



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*



## Cisco Fabric Manager Fundamentals Configuration Guide

Cisco MDS NX-OS Release 5.0(1a)  
Cisco MDS 9000 FabricWare Release 5.x  
July 2010

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Text Part Number: OL-21502-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.



## CONTENTS

### New and Changed Information **xv**

### Preface **lxi**

Audience **lxi**

Organization **lxi**

Document Conventions **lxii**

Related Documentation **i-lxiii**

Release Notes **i-lxiii**

Regulatory Compliance and Safety Information **i-lxiii**

Compatibility Information **i-lxiii**

Hardware Installation **i-lxiv**

Software Installation and Upgrade **i-lxiv**

Cisco NX-OS **i-lxiv**

Cisco Fabric Manager **i-lxiv**

Command-Line Interface **i-lxv**

Intelligent Storage Networking Services Configuration Guides **i-lxv**

Troubleshooting and Reference **i-lxv**

Obtaining Documentation and Submitting a Service Request **lxv**

---

### CHAPTER 1

### Cisco Fabric Manager Fundamentals Overview **1-1**

Fabric Manager Server **1-1**

Fabric Manager Client **1-1**

Device Manager **1-2**

Fabric Manager Web Client **1-2**

Performance Manager **1-3**

Authentication in Fabric Manager **1-3**

Cisco Traffic Analyzer **1-3**

Network Monitoring **1-4**

Performance Monitoring **1-4**

---

### CHAPTER 2

### Installing Cisco MDS NX-OS and Fabric Manager **2-1**

Starting a Switch in the Cisco MDS 9000 Family **2-1**

Initial Setup Routine **2-2**

Preparing to Configure the Switch **2-3**

Default Login **2-3**

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

Setup Options	2-4
Assigning Setup Information	2-4
Configuring Out-of-Band Management	2-5
Assigning a Switch Name	2-6
Configuring In-Band Management	2-9
Using the setup Command	2-12
Accessing the Switch	2-13
Where Do You Go Next?	2-13
About Cisco Fabric Manager	2-14
Fabric Manager Server	2-14
Fabric Manager Client	2-14
Fabric Manager Server Proxy Services	2-14
Device Manager	2-15
Performance Manager	2-15
Fabric Manager Web Server	2-16
Cisco MDS 9000 Switch Management	2-16
Storage Management Solutions Architecture	2-17
In-Band Management and Out-of-Band Management	2-18
mgmt0	2-18
IPFC	2-18
Installing the Management Software	2-18
Before You Install	2-19
Supported Software	2-19
Java Database Connectivity	2-20
Minimum Hardware Requirements	2-20
Upgrading Fabric Manager in Cisco SAN-OS Releases Prior to 3.1(2b)	2-21
Upgrading Fabric Manager in Cisco SAN-OS Releases 3.1(2b) and Later to 3.2(1)	2-21
Installing the Database	2-21
Directory Structure	2-21
2-22	
Installing Oracle	2-22
Increasing UDP Buffer Size	2-24
Database Backup and Restore-PostgreSQL	2-24
Backup	2-24
Restore	2-24
Importing PM Statistics Data to Fabric Manager	2-25
Installing Fabric Manager	2-25
Installing Device Manager	2-35
Creating FM/DM Shortcut Manually	2-37

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

Upgrading the Management Software	2-39
Upgrading Fabric Manager Server and Fabric Manager Standalone Version Using the Fabric Manager Update Installer	2-40
Integrating Cisco Fabric Manager with Other Management Tools	2-41
Running Fabric Manager Behind a Firewall	2-41
Uninstalling the Management Software	2-44

---

## CHAPTER 3

### **Fabric Manager Server** 3-1

Fabric Manager Server Overview	3-1
Fabric Manager Server Features	3-1
Installing and Configuring Fabric Manager Server	3-2
Installing Fabric Manager Server	3-2
Unlicensed Versus Licensed Fabric Manager Server	3-5
Data Migration in Fabric Manager Server	3-6
Verifying Performance Manager Collections	3-6
Managing a Fabric Manager Server Fabric	3-6
Selecting a Fabric to Manage Continuously	3-6
Fabric Manager Server Properties File	3-7
Modifying Fabric Manager Server	3-9
Adding or Removing Fabric Manager Server Users	3-9
Changing the Fabric Manager Server User Name and Password	3-10
Changing the Polling Period and Fabric Rediscovery Time	3-10
Using Device Aliases or FC Aliases	3-10
Server Clustering	3-11
Mapping Fabric ID to Server ID	3-11
Opening the Fabric on a Different Server	3-12
Viewing the Sessions in a Cluster	3-14
Viewing the Servers in a Cluster	3-14

