

nGenius® PFS Fabric Manager Software 6.5.1

Administrator Guide

733-1957 Rev. B

NETSCOUT SYSTEMS, INC.

Westford, MA 01886
Telephone: 978.614.4000
Fax: 978.614.4004

Web: <http://www.netscout.com>



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

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

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

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

NETSCOUT SYST, INC

Open Source Code Request

310 Littleton Road

Westford, MA 01886

Attn: Legal Department

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

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifications to this product not authorized by NETSCOUT could void the FCC approval and terminate your authority to operate the product. Please also see NETSCOUT's Compliance and Safety Warnings for NetScout Hardware Products document, which can be found in the documents accompanying the equipment, or in the event such document is not included with the product, please see the compliance and safety warning section of the user guides and installation manuals.

No portion of this document may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine form without prior consent in writing from NETSCOUT. The information in this document is subject to change without notice and does not represent a commitment on the part of NETSCOUT.

The products and specifications, configurations, and other technical information regarding the products described or referenced in this document are subject to change without notice and NETSCOUT reserves the right, at its sole discretion, to make changes at any time in its technical information, specifications, service, and support programs. All statements, technical information, and recommendations contained in this document are believed to be accurate and reliable but are presented "as is" without warranty of any kind, express or implied. You must take full responsibility for their application of any products specified in this document. NETSCOUT makes no implied warranties of merchantability or fitness for a purpose as a result of this document or the information described or referenced within, and all other warranties, express or implied, are excluded.

Except where otherwise indicated, the information contained in this document represents the planned capabilities and intended functionality offered by the product and version number identified on the front of this document. Screen images depicted in this document are representative and intended to serve as example images only.

Copyright 2009-2024 NETSCOUT Systems, Inc. All rights reserved.

Contacting NETSCOUT SYST, INC.

Customer Care

The best way to contact Customer Care is to submit a Support Request:

<https://my.netscout.com/mcp/Support/Pages/Home.aspx>

Telephone: US Toll Free: **+1-888-357-7667**; International Toll Free: **+800 4764 3337**.

Phone support hours are 8 a.m. to 8 p.m. Eastern Standard Time (EST).

When you contact Customer Care, the following information can be helpful in diagnosing and solving problems:

- Your organization's name, contact name, phone number, and location of system
- NETSCOUT Packet Flow Switch model number
- PFS Fabric Manager Software version
- Detailed description of the problem, or source of the problem based on its symptoms
- Error text messages, supporting screen images, logs, and error files, as appropriate

Sales

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

Table of Contents

Chapter 1 About This Document and Introduction

Related Documentation	1-1
Contacting NETSCOUT Customer Care	1-1
NETSCOUT Web Site	1-1
PFS Fabric Manager Overview	1-2
NMS and PFS Networking Requirements	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	2-6
Bringing a PFS into Central Management	2-7
Connecting to the PFS from the NMS	2-7
Configuring the NMS address in the PFS	2-8
Accepting Switches into Central Management	2-9
Importing the PFS Configuration into the NMS	2-9
Removing a PFS from Central Management	2-9
Issues	2-10
Alarms and Severities	2-11
Viewing Events	2-13
Changing the Theme	2-14
Documentation	2-14
End User License Agreement	2-15
Logout of PFS Fabric Manager	2-16

Chapter 3 Configure Lifecycle

Discover Switches	3-1
Device > Switch Acceptance	3-2
Perspective Menus	3-3
Rebooting Selected Management Cards/Entire Chassis	3-4
Perspective > Device	3-5
Active	3-5
Active Switch Sub-Menu	3-5
Reconnect Switch	3-5
Delete Switch	3-6
Blade Sub-Menu	3-6
Clear Blade	3-7
Reset Blade	3-7
Shutdown Blade	3-7
Line Card Display Details	3-8
Port Display Details	3-9
Line Card Port Indicators	3-9

Port Flapping State	3-10
Discovered	3-11
Unmanaged	3-12
PFX	3-12
Configure / Update Devices	3-12
Interfaces > Network Information	3-14
Profile > Default > Basic Information	3-15
Profile > Default > Service Profile	3-16
Profile > Default > Time Sources	3-17
Profile > Default > Logging	3-18
Profile > Default > Logging (Secure Syslog)	3-19
Profile > Default > SNMP Feature	3-20
Profile > Default > Features	3-21
Profile > Default > Authentication Order	3-22
Profile > Default > TACACS Server	3-23
Profile > Default > RADIUS Server	3-24
Profile > Default > LDAP Server	3-25
Profile > Default > SAML2 Server	3-26
Transceiver Details	3-27
Blade/Line Card Control	3-27
Locate Me	3-27
Connect to the Device	3-28
MIB File Viewing	3-28
External PowerSafe TAPs Configuration	3-29
PFX > Basic Information	3-30
Adding a PFX Device	3-31
Managing Database Sync (PFS6010 Devices Only)	3-32
Configure Search Filter	3-32
Port Perspective	3-32
Perspective > Port	3-33
Basic Information	3-34
Port Types	3-35
Trigger Based Alarms Port Feature Profile	3-36
Tunnel Termination Port Feature Profile	3-38
IP Tunnel Termination	3-39
Tunnel Termination Considerations And Limitations	3-40
VN, VLAN, VXLAN, MPLS Tag Stripping Port Feature Profile	3-41
VN, VLAN, VXLAN, MPLS Tag Stripping Port Feature Profile (UI for 5000/7000 Series Platforms)	3-41
VN, VLAN Tag Stripping Port Feature Profile (UI for 6000 Series Platforms)	3-42
Monitor_Stamping (PFS 6000 Series Only)	3-44
Port Properties from Deploy Lifecycle	3-45
Configure > Port on Topology Association	3-46
Configure > Inline Port	3-46
Perspective > Group	3-47
Basic	3-47
Ports	3-48
Inline Network Group Ports	3-49
Inline Monitor Group Ports	3-50
Additional Groups	3-50
Configuring a Destination Group as a Remote Monitor Group for pfsMesh	3-51
Removing a Load Balancing Group from a Remote Monitor Group	3-52
Port Group Sub-Menu	3-52
Configure > Group on Topology Association	3-53
Perspective > Profile	3-54
Port Profile	3-54
Creating a Port Profile	3-55
Port Profile Sub-Menu	3-56
Creating a Port Feature Profile	3-57
Tunnel Termination Profile	3-58
Egress VLAN Action Profile	3-58

