile ............................................... 3-61
Creating a Tunnel GRE Profile .................................................. 3-62

Perspective > Filter ................................................................. 3-64
Chapter 4  Deploy Lifecycle

Topology Types ............................................................... 4-1
  User Topologies .......................................................... 4-1
  Device Topologies ......................................................... 4-1
    Saving Imported Traffic Maps as User Topologies ............ 4-2
Create a New Topology .................................................. 4-2
Topology Screen / Features ............................................ 4-3
Populating a Topology ................................................... 4-4
  Port Nodes / Port Groups / Filter Details ....................... 4-4
    Port Nodes .......................................................... 4-4
    Flow Nodes ......................................................... 4-5
    Port Groups ......................................................... 4-6
Making Connections ....................................................... 4-7
  Flow Precedence ....................................................... 4-8
Adding Port Groups ....................................................... 4-9
Adding Drop Packets ..................................................... 4-10
Adding Remote Monitor Groups ....................................... 4-11
Publishing a Topology .................................................. 4-13
Chapter 5  Inline Lifecycle

Assign a New Inline Topology ................................................. 5-1
Inline Topology Screen / Features ........................................... 5-2
Creating an Inline Topology .................................................. 5-3
Inline Ports and Groups ....................................................... 5-3
Inline Topology Overview .................................................... 5-4
Inline Topology Connections
  Flow Nodes ................................................................. 5-5
Inline Topology Publication .................................................. 5-6
  Port Groups ............................................................... 5-7
  Filters ...................................................................... 5-7
  Tools ...................................................................... 5-7
  Toolchain (one per topology) .............................................. 5-7
  Inline Traffic Maps ....................................................... 5-7
Inline Topology Versioning
  Learning .................................................................. 5-8

Chapter 6  Monitor Lifecycle

Device Status .................................................................... 6-1
Blade Status ..................................................................... 6-2
Port Monitor ..................................................................... 6-3
  Port Status Indicators .................................................... 6-3
  Network Statistics .......................................................... 6-4
  Deduplication ................................................................ 6-5
  Control Packets ............................................................ 6-6
pfsMesh ......................................................................... 6-6
  Viewing Combination of Managed / Unmanaged Devices ....... 6-9
  PFSMesh - Refresh Display ............................................. 6-10
Events ............................................................................ 6-11
  Link Layer Discovery Protocol (LLDP) ............................. 6-13
Monitor Search Filter .......................................................... 6-14
Undocking Monitor Palettes ................................................ 6-15
  Undocking Limits .......................................................... 6-16

Chapter 7  System Settings

System Configuration ............................................................ 7-1
System Administration ......................................................... 7-1
  Backup/Restore ............................................................. 7-1
  Certificates ................................................................... 7-2
  IP Tables ...................................................................... 7-3
    Adding Rules .............................................................. 7-4
    Editing Rules .............................................................. 7-4
    Bulk Publishing ........................................................... 7-4
Appendix A   Installing PFS Fabric Manager Central Server (Software-Only Version or OS Upgrade)

  Server Requirements ................................................. A-1
  Server Operating System ........................................... A-1
  Attaching Cables to the Physical Server ......................... A-2
  Installing PFS Fabric Manager Software ......................... A-2
  Upgrading the Operating System on the PFS Fabric Manager NMS (CentOS 6 to CentOS 8) ......................... A-4

Appendix B   Configuring and Troubleshooting the Server Remotely

  Using the Dell™ Remote Access Controller ................. B-1
    iDRAC Requirements ........................................... B-2
      Additional Notes for Internet Explorer Users ................ B-2
      Firefox Users – Preventing Multiple Plugin Installations ................ B-3
      Network Requirements for Using iDRAC ......................... B-3
      Physical Connections ........................................ B-3
      Required Network Listener Ports ............................. B-3
      User Account Requirements ................................. B-4
  iDRAC Settings in System BIOS ................................. B-5
    Accessing iDRAC Settings in BIOS ......................... B-5
    Changing the iDRAC Password ................................ B-6
    Configuring iDRAC Network Settings ......................... B-7
    Restoring iDRAC Defaults ................................. B-9
  Connecting to the iDRAC Interface .......................... B-9
    Launching the iDRAC Virtual Console ................... B-10
    Using Virtual Media for Software Updates ....... B-11
      Preparing Software for Use as Virtual Media ........... B-11
      Verifying That Virtual Media Settings Are Enabled .... B-12
      Map Drives and Install from Virtual Media ................ B-12
      Next Steps: iDRAC8 ........................................ B-13
      Using the Virtual Console for Software Updates ....... B-14
  Other iDRAC Features ........................................... B-15
    Server > Alerts ........................................ B-15
    Server > Logs ........................................ B-15
    Server > Power/Thermal .................................... B-15
# Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2021</td>
<td>PFS FM 6.0.3 Rev A</td>
<td>• Updated <a href="#">Perspective &gt; Filter</a> to include new screen shots for creating a new filter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Custom Offset</a> to include new screen shot for the custom offset header drop-down menu and updated the corresponding table listing the descriptions for the Custom Offset port settings.</td>
</tr>
</tbody>
</table>
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.

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 **001 978-614-4000**.
Phone support hours are 8 a.m. to 8 p.m. Eastern Standard Time (EST).

**E-mail:** support@netscout.com

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

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).

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

**Important:** PFS Fabric Manager is only supported on a PC using Google Chrome.

### 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.nn`).
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.
2-4 PFS Fabric Manager Interface Screen
Deploy Lifecycle

Deploy Lifecycle allows creating, versioning, and publication of topologies. See Deploy Lifecycle on page 4-1 for details.

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
  - Certificates
  - IP Tables
  - Licenses
  - NTP
  - Storage
  - Switch Configs
  - Software/Firmware

- **Access Control**
  - Authentication Order
  - Authentication Servers
  - Password Policy
  - Roles
  - User Management
    - All Users
    - My Account
  - 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 3-4 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 2-10 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 2-10 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 PFM (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.
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**.

![Change Theme Screenshot]

Documentation

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

![Documentation Screenshot]
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**.
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 6010 Switch](image)

**PFS 5010 Switch**

![PFS 5010 Switch](image)

**PFS 5110 Switch**

![PFS 5110 Switch](image)
The Perspective menus provide access to all devices (switches), ports, groups, profiles, and filters.