---

## CHAPTER 4

### **Authentication in Fabric Manager** 4-1

Fabric Manager Authentication Overview	4-1
Best Practices for Discovering a Fabric	4-3
Setting Up Discovery for a Fabric	4-3
Performance Manager Authentication	4-4
Fabric Manager Web Server Authentication	4-4

---

## CHAPTER 5

### **Fabric Manager Client** 5-1

About Fabric Manager Client	5-1
-----------------------------	-----

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

Fabric Manager Advanced Mode	5-2
Launching Fabric Manager Client in Cisco SAN-OS Release 3.2(1) and Later	5-2
Launching Fabric Manager Client Using Launch Pad	5-7
Fabric Manager Client Quick Tour: Server Admin Perspective	5-10
Fabric Manager Main Window	5-10
Menu Bar	5-12
Tool Bar	5-12
Logical Domains Pane	5-12
Physical Attributes Pane	5-12
Information Pane	5-13
Fabric Pane	5-14
Fabric Manager Client Quick Tour: Admin Perspective	5-15
Menu Bar	5-16
File	5-16
View	5-17
Zone	5-17
Tools	5-18
Performance	5-20
Server	5-20
Help	5-20
Toolbar	5-20
Logical Domains Pane	5-22
Filtering	5-23
Physical Attributes Pane	5-23
Context Menu for Tables	5-23
Information Pane	5-26
Detachable Tables	5-27
Fabric Pane	5-27
Context Menus	5-29
Saving the Map	5-30
Purging Down Elements	5-30
Multiple Fabric Display	5-31
Filtering by Groups	5-32
Status Bar	5-33
Setting Fabric Manager Preferences	5-33
Network Fabric Discovery	5-35
Network LAN Discovery	5-35
Viewing Ethernet Switches	5-35
Removing a LAN	5-36

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

Modifying the Device Grouping	5-37
Using Alias Names as Enclosures	5-38
Using Alias Names as Descriptions	5-39
Controlling Administrator Access with Users and Roles	5-40
Using Fabric Manager Wizards	5-40
Fabric Manager Troubleshooting Tools	5-41
Integrating Fabric Manager and Data Center Network Management Software	5-41
Launching a Switch from the Topology Map	5-42

---

## CHAPTER 6

<b>Device Manager</b>	<b>6-1</b>
About Device Manager	6-1
Device Manager Features	6-2
Launching Device Manager	6-2
Using Device Manager	6-2
Menu Bar	6-3
Toolbar Icons	6-4
Dialog Boxes	6-5
Tabs	6-5
Legend	6-6
Supervisor and Switching Modules	6-7
Context Menus	6-7
Setting Device Manager Preferences	6-8

---

## CHAPTER 7

<b>Fabric Manager Web Client</b>	<b>7-1</b>
Fabric Manager Web Server	7-1
About Fabric Manager Web Client	7-1
Navigating Fabric Manager Web Client	7-2
Installing Fabric Manager Web Client	7-3
Using Fabric Manager Web Client with SSL	7-5
Launching Fabric Manager Web Client	7-7
Health	7-9
Viewing Summary Information	7-9
Viewing Fabric Information	7-10
Viewing Syslog Information	7-11
Viewing Analysis Reports	7-12
Performance	7-13
Viewing Performance Summary Information	7-14
Performance Detail Summary Report	7-15

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

7-16	
Viewing Performance Information for End Devices	7-16
Viewing Performance Information for ISLs	7-17
Viewing Performance Information for NPV Links	7-22
Viewing Performance Information for Flows	7-23
Viewing Performance Information for Gigabit Ethernet and Ethernet Ports	7-24
Viewing Other Statistics	7-24
Viewing Detailed Traffic Information	7-25
Viewing Switch Bandwidth	7-26
Viewing Predicted Future Performance	7-26
Using the Default Values	7-27
Using Your Own Values	7-27
Viewing Switch Bandwidth	7-28
Inventory	7-29
Viewing Summary Inventory Information	7-30
Viewing Detailed Summary Inventory Information	7-30
Viewing Detailed Information for VSANs	7-31
Viewing Detailed Information for Switches	7-32
Viewing License Information	7-33
Viewing Detailed Information for Modules	7-34
Viewing Detailed Information for End Devices	7-35
Viewing Detailed Information for ISLs	7-36
Viewing Detailed Information for NPV Links	7-37
Viewing Detailed Information for Zones	7-38
Reports	7-39
Creating a Custom Report Template	7-39
Viewing Custom Reports by Template	7-42
Viewing Custom Reports by Users	7-42
Delete a Report Template	7-43
Generating Custom Reports by Template	7-44
Modifying a Custom Report Template	7-46
Deleting Custom Reports	7-47
Viewing Scheduled Jobs by Report Template	7-47
Modifying Scheduled Jobs	7-48
Admin	7-49
Recovering a Web Server Password	7-49
Starting, Restarting, and Stopping Services	7-50
Adding, Editing, and Removing Managed Fabrics	7-50
Viewing Trap and Syslog Registration Information	7-52