Creating an Egress VLAN Action Profile	3-58
Deduplication Profile (PFS 6000 Series Only)	3-60
Packet Slicing Profile (PFS 6000 Series Only)	3-61
Extended Load Balancing Profile (PFS 6000 Series Only)	3-66
Protocol Stripping Profile (PFS 6000 Series Only)	3-68
Group Profile	3-70
Creating a Group Profile	3-71
Tunnel Profile	3-72
Creating a Tunnel IP Interface Profile	3-72
Creating a Tunnel VxLAN Profile	3-73
Creating a Tunnel GRE Profile	3-74
Mirror Session Profile	3-75
Creating a Mirror Session Profile	3-75
Perspective > Filter	3-78
Creating a Filter	3-78
Define the Filter Requirements	3-79
Packet	3-79
Protocol	3-81
Port	3-82
Custom Offset	3-82
Custom	3-83
Saving the New Filter	3-84
Editing Filter Properties	3-85
Filter Sub-Menu	3-86
Perspective > Trigger	3-87
Timer Settings	3-87
Active set time	3-87
Active clear time	3-87
Select Ports or Groups	3-88
Select Ports	3-88
Select Groups	3-88
Trigger Actions	3-89
Send Notifications	3-89
Force Port Link Down	3-89
Trigger Types	3-89
Linkstate Trigger Type	3-89
Specific Options	3-89
BandwidthUtilization Trigger Type	3-90
Specific Options	3-90
Overflow Trigger Type	3-91
HealthCheck Trigger Type	3-91
Specific Options:	3-91
Combo Trigger Type	3-92
Specific Options:	3-92
pfsMesh Option	3-95
Select Trigger Policies	3-95
Configuration	3-96
Port Link State	3-96
Monitoring	3-97
Topology	3-97
Publication and Learning	3-98
Publication	3-98
Learning	3-98
Topology Mismatch	3-99
Accept Mismatch Workflow	3-99

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	4-3
Topology Screen / Features	4-4
Populating a Topology	4-5
Port Nodes / Port Groups / Filter Details	4-5
Port Nodes	4-5
Port Node Quick Info	4-6
Flow Nodes	4-6
Flow Node Quick Info	4-6
Port Groups	4-7
Port Group Quick Info	4-8
Making Connections	4-8
Flow Precedence	4-9
Adding Port Groups	4-10
Adding Drop Packets	4-11
Adding Remote Monitor Groups	4-11
Enabling/Disabling Local Configuration	4-13
Local vs. Global	4-15
Publication	4-16
Conflicts and Validation	4-16
Upgrade and Down-rev support	4-16
Topology Node Statistics	4-17
Statistics Toggle	4-17
Topology Statistics Expand Button	4-17
Mirroring on Deploy Lifecycle	4-18
Topology Notes	4-19
Topology vCards	4-19
New Topology and Save As	4-20
Topology Canvas	4-21
Publishing a Topology	4-22
Unpublish a Topology	4-23
Validate a Topology	4-23
Schedule a Topology	4-24
Accept a Mismatched Topology	4-24
PFSMesh Topology - Items to Remember	4-25
Save a Topology	4-25
Topologies and Versions	4-25
Viewing List of Topologies	4-26
Delete a Topology	4-26
Topology Layers	4-26
Topology Search	4-27
Topology > Port on Topology Association	4-28
Topology > Port on Filter Resources	4-29
Topology > Tabular View	4-30
Deploy Lifecycle	4-30
Selecting Columns	4-30
Editing Topology and Flows	4-31
Adding traffic maps	4-31
Ports and Groups	4-32
Topology Subsets	4-33
Tabular Topology Statistics	4-34
Topology > Configuration Changes Scheduling	4-35
Topology Tab	4-35
Schedule Tab	4-35
Managing Scheduled Jobs	4-35
Creating a Scheduled Job	4-36
Editing a Scheduled Job	4-38