Five categories are available from the Perspective menu:
- Device - refer to Perspective > Device on page 3-4
- Port - refer to Perspective > Port on page 3-30
- Group - refer to Perspective > Group on page 3-42
- Profile - refer to Perspective > Profile on page 3-49
- Filter - refer to Perspective > Filter on page 3-64
- Trigger - refer to Perspective > Trigger on page 3-74
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:

```
Perspective: DEVICE
Views
1  ACTIVE
   9  PFS6100VM-48
2  DISCOVERED
   1  PFS6100VM-48
   1  PFS100VM-48
2  UNMANAGED
   0  PFS6100VM-48
   0  PFS100VM-48
2  PFX
   3  PFX-1
   0  PFX-2
```

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 3-9) of the device.

Active Switch Sub-Menu

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

- Reconnect
- Delete

Reconnect

Selecting Reconnect 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

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

Line Card Display Details

Port attributes are accessible by hovering the cursor over an active line card port from the Hardware graphic view. Selecting Information displays the details / settings of the installed transceiver.
Line Card Port Indicators

Status of line card ports are displayed as follows:

- Green - Transceiver is installed and connected
- Red - Transceiver is installed but in alarm mode
- Blank - Transceiver not active
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 a Hardware screen allowing detailed viewing of each device and installed line cards (refer to Device > Switch Acceptance on page 3-2).
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:
  - Basic Information
  - Service Profile
  - Time Clients
  - Logging
  - SNMP
  - Feature
  - Authentication Order
  - TACACS Server
  - RADIUS Server
  - Stripping
- PFX > Basic Information
Interfaces > Primary Interface

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the device / switch.</td>
</tr>
<tr>
<td>DHCP</td>
<td>Enable/Disable DHCP</td>
</tr>
<tr>
<td>IPv4 Settings</td>
<td>Address Devices network IPv4 address (e.g., 192.168.255.11/24)</td>
</tr>
<tr>
<td></td>
<td>Gateway Devices network gateway address (e.g., 10.250.176.1)</td>
</tr>
<tr>
<td></td>
<td>DNS DNS server address (e.g., 10.200.96.11)</td>
</tr>
<tr>
<td>IPv6 Settings</td>
<td>Address Device IPv6 address (e.g., fc00:0:3:1ad3::23:a/64)</td>
</tr>
<tr>
<td></td>
<td>Gateway Device network gateway address (e.g., fc00:0:3:1ad3::23:a/64)</td>
</tr>
<tr>
<td></td>
<td>DNS DNS server address (e.g., fc00:0:3:1ad3::23:b/64)</td>
</tr>
</tbody>
</table>
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 \textbf{X} to cancel the changes.

<table>
<thead>
<tr>
<th>Port Prefix Name</th>
<th>(Option) Enter a port prefix name to be used to identify the ports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>Base VLAN ID</td>
</tr>
<tr>
<td>TPID Ether Type</td>
<td>Select the TPID Ether Type:</td>
</tr>
<tr>
<td>Replication Mode</td>
<td>Select Ingress or Egress (PFS 6000 series only)</td>
</tr>
<tr>
<td>Location</td>
<td>Physical location of device.</td>
</tr>
<tr>
<td>Contact</td>
<td>Contact information.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Enables or disables the LCD panel on the front of PFS 6000 series devices</td>
</tr>
<tr>
<td>Netconf (SSH)</td>
<td>Disabled</td>
</tr>
<tr>
<td>Netconf Port</td>
<td>Default port = 832 for Netconf over SSH. Do not change this parameter.</td>
</tr>
<tr>
<td>SSH</td>
<td>Enable or Disable SSH access.</td>
</tr>
<tr>
<td>SSH Port</td>
<td>Enter port number (default = 22) for SSH access.</td>
</tr>
</tbody>
</table>
Profile > Default > Time Clients

Click the edit icon to make any changes to the time clients 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.  
<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Note: Entering and saving an address for NTP Server 1, Server 2, and/or Server 3 sets NTP to Enabled mode.</th>
</tr>
</thead>
</table>
| GPS       | Cable Length         | Specify the maximum cable length (1 to 300 meters; default = 1) between system chassis and a GPS receiver.  
|           |                      | Note: Entering a value for cable length sets GPS to Enabled mode. |
| PTP       | Note: Entering a value or enabling an option sets PTP to Enabled mode. |
|           | IP Address           | Configures the IP address/mask of the PTP module on the chassis. Assign a static IP address or enable the DHCP field. |
|           | PTP Domain           | Specifies the PTP domain (1-255, default 0). |
|           | Announce Message Interval | Configures the interval between PTP announcement messages (-4 to 5, default 1). |
|           | Announce Receive Timeout | Configures the number of attempts before timeout of receive messages (2 to 10, default 3). |
|           | Sync Interval        | Configures the synchronization interval (-8 to 2, default 0). |
|           | DHCP                 | Enables or disables DHCP for the IP address of the PTP module on the chassis. |
|           | Transport            | Specifies the transport type for PTP messages (UDP or Ethernet). |
|           | PTP Port             | Specifies the port as PTP or Ethernet. |
|           | Delay Mechanism      | Configures either end-to-end or peer-to-peer for PTP delay messages. |
|           | PPS Source           | Specifies the source for pulse per second (PPS) (default is ptp_port). |
|           | PPS Cable Length     | Maximum cable length for the distance between the system chassis and the PTP receiver (1-300m, default 10m). |
|           | Telecom Profile      | Enable or disable the telecom profile. |
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.

<table>
<thead>
<tr>
<th>Logging</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Trace Log</td>
<td>Facility / Severity</td>
<td>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).</td>
</tr>
<tr>
<td>Syslog</td>
<td>Server 1 /Server 2/Server 3</td>
<td>Enter the server IP addresses. Note: Entering and saving an address for one or more servers sets Syslog to Enabled mode.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>SNMP</th>
<th>Enable / Disable</th>
<th>Enable or Disable this feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Select which versions (v1, v2c, and/or v3) of SNMP to use - one or more versions can be selected.</td>
<td></td>
</tr>
<tr>
<td>Maximum Message Size</td>
<td>Enter the maximum message size (default = 50,000).</td>
<td></td>
</tr>
<tr>
<td>VACM</td>
<td>From VACM Settings, enter the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• View-based Access Control Model groups and MIB views.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Member of the VACM group and define access rights for groups.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Subtree for each view.</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td>Add and edit members of the VACM group and define access rights.</td>
<td></td>
</tr>
<tr>
<td>View</td>
<td>Add and edit new subtree views.</td>
<td></td>
</tr>
<tr>
<td>USM</td>
<td>User-based Security Model:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Add users and set authentication and privacy settings in the User-based Security Model.</td>
<td></td>
</tr>
<tr>
<td>Target</td>
<td>Specify the SNMP target addresses and security model(s) to use.</td>
<td></td>
</tr>
<tr>
<td>Community</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Notify</td>
<td>Specify which SNMP target addresses will receive notifications.</td>
<td></td>
</tr>
<tr>
<td>Traps</td>
<td>Specify which SNMP traps will be enabled.</td>
<td></td>
</tr>
</tbody>
</table>
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.