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

Configuring Forwarding of Notifications for Events	7-53
Viewing and Disconnecting Clients	7-54
Configuring Fabric Manager Server Preferences	7-55
Adding and Removing Communities	7-55
Configuring AAA Information	7-57
Adding and Removing Users	7-57
Adding and Removing Roles	7-58
Creating Performance Collections	7-60
Configuring Other Statistics	7-61
Configuring Collection Thresholds	7-63
Importing the RRD Statistics Index	7-64
Configuring the RRD Database	7-64
Viewing Log Information	7-66
Downloading Fabric Manager Client	7-66
Fabric Manager Web Search Engine	7-66
Using Fabric Manager Search Engine	7-66
Configuring Backups using Fabric Manager Webclient	7-71
Viewing Configuration	7-71
Compare Configurations	7-71
Restore Configurations	7-72
Creating Backups	7-73
Viewing Scheduled Jobs	7-74

---

## CHAPTER 8

<b>Performance Manager</b>	<b>8-1</b>
Performance Manager Architecture	8-1
Data Interpolation	8-2
Data Collection	8-2
Using Performance Thresholds	8-2
Flow Setup Wizards	8-3
Creating a Flow Using Flow Configuration Wizard	8-3
Flow Statistics	8-6

---

## CHAPTER 9

<b>Cisco Traffic Analyzer</b>	<b>9-1</b>
Understanding SPAN	9-1
Using Cisco Traffic Analyzer with Performance Manager	9-2
Understanding the PAA-2	9-2
Understanding Cisco Traffic Analyzer	9-3
Installing Cisco Traffic Analyzer	9-3