Viewing a Scheduled Job Status	4-38
Topology > Alarm Indicators	4-39

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	5-5
Flow Nodes	5-6
Inline Topology Publication	5-7
Port Groups	5-7
Filters	5-7
Tools	5-7
Toolchain (one per topology)	5-7
Inline Traffic Maps	5-7
Inline Topology Versioning	5-7
Learning	5-7

Chapter 6 Monitor Lifecycle

Device Status	6-1
Blade Status	6-1
Port Monitor	6-3
Port Status Indicators	6-3
Network Statistics	6-4
Deduplication	6-5
Flow Ports	6-6
Control Packets	6-7
nGeniusOne Status	6-8
pfsMesh	6-8
Viewing Combination of Managed / Unmanaged Devices	6-10
PFSMesh - Refresh Display	6-10
Events	6-11
Link Layer Discovery Protocol (LLDP)	6-13
Dashboard	6-14
Monitor Search Filter	6-16
Undocking Monitor Palettes	6-17
Undocking Limits	6-18

Chapter 7 System Settings

System Configuration	7-1
System	7-1
ServiceNow	7-2
Alarm Notifications	7-3
nGeniusOne	7-6
System Administration	7-7
Backup/Restore	7-7
Backup/Restore Dashboard	7-7
Backups Tab	7-7
Restores Tab	7-9
Schedule Tab	7-9
Manual Backup/Restore	7-11
Banner	7-12

Certificates	7-16
Device Summary Tab	7-16
Inventory Tab	7-17
High Availability	7-18
Active/Standby Role Management	7-21
Virtual IP	7-21
Host IP	7-21
HA Role	7-21
Synchronization States (As seen on NMS HA Status page)	7-22
Switchover Rules	7-22
Switchover from Active	7-22
Switchover from Standby	7-22
Going Standalone:	7-23
IP Tables	7-23
Adding Rules	7-24
Editing Rules	7-24
Bulk Publishing	7-25
Device Details	7-25
Labels	7-25
Labeling Switches	7-25
Labeling Ports	7-26
Labeling Topologies	7-27
Global Filtering	7-28
Licenses	7-28
NTP	7-29
SNMP	7-30
Power Usage	7-34
Switch Power Consumption	7-34
Switch Power Consumption Real Time Statistics	7-34
Port Laser TX Setting	7-34
SSH Known Hosts	7-37
Syslog Servers	7-37
Storage	7-40
Switch Configs	7-40
Software/Firmware	7-42
Uploading / Upgrading PFOS Firmware	7-46
Access Control	7-47
User Management	7-47
My Account	7-47
All Users	7-47
Add Users	7-47
Delete User	7-48
Reset Password	7-48
Access Policy	7-49
Client IP Lockout	7-49
Configuration	7-49
Authentication Order	7-51
Configuring TACACS	7-52
Configuring RADIUS	7-54
Configuring LDAP	7-55
Configuring SAML2 (NMS only)	7-56
Roles Based Access Control (RBAC)	7-57
Sample Configuration for Authorization	7-59
My Account	7-61
Managed Devices	7-61

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

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 6/8 to Oracle Linux 9)	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
Monitoring Server Health	B-15

Appendix C Switch RMA Replacement

Fabric Manager Switch RMA Replacement	C-1
Fabric Manager Switch RMA Replacement Prerequisites	C-1
Fabric Manager Switch RMA Replacement Verification	C-1
Possible issues and workarounds:	C-1

Revision History

Date	Revision	Description
June 2024	PFS FM 6.5.1 Rev B	<ul style="list-style-type: none"> Added the new section Topology Notes. Updated SNMP to include SNMP Traps and UI improvements.
April 2024	PFS FM 6.5.0 Rev A	<ul style="list-style-type: none"> NMS and PFS Networking Requirements moved from PFS Fabric Manager Release Notes to this document. Updated System Settings to include references to the new SNMP and Power Usage features. Updated Alarms and Severities to include the alarms for the new Watermark feature. Updated Profile > Default > Features to include the new Slicing feature. Added the new section Mirror Session Profile in Perspective > Profile. Updated Topology Node Statistics section. Added the new section Mirroring on Deploy Lifecycle. Updated Dashboard to include reference to the new Power Consumption feature. Updated System in System Administration to include references to the new Upper/Lower Watermark limits. Added the new section SNMP in System Administration. Added the new section Power Usage in System Administration. Updated Appendix A, "Installing PFS Fabric Manager Central Server (Software-Only Version)" to include the section Upgrading the Operating System on the PFS Fabric Manager NMS (CentOS 6/8 to Oracle Linux 9). Updated Appendix B, "Configuring and Troubleshooting the Server Remotely" to reference the new R760 appliance and remove references to using a DVD drive.