- **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 hash algorithm for PFS 5000/7000 series.
- **MAP Profile**:
- **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.
- **Powersafe**: To enable or disable the feature, either select or deselect the Powersafe checkbox. This feature requires a PowerSafe device.
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 7-17) 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 7-9) for a switch.

To add a new TACACS server click on the Add More TACACS (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.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host / IP Address</td>
<td>IPv4/IPv6 address or a fully qualified domain name of the TACACS server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port for access to the server (default 49).</td>
</tr>
<tr>
<td>Key</td>
<td>AES encrypted string to authenticate to the server.</td>
</tr>
<tr>
<td>Prompts</td>
<td>TACACS prompts parameter.</td>
</tr>
<tr>
<td>Service</td>
<td>TACACS service parameter. Note: Service value is recommended for the authentication to work correctly.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Time after which requests to the server time out (default 30 seconds).</td>
</tr>
<tr>
<td>Retransmit</td>
<td>Number of times PFOS attempts to contact the TACACS server (default 3).</td>
</tr>
</tbody>
</table>
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 7-11) for a switch.

To add a new RADIUS server click on the **Add More RADIUS** (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**

<table>
<thead>
<tr>
<th>Host / IP Address</th>
<th>IPv4/IPv6 address or a fully qualified domain name of the RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Port for access to the server (default 0).</td>
</tr>
<tr>
<td>Key</td>
<td>AES encrypted string to authenticate to the server.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Time after which requests to the server time out (default 30 seconds).</td>
</tr>
<tr>
<td>Retransmit</td>
<td>Number of times PFOS attempts to contact the RADIUS server (default 3).</td>
</tr>
</tbody>
</table>

---

Transceiver Details

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

<table>
<thead>
<tr>
<th>Details</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model: FTX8874D3BACV</td>
<td>Line Card Slot: 1</td>
</tr>
<tr>
<td>Manufacturer: FINISAR CORP.</td>
<td>Cage Location: 1</td>
</tr>
<tr>
<td>Version: 1.0</td>
<td></td>
</tr>
<tr>
<td>Interface Type: SFP</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLVR</td>
<td>-</td>
</tr>
<tr>
<td>LLVR State</td>
<td>-</td>
</tr>
<tr>
<td>LLVR Power Rx</td>
<td>-</td>
</tr>
<tr>
<td>LLVR Power Tx</td>
<td>-</td>
</tr>
<tr>
<td>LLVR Bias Current</td>
<td>-</td>
</tr>
<tr>
<td>LLVR Channel Power Rx</td>
<td>-</td>
</tr>
<tr>
<td>LLVR Channel Power Tx</td>
<td>-</td>
</tr>
<tr>
<td>LLVR Supply Voltage</td>
<td>-</td>
</tr>
<tr>
<td>LLVR Volt</td>
<td>-</td>
</tr>
<tr>
<td>Temperature</td>
<td>-</td>
</tr>
</tbody>
</table>
Blade/Line Card Control

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

![Blade/Line Card Control Diagram]

**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 its lights continuously for 2 minutes then turn off. A "System Locator Activated for <Switch Name>" will be displayed in a message prompt.

![Locate Me Diagram]

Connect to the Device

You can connect to either the PFOS web UI or CLI 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.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module Type</td>
<td>Enter the module type</td>
</tr>
<tr>
<td>Segment Name</td>
<td>Enter the segment name</td>
</tr>
<tr>
<td>Fiber Pair State</td>
<td>Enter the Fiber Pair state</td>
</tr>
<tr>
<td>Operational State</td>
<td>Enter the Operational state</td>
</tr>
<tr>
<td>Manual Mode</td>
<td>Select from Off, Bypass, Forward, Block, or InPairDown</td>
</tr>
<tr>
<td>Bypass Mode</td>
<td>Select from Bypass, Forward, Block, or InPairDown</td>
</tr>
</tbody>
</table>
PFX > Basic Information

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

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the PFX device</td>
</tr>
<tr>
<td>IP Address/Host Name</td>
<td>IPv4/IPv6 address or a fully qualified domain name of the PFX device</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for CLI connectivity</td>
</tr>
</tbody>
</table>
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.
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, using wild card * and ? variables.

Examples:
PF55*, *6100*, *6??, where
* matches zero or more characters
? matches exactly one character

Examples:
Port 1* matches all entries starting with Port 1
*6100* matches all entries containing 6100
Port ?-1 matches all entries such as Port 1-1, Port 2-1, etc.
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
- 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Name</td>
<td>Use the default name or assign a name for the port to help identify the devices or network segments connected to the unit.</td>
</tr>
<tr>
<td>Port ID</td>
<td>Use the default ID or assign an ID for the port to help identify the devices or network segments connected to the unit.</td>
</tr>
<tr>
<td>Port Type</td>
<td>Specify the port type:</td>
</tr>
<tr>
<td></td>
<td>• Network</td>
</tr>
<tr>
<td></td>
<td>• Monitor</td>
</tr>
<tr>
<td></td>
<td>• Service</td>
</tr>
<tr>
<td></td>
<td>• Duplex</td>
</tr>
<tr>
<td></td>
<td>• pStack</td>
</tr>
<tr>
<td></td>
<td>• Inline Network</td>
</tr>
<tr>
<td></td>
<td>• Inline Monitor</td>
</tr>
<tr>
<td>Network</td>
<td>Port Profile</td>
</tr>
<tr>
<td>Speed</td>
<td>Select the transceiver port speed, if the inserted transceiver supports more than one speed.</td>
</tr>
<tr>
<td>Link State</td>
<td>Select the link state for the port:</td>
</tr>
<tr>
<td></td>
<td>• Auto – Normal operation</td>
</tr>
<tr>
<td></td>
<td>• Force Down – Force the link down</td>
</tr>
<tr>
<td></td>
<td>• Force Up – Force the link up</td>
</tr>
<tr>
<td>VLAN Tagging</td>
<td>Enable / Disable VLAN Tagging in this port. Note: VLAN ID setting is ignored on pStack ports.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.
- **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.
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.

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

**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.

<table>
<thead>
<tr>
<th>Feature Profile</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VN Tag Stripping</td>
<td>Enable / Disable VN Tag Stripping on this port.</td>
</tr>
<tr>
<td>VLAN Tag Stripping</td>
<td>Enable / Disable VLAN Tag Stripping on this port.</td>
</tr>
<tr>
<td>Number of Tags to Strip</td>
<td>User-selectable number (i.e., 1, 2, or all) of tags to be removed.</td>
</tr>
<tr>
<td>VXLAN Tag Stripping</td>
<td>Enable / Disable VXLAN Tag Stripping on this port.</td>
</tr>
<tr>
<td>MPLS L3 Label Stripping</td>
<td>Enable / Disable MPLS L3 Label Stripping on this port.</td>
</tr>
</tbody>
</table>

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.
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.

<table>
<thead>
<tr>
<th>VLAN Tag Stripping Port Feature Profile</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VLXAN Tag Stripping</td>
<td>Enable / Disable VXLAN Tag Stripping on this port.</td>
</tr>
<tr>
<td>VTEP</td>
<td>IP address for VXLAN Tunnel End Point.</td>
</tr>
<tr>
<td>UDP Port</td>
<td>Port number for UDP.</td>
</tr>
<tr>
<td>VNID</td>
<td>24-bit segment ID number for VXLAN.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VN Tag Stripping</td>
<td>Enable / Disable VN Tag Stripping on this port.</td>
</tr>
<tr>
<td>VLAN Tag Stripping</td>
<td>Enable / Disable VLAN Tag Stripping on this port.</td>
</tr>
<tr>
<td>Number of Tags to Strip</td>
<td>User-selectable number (i.e., 1, 2, or all) of tags to be removed.</td>
</tr>
<tr>
<td>TPID</td>
<td>Tag Protocol Identifier (TPID) with standard value of 0x8100.</td>
</tr>
</tbody>
</table>
Deduplication Port Feature 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.

<table>
<thead>
<tr>
<th>Deduplication Port Feature Profile</th>
<th>Enable / Disable Deduplication on this port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Window</td>
<td>Specify a time window of between 1 and 4,000 milliseconds (default = 10) for tracking and comparison for each unique packet.</td>
</tr>
<tr>
<td>Use Packet Fields</td>
<td>Layer 2</td>
</tr>
<tr>
<td></td>
<td>VLAN Tags</td>
</tr>
<tr>
<td></td>
<td>MPLS Labels</td>
</tr>
<tr>
<td></td>
<td>Layer 3</td>
</tr>
<tr>
<td></td>
<td>Identification</td>
</tr>
<tr>
<td></td>
<td>Time to Live</td>
</tr>
<tr>
<td></td>
<td>End of Frame</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Monitor Stamping

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.

<table>
<thead>
<tr>
<th>Monitor Stamping</th>
<th>Enable / Disable Monitor Stamping on this port. Assigns a port stamp when traffic leaves a monitor port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Stamping</td>
<td>Select One Byte Flat or Two Byte Flat as the portstamping option (Two Byte Flat is the default).</td>
</tr>
<tr>
<td>Monitor Output Timestamping</td>
<td>Enable / Disable Monitor Time Stamping on this port. Assigns a time stamp when traffic leaves a monitor port.</td>
</tr>
</tbody>
</table>
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**.
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.
Ports

Select the ports to be included in the new port group by clicking on the square next to each applicable port name. The port names are listed in 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.

  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 and having pfsMesh Visibility set to Enabled 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 3-42) and Ports (Ports on page 3-43) 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
- Clone 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: PFS 6010 Advanced Line Card Features**

Currently, PFS Fabric Manager supports a PFS 6000 with advanced line cards inserted, however, some advanced features (e.g., Packet Slicing, and Packet Masking) are not yet configurable within the GUI.
Creating a Port Profile

1 From Perspective > Profile, click on **Profile**. Select **Port Profiles** and **New Port Profile** from the profile menu, then click on the Accept icon.

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

<table>
<thead>
<tr>
<th>Profile Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Select the required switch.</td>
</tr>
<tr>
<td>Blade Model</td>
<td>Select the required line card for the selected switch.</td>
</tr>
<tr>
<td>Port Type</td>
<td>Select the required port for the selected line card.</td>
</tr>
<tr>
<td>Basic Name</td>
<td>Profile Name (56 characters maximum)</td>
</tr>
<tr>
<td>Properties</td>
<td>Speed: Select the transceiver port speed, if the inserted transceiver supports more than one speed.</td>
</tr>
</tbody>
</table>
|                  | 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
- Clone the selected profile
- Delete port feature profile
Creating a Port Feature Profile

1. From Perspective > Profile, click on + Profile. Select Port Profiles and New Port Feature Profile from the profile menu, then click on the Accept icon.

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 enter the IP address of the device the port feature profile is associated with.

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

When accessing data from networks, duplicates of packets are often captured and aggregated together. This then requires that the tools identify and remove the duplicate packets, and if not, the tools will alarm on the duplicates or produce compromised data and results.

Typical causes of duplication include planned redundancies in network and monitoring design and filter overlap during traffic capture and aggregation, both leading to duplicate packets. This creates challenges such as consumption of bandwidth on a monitoring tool’s receiving port, usage of valuable monitoring tool processing resources resulting in decrease of actual processing bandwidth, and generation of false positive errors reported in monitoring tools.

PFS Fabric Manager’s ability to remove duplicates provides a substantial reduction in the volume of traffic to the tools, an increase in tool efficiency, reduction in errors on the monitoring tool, and closure of security holes that exist in other implementations.

De-duplication capabilities include:

- Selective packet de-duplication.
- Keyed secure hash for identifying duplicates.
- Configurable packet/time window.
- Full 10G line rate de-duplication per port.
- Discarding of all subsequent duplicates of any packet (within the specified time window).
- Generation of duplicated traffic statistics.

Deduplication is available on the 40SadvR line card for eight ports in each group, allowing up to 24 ports of deduplication per line card.

MPLS-L3, VLAN and VN Tag Stripping

Many monitoring and analysis tools cannot handle data flows that are tagged with MPLS labels or multiple VLAN tags, which are primarily used to transport traffic across networks to provide services such as virtual private networks (VPNs), or with VN-tags, which are used between Cisco Nexus distributed virtual switches. Removing these labeling or tagging protocols also allows the packets to be more easily filtered and load-balanced based on the Layer 3 and Layer 4 headers.

MPLS label stripping removes all MPLS labels, and allows you to specify:

- The value of the source MAC address, for the purpose of (for example) retaining reference to the original outer MPLS label value.
- The packet’s Ethertype, since the MPLS labels themselves do not contain the encapsulated frame’s Ethertype.