Chapter 1

About This Document and Introduction

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



IMPORTANT

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

Related Documentation

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

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

Contacting NETSCOUT Customer Care

Customer Care:

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

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

When contacting Customer Care, the following information can be helpful in diagnosing and solving problems:

- Your organization's name, contact name, phone number, and location of system
- NETSCOUT Packet Flow Switch model number
- PFS Fabric Manager Software version
- Detailed description of the problem, or source of the problem based on its symptoms
- Error text messages, supporting screen images, logs, and error files, as appropriate

NETSCOUT Web Site

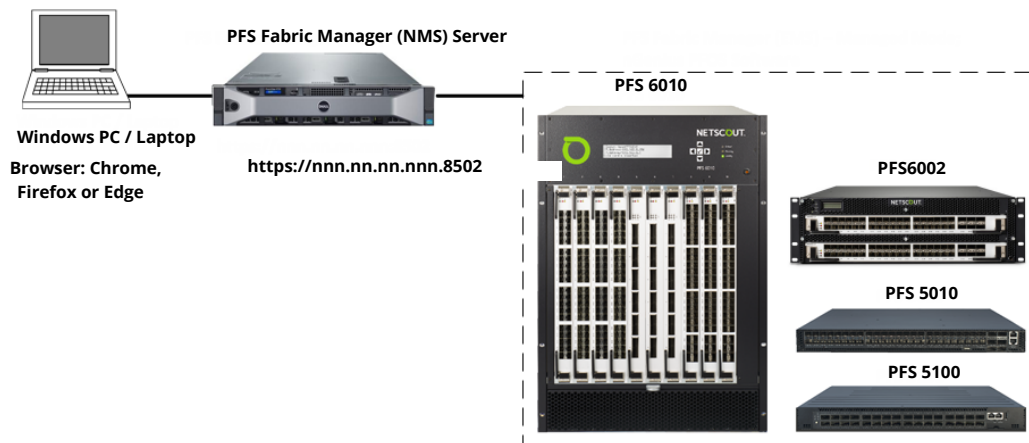
Visit our Web site at <http://www.netscout.com>.

PFS Fabric Manager Overview

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

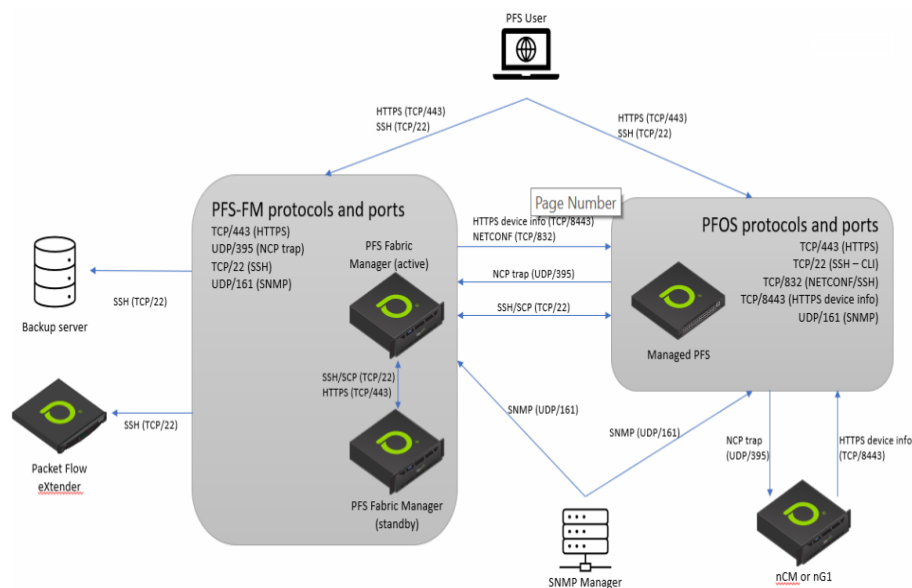
PFS Fabric Manager runs on a central server (or VM) connected to the networked PFS switches running PFOS. The PFS Fabric Manager central server is also called the NMS.

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



NMS and PFS Networking Requirements

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



Note: Multiple optional remote servers are not shown.

NMS Ports

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

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

Managed PFS Ports

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

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

Chapter 2

Login and Setup PFS Fabric Manager

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

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

Starting / Login to PFS Fabric Manager

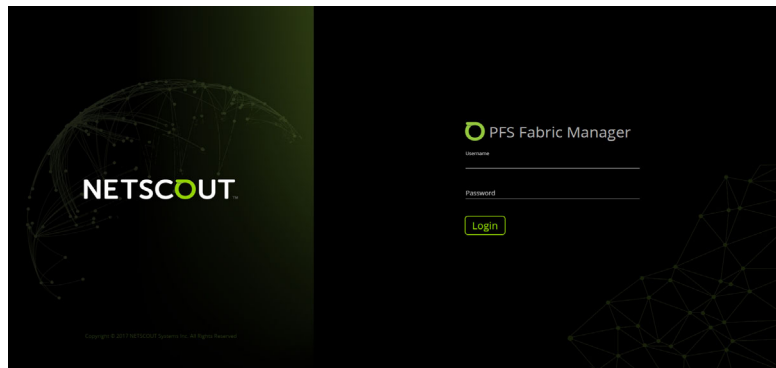
PFS Fabric Manager can be started / logged in from the PFS Fabric Manager (NMS) server.