VLAN tag stripping allows user-selectable number (such as 1, 2, or all) of tags and types (such as IEEE 802.1q, IEEE 802.1ad, and non-standard) of tags to be removed.

VN-tag stripping simply removes the VN-tag.

Generic Stripping

Many monitoring and analysis tools cannot handle data flows that are encapsulated within numerous protocols, which are primarily used to transport traffic across various managed networks to provide service level assurance or transparency. Removing the encapsulation or tagging protocols also allows the packets to be more easily filtered and load-balanced based on the inner Layer 2, Layer 3, and Layer 4 headers.

The generic stripping feature supports pre-defined protocols that make use of the generic stripping capability. The pre-defined protocols are:

- Cisco FabricPath
- MAC-in-MAC
- TRILL (Transparent Interconnection of Lots of Links)
- VxLAN (Virtual Extensible LAN)

Only one of these generic stripping protocols will be processed on any given packet.
Port and Time Stamping

Port and time stamping are available on the 40SadvR line card for up to six ports in each group of 14 with the Deduplication image, allowing up to 16 ports of stamping per line card, or all 14 ports with the vSlice image, allowing up to 40 ports of stamping.

Port Stamping

Port stamping allows, on an input network port basis, the addition of a single or double byte to the end of the payload of each packet, immediately before the CRC (in the packet’s trailer), indicating the input port of the system on which the packet was captured. The CRC is recalculated after the addition of the port stamp to preserve the integrity of the packet, thereby enabling the port stamped packet to be added to the destination ports as a standard Ethernet packet.

There are two port numbering methods for the byte stamp: single-byte and dual-byte. For the single-byte method, the first port is numbered 0 at the furthest left and uppermost port (by conceptually turning the line card on its side). From there, PFS Fabric Manager counts sequentially down the column of ports and moves on to the next column on the right, starting from the top down again, and so on, until all ports are counted for each line card slot, before moving on to the next slot. After the numbering reaches 255, it will stay at 255 for the rest of the ports.

For the dual-byte method, the ports are numbered in accordance with the value of the port minus 1. (Port stamp numbering is zero-based.)

For example, the following packet shows the single-byte port stamp 04 in a red box, and the four-byte recalculated CRC in a blue box.

Time Stamping

Time stamping provides, on an input network port basis, the addition of an eight-byte time stamp to the end of the data payload of each packet.

The eight-byte (64-bit) time stamp has this format:

<table>
<thead>
<tr>
<th>Bits</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-31</td>
<td>Time in seconds since Epoch (00:00:00 GMT January 1, 1970)</td>
</tr>
<tr>
<td>32-61</td>
<td>Subsecond time in nanoseconds, in 20nsec increments</td>
</tr>
<tr>
<td>62-63</td>
<td>Time synchronization source:</td>
</tr>
<tr>
<td></td>
<td>00: Uncalibrated; internal clock only</td>
</tr>
<tr>
<td></td>
<td>01: NTP synchronization</td>
</tr>
<tr>
<td></td>
<td>10: GPS (1PPS with TSIP) or 1PPS-only synchronization</td>
</tr>
<tr>
<td></td>
<td>11: PTP synchronization</td>
</tr>
</tbody>
</table>

The first four bytes count in seconds, and the second four bytes count in nanoseconds. These two groups of bytes are effectively separated by a decimal point. The time stamp is created as the first bit enters the input Network port.

For example, the following packet shows the eight-byte time stamp in a red box, and the four-byte recalculated CRC in a blue box. The value of the time stamp is 00000B7F = 2,943 seconds since Epoch time, 002DC940 = 3000640ns = 0.003000640 seconds, and 0 = internal clock source. The resulting value is 2943.003000640 seconds.
Time stamp values start at 0.0 seconds from PFS Fabric Manager boot time, but then switch over to values referenced to Epoch time as soon as the system time is accepted as stable. This can take a few minutes following boot.

Each time stamp value is the number of seconds since Epoch time, which is 00:00 UTC 1st January 1970, and does not take into account the leap seconds adjustment. All ports are exactly synchronized with one another because they use the same clock source. The timestamp is in TAI (Temps Atomique International) format.

Packet Slicing

Many monitoring and analysis tools, such as for VoIP or video, need to see and analyze every packet in a flow for the protocols of interest but do not necessarily require seeing the entire contents of each packet. They might only require visibility into, for example, IP, UDP, and RTP header information. Other tools, such as those for security monitoring, might not be legally allowed to see or have access to the payload part of a flow, such as HTTP or email content.

PFS Fabric Manager supports conditional slicing of packets, from a user-defined point, such that any data following the defined point is removed from the packets that are forwarded out the system’s Monitor ports.

![Packet Slicing Diagram]

The point at which the slicing occurs is determined by an expression, similar to those used in creating filter expressions. The cyclic redundancy check (CRC) is recalculated for each packet.

Definition and capabilities of slice filtering are similar to normal filtering, except for the following specific differences:

- Conditional slicing does not support a custom offset mask.
- Conditional slicing supports a maximum of eight filters per port.

Conditional slicing is available on the 40SadvR line cards for all ports in each group of 14, allowing up to 40 ports of stripping per line card.

Packet Masking

Companies often need to see and analyze every packet for monitoring purposes, or even store various data types for troubleshooting or data retention compliance reasons. However, these packets typically contain sensitive or personal information which, if not removed or hidden, can result in noncompliance with regulations such as HIPAA, PCI-DSS, and GDPR.

Although slicing the packet, such as with Packet Slicing, might be one way to address this, monitoring or security applications often want to have the original packet frame retained. Therefore, the ability to write over or mask out the data in the packet becomes necessary.

Packet Masking enables conditional masking of packets, from a user-defined point, such that a specified length of data following the defined point is written over within the packets that are forwarded out the Monitor ports.

You can specify the packets to be masked, a mask pattern, the length of the mask, an offset for the mask, and an anchor point.

Packet masking is available on the 40SadvR line cards for all ports in each group of 14, allowing up to 40 ports of stripping per line card.

For example, consider a masking definition with an anchor point at the start of the packet, an offset of 100 bytes, a mask length of 100 bytes, and a mask pattern of 0xE. After processing, a packet would look like this:
Up to eight mask definitions can be present for any one port.
Packet masking is supported on all port types except Service.
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 Profiles and Group Features from the profile menu, then click on the Accept icon. 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 Profiles and IP Interface from the profile menu, then click on the Accept icon. 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 Profiles** and **VxLAN** from the profile menu, then click on the Accept icon. 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 Profiles and GRE from the profile menu, then click on the Accept icon. 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.
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 3-66
- **Protocol** on page 3-67
- **Port** on page 3-68
- **Custom Offset** on page 3-68
- **Custom** on page 3-69

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.
### MAC Address

<table>
<thead>
<tr>
<th>Operator</th>
<th>Select how to combine source and destination (logical and / or) of MAC address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bi-Directional</td>
<td>Enable/disable bi-directional functionality</td>
</tr>
<tr>
<td>Source</td>
<td>Ethernet (IEEE 802.3 - Layer 2) source address. Additional addresses can be added as required.</td>
</tr>
<tr>
<td>Destination</td>
<td>Ethernet (IEEE 802.3 - Layer 2) destination address. Additional addresses can be added as required.</td>
</tr>
</tbody>
</table>

### IP Address

<table>
<thead>
<tr>
<th>Operator</th>
<th>Select how to combine source and destination (logical and / or) of IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bi-Directional</td>
<td>Enable/disable bi-directional functionality</td>
</tr>
<tr>
<td>Source / Mask</td>
<td>IP (Layer 3) source address (if an IP packet). Additional masks can be added as required.</td>
</tr>
<tr>
<td>Destination / Mask</td>
<td>IP (Layer 3) destination address (if an IP packet). Additional masks can be added as required.</td>
</tr>
</tbody>
</table>

### Others

<table>
<thead>
<tr>
<th>Operator</th>
<th>Select how to combine the Layer 2 / Layer 3 values (logical and / or).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 Etype</td>
<td>Ethernet Type. Refer to the Protocol list to restrict the EType settings to a particular protocol. Additional ranges can be added as required.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Enter the IEEE 802.1q VLAN ID (if a tagged packet). Additional ranges can be added as required.</td>
</tr>
<tr>
<td>Tag Priority</td>
<td>Enter the IEEE 802.1p/q priority (if a tagged packet). Additional ranges can be added as required.</td>
</tr>
<tr>
<td>Layer 3 IP TOS</td>
<td>Enter the type of service (TOS) class for the filter. Additional ranges can be added as required.</td>
</tr>
<tr>
<td>IPv6 Flow</td>
<td>Enter the IP Flow field (if an IPv6 packet). Additional ranges can be added as required.</td>
</tr>
</tbody>
</table>
**Protocol**

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

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

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

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

<table>
<thead>
<tr>
<th><strong>Operator</strong></th>
<th>Select how to combine (logical and / or) of TCP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Feature Set</strong></td>
<td>Specify with which PFS the Custom Offset filter should be compatible.</td>
</tr>
<tr>
<td></td>
<td>Generation 1 - Most Generation 1 filter are compatible with all switches.</td>
</tr>
<tr>
<td></td>
<td>Generation 2 - Generation 2 filters are compatible with 7031 model switches.</td>
</tr>
<tr>
<td><strong>Presets</strong></td>
<td>GTP Flags, GTP Length, GTP Message Type, GTP Destination IP Address,</td>
</tr>
<tr>
<td></td>
<td>GTP Source IP Address, GTP TEID, GTP-U Destination IPv4, GTP-U Source IPv4,</td>
</tr>
<tr>
<td></td>
<td>VN TAG Destination IP, VN Tag Source IP, VxLAN VNID</td>
</tr>
<tr>
<td><strong>Header</strong></td>
<td>Gen1 - MAC, IP, L2, L3, L4, TCP, UDP, LLC</td>
</tr>
<tr>
<td></td>
<td>Gen 2 - MAC, L2, L4, TCP, UDP, L2 with VLAN, Unknown L3, Known Non-IP, IPv4,</td>
</tr>
<tr>
<td></td>
<td>IPv6, MPLS Header, Unknown L4, GRE</td>
</tr>
<tr>
<td><strong>Offset</strong></td>
<td>Specify an offset from the beginning of the header window with the desired</td>
</tr>
<tr>
<td></td>
<td>hexadecimal data pattern to be compared to receive packets (range: 0-63).</td>
</tr>
<tr>
<td><strong>Value</strong></td>
<td>Valid IPv4/IPv6 address or a value from 0 to 8 hexadecimal digits.</td>
</tr>
<tr>
<td><strong>Mask</strong></td>
<td>(Optional) Valid IPv4/IPv6 mask or a value from 0 to 8 hexadecimal digits.</td>
</tr>
</tbody>
</table>

**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.

- Clone 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
- 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 Ports Image]

Select Groups

![Select Groups Image]
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 its 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
  - pfSMesh-enabled triggers that are visible to all nodes in pfSMesh

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

- Disbale: 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 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.

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 4.3 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.
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.

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 **Save As > New Topology**.

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

The following procedure may be used to import a PFS’ existing configuration into one or more 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. Decide how many user topologies should be created; see **User Topologies on page 4-1** for more information.
3. Perform the Save-As operation on the Device topology once for each User Topology to be created. For example, if you want a PFS’ traffic maps to be split among 3 new user topologies, perform the Save-As operation 3 times.
4. Edit each new user topology to remove duplicate connections. For example, one might leave connections 1-4 only on topology A, connections 5-8 only on topology B, etc. This step will involve the following steps (see the rest of this chapter for details on each step):
   - a. Saving each user topology as a new version
   - b. Editing the new version to remove the duplicate connections
   - c. Finally, publishing the new topology

---

Create a New Topology

From the interface screen, select Deploy then click on Topology - a New Topology screen displays.
Enter a name for the new topology 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

- Selected Topology
- Return to Topology Lists
- Save As
- Publish
- Delete Topology
- Add / Create
- + / - Zoom (Double-click to Reset)
- Topology Layers
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.
Flow Nodes

![Flow Nodes Diagram]

- Filter Resources
- Edit
- Remove Node
- Info

Deploy Lifecycle
**Port Groups**

- **Remove from Topology**
- **Information**
- **Source Group**
  - Click on Ports to Expand Port List
- **Destination Group**
- **Load Balance Group**
- **Expanded Port List**
- **Click to Collapse Port List**
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.
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.

**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.

- Connection is Established and Group is visible (line is solid and green)
- Groups are Published and Visible to pfsMesh
- Published Connection with pStack Connectivity Issue (Solid Red Line)
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.
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 **Save As** icon and selecting **New Topology**. Enter a name for the topology plus any optional information. Click on the **Save As** check mark to save the topology. To save (clone) the topology as a different version, select **New Version**.