PFS Fabric Manager (NMS) Server

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

Login to PFS Fabric Manager

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



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

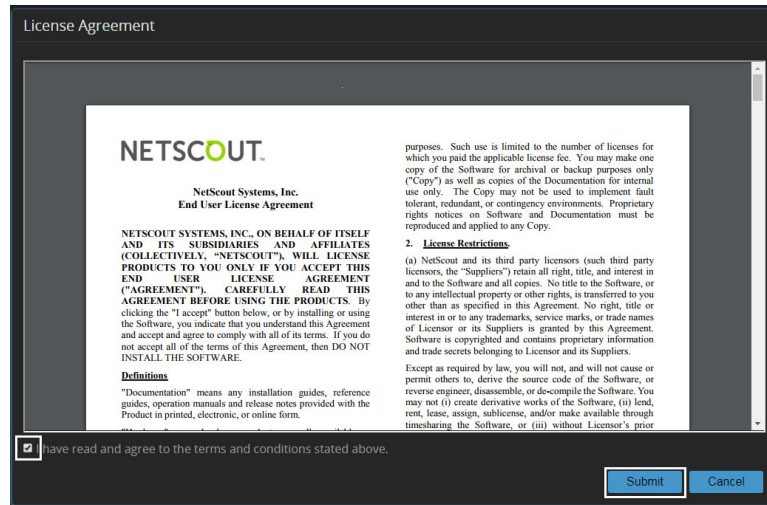
Important: The first time the admin user logs in to a Fabric Manager appliance, the user will be required to change their password.

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

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

6 Click **Login**.

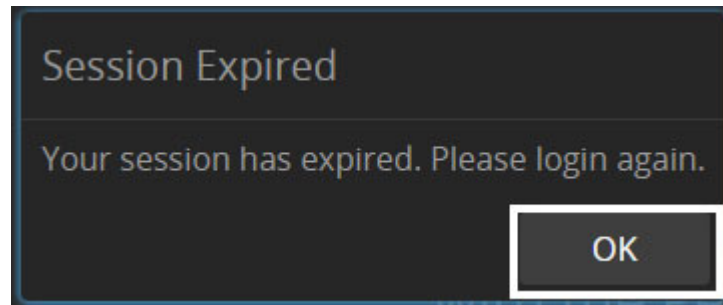
7 Click on the End User License Agreement acceptance statement check box then click **Submit**.



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

PFS Fabric Manager Session Expiration

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



PFS Fabric Manager Interface Screen

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



Configure Lifecycle

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

DEVICE

Search

6 ACTIVE

0 DISCOVERED

0 UNMANAGED

0 PFX

DEVICE

CONFIGURE

DEPLOY

INLINE

MONITOR

ACTIVE Switches(6)

Reconnect

Delete

PFS5010_6
172.22.38.185

Name: PFS5010_6

Model: PFS 5010

Software: VXOS 6.3.0.61

Labels: 5010, RMA, 7K, VM

PFS5010-Auto
172.22.38.37

Name: PFS5010-Auto

Model: PFS 5010

Software: VXOS 6.3.0.61

Labels: 5010, 7K, Automation, Rack-53, Physical(BEC)

PFS5010-BEC-LABS
172.22.38.103

Name: PFS5010-BEC-LABS

Model: PFS 5010

Software: VXOS 6.3.0.61

Labels: 5010, 7K, Rack-51, Physical(BEC)

PFS5041-32D-BEC-38dot36
172.22.38.36

Name: PFS5041-32D-BEC-38dot36

Model: PFS 5041-32D

Software: VXOS 6.3.0.61

Labels:

PFS5110-BEC-LABS
172.22.38.104

Name: PFS5110-BEC-LABS

Model: PFS 5110

Software: VXOS 6.3.0.61

Labels: 7K, Physical(BEC), 5110, Rack-52

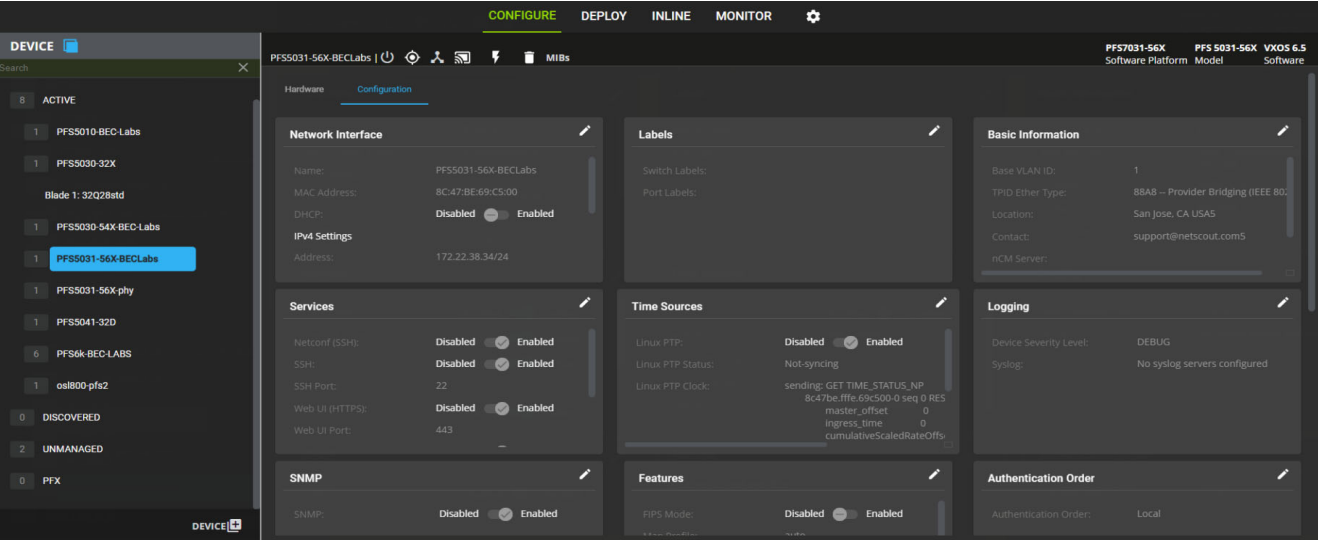
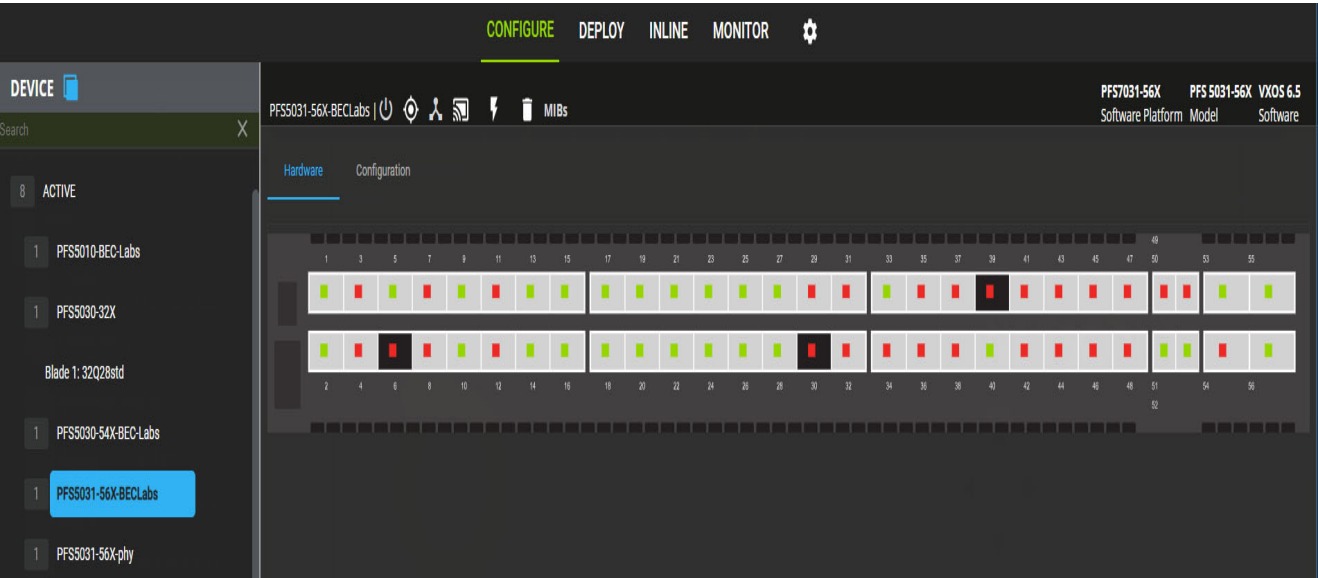
PFS6010
172.22.31.208