![Save As dialog]

### 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.

![Topologies list]

### 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**.

![Delete Topology]

---

**Deploy Lifecycle**

4-15
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 Perspective > Trigger on page 3-74, 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.
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 Filter Resources menu option. Clicking on the Filter Resources icon opens a new information screen displaying the current configuration of the selected filter.
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 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

Selected Inline Topology
Return to Inline Topology Lists

Save As
Publish
Delete Topology
Add / Create

+ / - Zoom (Double-click to Reset)
Toggle Filters
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.

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 from inline 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 Inline 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 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.
This chapter describes the switch and port monitoring functions of PFS Fabric Manager. Monitor allows 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.
  - Part Number - Vendor part number.
  - Product ID - Blade Identifier
- 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 ID
- Port Name
- 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 (Xcvr Model) - Transceiver model number.
- Transceiver Type (Xcvr Type) - Transceiver type (e.g. 10GBase-SR or 1G/10GBase -SR)
- Transceiver State (Xcvr State) - Transceiver operating status and specifications (i.e., manufacturer / model number, transceiver type, firmware version).
- 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.

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.
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.

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 Group 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 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 Alarms, Audit Log or Syslog History.

- **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 deselecting the Acknowledge field.
  - View the times of the displayed events and alarms in the user's time zone.

- View the expiration date of the trial license on the front page of the application, by clicking on Critical/Warning Messages.
• Audit Log:
  – Displays all of the actions performed on the device.

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

<table>
<thead>
<tr>
<th>Profile Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td></td>
</tr>
<tr>
<td>Local Port</td>
<td></td>
</tr>
<tr>
<td>Chassis ID</td>
<td>Identifies the device</td>
</tr>
<tr>
<td>Hold Time</td>
<td></td>
</tr>
<tr>
<td>System Name</td>
<td>Displays given name for the device</td>
</tr>
<tr>
<td>System Desc</td>
<td>Displays version of the software</td>
</tr>
<tr>
<td>Management Address</td>
<td>Displays the IP or MAC address of the device</td>
</tr>
<tr>
<td>Remote Port</td>
<td></td>
</tr>
<tr>
<td>Port Description</td>
<td>Displays details about the port</td>
</tr>
</tbody>
</table>

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.
Monitor Search Filter

From Monitor Lifecycle, using the same port search criteria described in Perspective > Trigger on page 3-74, 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 (refer to Monitor Palette on page 6-13).
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:

![Error Message]

Limit Reached!

You have reached the maximum number of undocked monitors palettes.

OK
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 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 PFM’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 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.

**Note:** A restore operation can fill up the disk, if the disk space is almost full. The user should check the disk space, for each managed device, before performing a restore operation.
Certificates

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

- 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.

- 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.
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 from 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 device's 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. |

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.

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. The panel also allows for the deletion of user config files and permits new configs to be uploaded to the device.

Software/Firmware

The Software/Firmware feature displays the software and firmware that is currently installed on the PFS Fabric Manager Central server and Managed 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.
**Software Management**

Software Management allows the user to determine the current software versions of PFS Fabric Manager and PFOS operating on the central server and managed devices. Uploading and installing updated software versions to the system are also performed from Software Management.

*Note: Software downgrades are not supported at this time.*

Clicking on **Software Management** displays the current and standby software installed on the PFS Fabric Manager server and managed devices. Clicking on the **Install** icon (under Actions) 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 **Managed Devices** 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.
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 Authentication Order, Authentication Servers, Roles and User Management of the PFS Fabric Manager.

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, 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 (TACACS, RADIUS, and Local) 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.
**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.

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

---

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host / IP Address</td>
<td>IPv4/IPv6 address or a fully qualified domain name of the RADIUS server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port for access to the server (default 0).</td>
</tr>
<tr>
<td>Key</td>
<td>AES encrypted string to authenticate to the server.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Time after which requests to the server time out (default 30 seconds).</td>
</tr>
<tr>
<td>Retransmit</td>
<td>Number of times PFOS attempts to contact the TACACS server (default 3).</td>
</tr>
</tbody>
</table>
Password Policy

To add a new Password policy, select Settings > Access Control > Password Policy. From the Password Policy tab, click on the Edit icon to access the Password Policy configuration screen. Specify the settings based on the users password requirements.

The user will be prompted for a new password if the current password has expired or no longer complies with the password policy.

**Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expiration, day(s)</td>
<td>Number of days in which the password will expire.</td>
</tr>
<tr>
<td>Minimum Password Requirements</td>
<td></td>
</tr>
<tr>
<td>Length</td>
<td>Minimum password length.</td>
</tr>
<tr>
<td>Upper Case</td>
<td>Minimum number of upper case characters allowed.</td>
</tr>
<tr>
<td>Lower Case</td>
<td>Minimum number of lower case characters allowed.</td>
</tr>
<tr>
<td>Numerical</td>
<td>Minimum number of numerical characters allowed.</td>
</tr>
<tr>
<td>Special</td>
<td>Minimum number of special characters allowed.</td>
</tr>
<tr>
<td>Login Restrictions</td>
<td></td>
</tr>
<tr>
<td>Session Limit</td>
<td>Enable / Disable the session limit.</td>
</tr>
</tbody>
</table>

*Note:* Click on View Password Policy to view the current password policy.
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
To assign roles via TACACS+ or RADIUS, users must be configured in the TACACS+ or RADIUS server with an 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.

Sample Configuration for Authorization with RADIUS

This example shows a Cisco ACS RADIUS Server configuration. It is independent of PFS Fabric Manager, but assists with troubleshooting.

This example shows the “admin” role being set. Change to “user” for the user role.
Sample Configuration for Authorization with TACACS+

This example shows a "tac_plus" Server configuration. It is independent of PFS Fabric Manager, but assists with troubleshooting.

```
group = myadmin
  default service = permit
  service = shell
  default command = permit
  default attribute = permit
  set priv -l = 15
  set acl = [groups=admin]
}
group = user
  default service = permit
  service = shell
  default command = permit
  default attribute = permit
  set priv -l = 15
  set acl = [groups=user]
```

Setting Authorization for the Admin Role

Setting Authorization for the User Role

User Management

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.
Delete User
You can delete a user by checking the Delect User icon located on the user account window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter a user name (e.g., admin, admin-1, user, user-1)</td>
</tr>
<tr>
<td>Password</td>
<td>Assign a login password (minimum length of 8 characters and must contain at least 1 uppercase and 1 lowercase character).</td>
</tr>
<tr>
<td>Confirm</td>
<td>Confirm the assigned password</td>
</tr>
<tr>
<td>First Name</td>
<td>Enter user first name</td>
</tr>
<tr>
<td>Last Name</td>
<td>Enter user last name</td>
</tr>
<tr>
<td>Email</td>
<td>Enter users email address</td>
</tr>
<tr>
<td>Selected Roles</td>
<td>Role or roles to be assigned to the new user</td>
</tr>
</tbody>
</table>
My Account

Reset Password
You can reset a user's 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.