Name: PFS6010

Model: PFS 6010

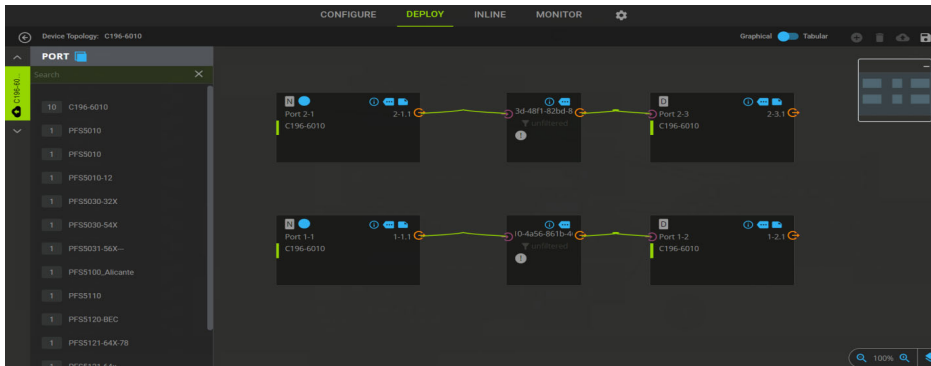
Software: VXOS 6.3.0.61

Labels: VM, 6010



Deploy Lifecycle

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



Graphical

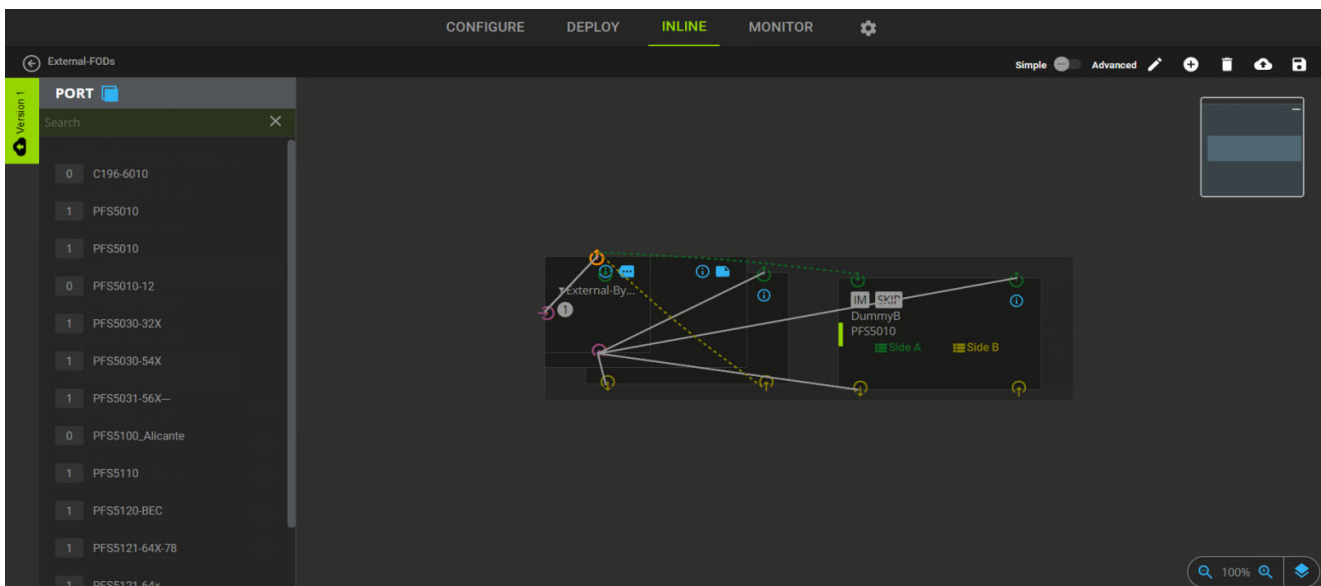
The screenshot shows the 'Tabular' view of a topology. It features a table with columns for MAP NAME, ISSUES, DEVICE, PRECEDENCE, PRIORITY, MAP STATE, FILTER, INPUT PORT, OUTPUT PORT, LOAD BALANCE GROUP, LBC PROFILE, DESCRIPTION, and ACTIONS. The table lists three entries for PFS5010.

MAP NAME	ISSUES	DEVICE	PRECEDENCE	PRIORITY	MAP STATE	FILTER	INPUT PORT	OUTPUT PORT	LOAD BALANCE GROUP	LBC PROFILE	DESCRIPTION	ACTIONS
PFS5010		PFS5010	1	-1	Enabled	unfiltered	Port 8-16	Port 8-14				
PFS5010		PFS5010	1	-1	Enabled	unfiltered	Port 8-18	Port 9-14				
PFS5010		PFS5010	1	-1	Enabled	unfiltered	Port 8-14	Port 8-12				

Tabular

Inline Lifecycle

Inline Lifecycle allows creating, versioning, and publication of Inline topologies. See [Inline Lifecycle on page 5-1](#) for details.



Monitor Lifecycle

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

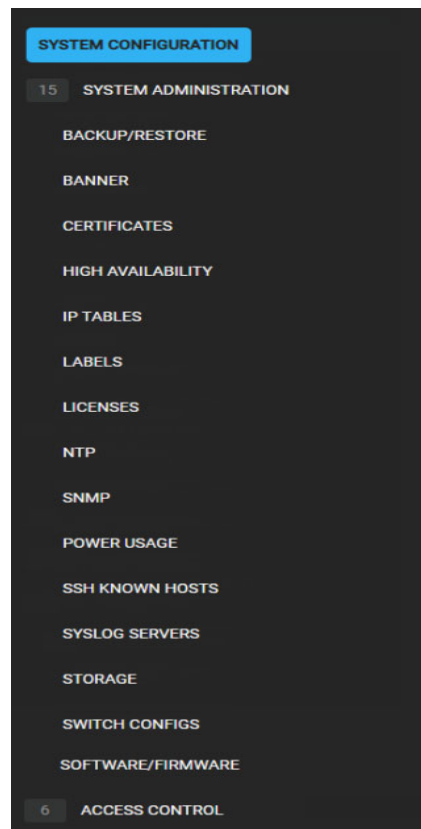
Port Statistics PFS5010-BEC-LABS Slot 1: 48S6Qstd											
Auto Refresh (in seconds): 5											
Status Network Deduplication Flow Ports Control Packet nGeniusOne Status											
PORT NAME	PORT ID	CLASS	SPEED	LINK STATE	PWR RX (DBM)	PWR TX (DBM)	XCVR MODEL	XCVR TYPE	XCVR SUPPLY VOLTAGE	XCVR TEMPERATURE	XCVR BIAS CURRENT
Port 1-1	1-1	pStack	10000	up	-N/A-	-N/A-	Amphenol 624380003	10G DAC 3M	-N/A-	-N/A-	-N/A-
Port 1-2	1-2	Network	10000	up	-N/A-	-N/A-	Amphenol NDBBDA-C103	10G DAC 3M	-N/A-	-N/A-	-N/A-
Port 1-3	1-3	Network	10000	down							
Port 1-4	1-4	Network	10000	up	-N/A-	-N/A-	DELL L56SF018-SD-R	10G DAC 3M	-N/A-	-N/A-	-N/A-
Port 1-5	1-5	Network	10000	down							
Port 1-6	1-6	Network	10000	down							
Port 1-7	1-7	Network	10000	up	-N/A-	-N/A-	Amphenol NDBBDA-C103	10G DAC 3M	-N/A-	-N/A-	-N/A-
Port 1-8	1-8	Network	10000	up	-N/A-	-N/A-	Amphenol NDBBDA-C103	10G DAC 3M	-N/A-	-N/A-	-N/A-
Port 1-9	1-9	Network	10000	up	-N/A-	-N/A-	Amphenol NDBBDA-C103	10G DAC 3M	-N/A-	-N/A-	-N/A-
Port 1-10	1-10	Network	10000	up	-N/A-	-N/A-	Amphenol 624380003	10G DAC 3M	-N/A-	-N/A-	-N/A-
Port 1-11	1-11	Network	10000	up	-N/A-	-N/A-	Amphenol NDBBDA-C103	10G DAC 3M	-N/A-	-N/A-	-N/A-
Port 1-12	1-12	Network	10000	up	-N/A-	-N/A-	Amphenol 624380003	10G DAC 3M	-N/A-	-N/A-	-N/A-
Port 1-13	1-13	Network	10000	up	-N/A-	-N/A-	Amphenol 624380003	10G DAC 3M	-N/A-	-N/A-	-N/A-

System Settings

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

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

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



See [System Settings on page 7-1](#) for details.

Bringing a PFS into Central Management

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

Connecting to the PFS from the NMS

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

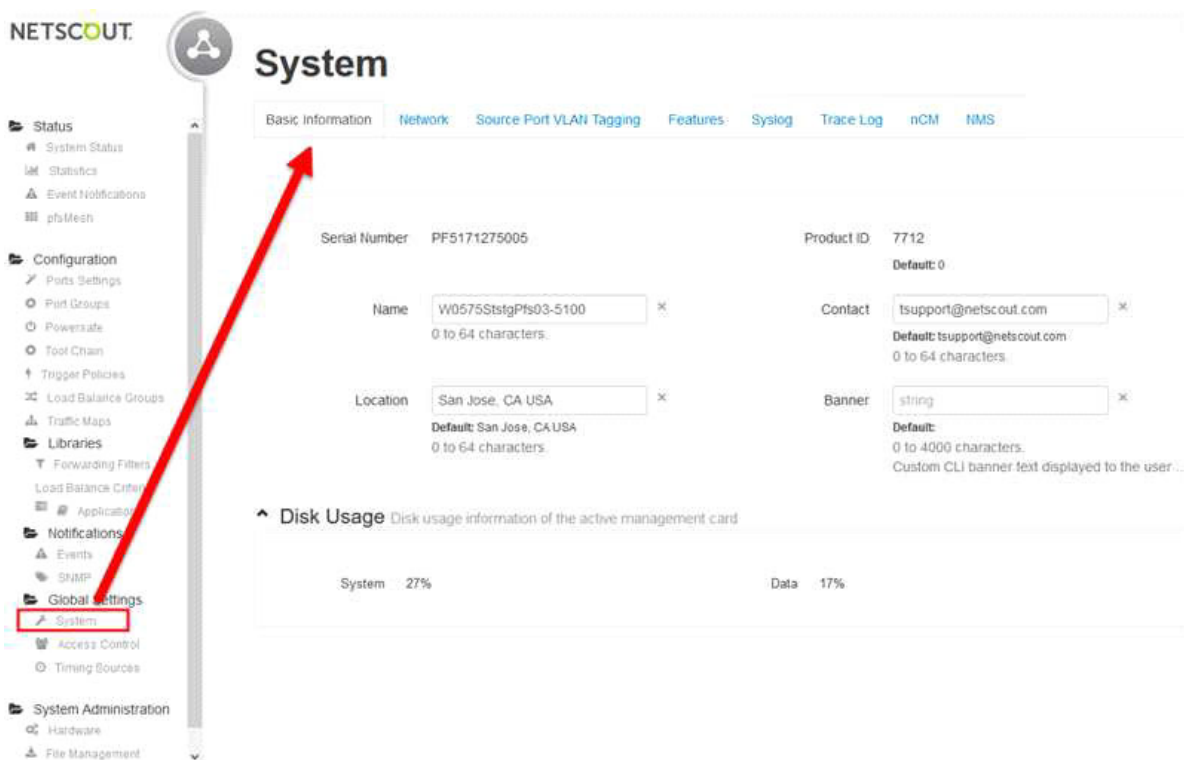
The NMS will now connect to the PFS, retrieve basic information about the switch, and place it in the list of Discovered switches. Proceed to [Accepting Switches into Central Management on page 2-9](#) to accept the switch into the list of devices managed by the NMS.

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

Configuring the NMS address in the PFS

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

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



- 3 Click on the NMS tab.