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 7-8
- TACACS Server - Refer to Configuring TACACS on page 7-9
- RADIUS Server - Refer to Configuring RADIUS on page 7-11
- Password Policy - Refer to Password Policy on page 7-12
**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 or OS Upgrade)

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). These instructions can also be used as part of an OS upgrade for an existing NMS, see Upgrading the Operating System on the PFS Fabric Manager NMS (CentOS 6 to CentOS 8) on page A-4.

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 it can be transferred to a DVD for installation 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.

Note: Servers or VMs must be configured to use BIOS (rather than UEFI/EFI) before attempting to install PFS Fabric Manager.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>16 GB</td>
<td>32 GB</td>
</tr>
<tr>
<td>Disk Space</td>
<td>1 TB</td>
<td>2 TB</td>
</tr>
<tr>
<td>CPU</td>
<td>6 cores or vCPUs @ 2.1 GHz</td>
<td>8 cores or vCPUs @ 2.1 GHz</td>
</tr>
<tr>
<td>Required Drives</td>
<td>DVD</td>
<td>DVD</td>
</tr>
<tr>
<td>Network Cards</td>
<td>1 Gbps Ethernet</td>
<td>1 Gbps Ethernet</td>
</tr>
</tbody>
</table>

Note: System disk space should be in a single logical disk. Use of RAID for redundancy is recommended in physical servers.

Server Operating System

The CentOS 8 Linux 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 CentOS 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: 
   *CentOS-8.1_pfm-nms8-<version>* from the [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: from your local PC, burn the PFS Fabric Manager ISO image file to a DVD.

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 or DVD image in order to begin re-imaging/installing the required CentOS platform.

a On a physical server: place the DVD into the server’s DVD drive tray, then reboot the server.

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 CentOS 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 Chrome browser, enter the assigned IP address of the nGenius PFS Fabric Manager Server (e.g., `https://nnn.nn.nn.nnn`).
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 (refer to Software Management on page 7-7) 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 to CentOS 8)

Please follow these steps to upgrade the Operating System on the PFS Fabric Manager NMS.

1. Upgrade the NMS to 6.0.3, refer to Upgrading PFS Fabric Manager (NMS) on a Central Server in the nGenius® PFS Fabric Manager Software 6.0.3 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 7-1 for more information).
4. Using the PFM installation disk/ISO, install CentOS 8 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 7-1 for more information).
7. If a TLS certificate for the NMS was installed on the old (CentOS 6) NMS, it must be reinstalled (refer to Certificates on page 7-2 for more information).
8. 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 nGeniusONE 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.

- iDRAC Requirements
- iDRAC Settings in System BIOS
- Connecting to the iDRAC Interface
- Launching the iDRAC Virtual Console
- Using Virtual Media for Software Updates
- Using the Virtual Console for Software Updates
- Other iDRAC Features

For complete details on the controller’s features and functions, refer to the Dell Remote Access Controller Documentation on the Dell website.

- Dell R740 (iDRAC9)
- Dell R730 (iDRAC8)

Using the Dell™ Remote Access Controller

The nGeniusONE 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).
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

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>22*</td>
<td>Secure Shell (SSH)</td>
</tr>
<tr>
<td>23*</td>
<td>Telnet</td>
</tr>
<tr>
<td>80*</td>
<td>HTTP</td>
</tr>
<tr>
<td>443*</td>
<td>HTTPS</td>
</tr>
<tr>
<td>623*</td>
<td>RMCP/RMCP+</td>
</tr>
<tr>
<td>5900*</td>
<td>Virtual Console keyboard/mouse, Virtual Media Service, Virtual Media Secure Service, and Virtual Console video</td>
</tr>
</tbody>
</table>

Table B–2 iDRAC Client Ports

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>SMTP</td>
</tr>
<tr>
<td>53</td>
<td>DNS</td>
</tr>
<tr>
<td>68</td>
<td>DHCP-assigned IP address</td>
</tr>
<tr>
<td>69</td>
<td>TFTP</td>
</tr>
<tr>
<td>162</td>
<td>SNMP trap</td>
</tr>
<tr>
<td>636</td>
<td>LDAPS</td>
</tr>
<tr>
<td>3269</td>
<td>LDAPS for global catalog (GC)</td>
</tr>
</tbody>
</table>

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. However, if you find that you are unable to log in to the iDRAC UI with the default root password of netscout1, the default password may have been reset to calvin during a firmware factory reset. 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 nGeniusONE 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.

![System Setup Main Menu](image)

*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
   - **Enter 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.

![Image of iDRAC Settings](image)

**Figure B-3** iDRAC BIOS Level Configuration

### Changing the iDRAC Password

The default iDRAC user is root and the password is netscout1. However if a firmware factory reset occurs, the password could have been reset to the Dell default, calvin. If you cannot connect with your original password or with “calvin,” you may need 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.

![Image of User Configuration](image)

**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](image)

**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” and the default password is “netscout1.” NETSCOUT SYST recommends changing these defaults as soon as possible. If the default password of “netscout1” does not work, try “calvin” instead. This is the Dell default password. NETSCOUT SYST changes this to “netscout1” before shipping your unit. You can reset this password in BIOS.

After you have successfully logged in, the main web-based interface displays.

![Main Menu of the iDRAC Web Interface](image)

**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 nGeniusONE 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.

---

Using Virtual Media for Software Updates

You can use the iDRAC Virtual Console’s Virtual Media option to upgrade the application software or reimagine the nGeniusONE 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 reimaging 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 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 a local CD/DVD drive or ISO to function as a Virtual Medium on the remote nGeniusONE 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)]
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.

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.

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 nGeniusONE Server Hardware from Virtual Console](image)

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**

For nGeniusONE Server Hardware with an attached CD/DVD drive or for software updates that can be run from the system command line (bin files, rpm files), use of the Virtual Media option is not necessary. In these cases you can use the iDRAC Virtual Console like a local console to run the installers.

You can either insert the CD/DVD into the remote system or 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 or from an Application CD.
2. Insert the CD/DVD into the drive, if available on your server hardware, or 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.