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

[Accessing Traffic Analyzer from Fabric Manager Web Server](#) 9-5

## CHAPTER 10

### Network Monitoring 10-1

[SAN Discovery and Topology Mapping](#) 10-1

[Device Discovery](#) 10-1

[Topology Mapping](#) 10-2

[Using the Topology Map](#) 10-2

[Saving a Customized Topology Map Layout](#) 10-2

[Using Enclosures with Fabric Manager Topology Maps](#) 10-3

[Mapping Multiple Fabrics](#) 10-3

[Inventory Management](#) 10-3

[Using the Inventory Tab from Fabric Manager Web Server](#) 10-4

[Viewing Logs from Device Manager](#) 10-4

[Health and Event Monitoring](#) 10-4

[Fabric Manager Events Tab](#) 10-5

[Event Information in Fabric Manager Web Server Reports](#) 10-5

[Events in Device Manager](#) 10-5

## CHAPTER 11

### Performance Monitoring 11-1

[Real-Time Performance Monitoring](#) 11-1

[Device Manager Real-time Performance Monitoring](#) 11-1

[Configuring the Summary View](#) 11-2

[Fabric Manager Real-Time ISL Statistics](#) 11-3

[Historical Performance Monitoring](#) 11-4

[Creating a Flow with Performance Manager](#) 11-4

[Creating a Collection with Performance Manager](#) 11-4

[Using Performance Thresholds](#) 11-4

[Using the Performance Manager Configuration Wizard](#) 11-5

[Viewing Statics Using Fabric Manager](#) 11-6

[Viewing Performance Manager Reports](#) 11-7

[Performance Summary](#) 11-7

[Performance Tables and Details Graphs](#) 11-7

[Viewing Performance of Host-Optimized Port Groups](#) 11-7

[Viewing Performance Manager Events](#) 11-8

[Generating Top10 Reports in Performance Manager](#) 11-8

[Generating Top10 Reports Using Scripts](#) 11-8

[Exporting Data Collections to XML Files](#) 11-9

[Exporting Data Collections in Readable Format](#) 11-9

[Configuring Performance Manager for Use with Cisco Traffic Analyzer](#) 11-10

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

Analyzing SAN Health	11-12
Installing SAN Health Analysis Tool	11-13

## CHAPTER 12

### Software Images 12-1

About Software Images	12-1
Dependent Factors for Software Installation	12-1
Selecting the Correct Software Images for Cisco MDS 9100 Series Switches	12-2
Selecting the Correct Software Images for Cisco MDS 9200 Series Switches	12-2
Selecting the Correct Software Images for Cisco MDS 9500 Family Switches	12-2
Essential Upgrade Prerequisites	12-3
Software Upgrade Methods	12-5
Determining Software Compatibility	12-5
Automated Upgrades	12-6
Benefits of Using the Software Install Wizard	12-6
Recognizing Failure Cases	12-7
Using the Software Install Wizard	12-8
Upgrading Services Modules	12-13
Nondisruptive Upgrades on Fabric and Modular Switches	12-14
Preparing for a Nondisruptive Upgrade on Fabric and Modular Switches	12-14
Performing a Nondisruptive Upgrade on a Fabric Switch	12-15
Maintaining Supervisor Modules	12-15
Replacing Supervisor Modules	12-16
Migrating from Supervisor-1 Modules to Supervisor-2 Modules	12-16
Standby Supervisor Module Boot Variable Version	12-16
Standby Supervisor Module Bootflash Memory	12-17
Standby Supervisor Module Boot Alert	12-17
Installing Generation 2 Modules in Generation 1 Chassis	12-17
Replacing Modules	12-18
Default Settings	12-18

## CHAPTER 13

### Management Software FAQ 13-1

Installation Issues	13-3
When installing Fabric Manager from windows, why does clicking install fail?	13-3
Why do I have trouble launching Fabric Manager on Solaris?	13-3
What do I do if my browser prompts to save JNLP files?	13-3
What do I do if I see a "Java Web Start not detected" error?	13-4
What do I do if my desktop shortcuts not visible?	13-4
How do I upgrade to a newer version of Fabric Manager or Device Manager?	13-4

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

How do I downgrade Fabric Manager or Device Manager?	13-4
What do I do if an upgrade is not working?	13-4
What do I do if Java Web Start hangs on the download dialog?	13-5
How do I manually configure a browser for Java Web Start?	13-5
How do I run Java Web Start from the command line?	13-5
How do I clear the Java Web Start cache?	13-6
What do I do if during a Fabric Manager upgrade, the installer doesn't display a prompt to create a shortcut?	13-6
What do I do if my login does not work in Fabric Manager or Device Manager?	13-6
What do I do if I cannot install Fabric Manager or Device Manager, or run Java, when pcAnywhere is running?	13-6
What do I do if the Fabric Manager or Performance Manager service shows up as "disabled" in the Services menu?	13-6
What do I do if I am unable to install Fabric Manager or Device Manager, or run Java, when McAfee Internet Suite 6.0 Professional is running?	13-7
General	13-7
What do I do if I see errors while monitoring Area chart graphing?	13-7
What do I do if I see "gen error" messages?	13-7
What do I do if disk images in the Device Manager Summary View are not visible?	13-7
What do I do if I am unable to set both the D_S_TOV and E_D_TOV timers in Device Manager?	13-7
What do I do if columns in Device Manager tables are too small?	13-8
What do I do if fabric changes are not propagated onto the map (for example, links don't disappear)?	13-8
What do I do if the PortChannel creation dialog becomes too small after several uses?	13-8
What do I do if I see errors after IPFC configuration?	13-8
What do I do if Fabric Manager or Device Manager is using the wrong network interface?	13-8
What do I do if I see display anomalies in Fabric Manager or Device Manager?	13-8
What do I do if most of my Physical Attributes categories disappear?	13-9
What do I do if I can't see the Information pane?	13-9
Why is the active zone set in edit zone always shown in bold (even after successful activation)?	13-9
Can I create a zone with prefix IVRZ or a zone set with name nozonset?	13-9
What do I do when One-Click License Install fails, and I cannot connect to the Cisco website?	13-9
What do I do when Fabric Manager client and Device Manager cannot connect to the switch?	13-10
How do I increase the log window size in Fabric Manager Client?	13-10
When do I do when the FM Server Database fails to start or has a file locking error?	13-10
How do I re-synchronize Fabric Manager Client with Fabric Manager Server?	13-10
How do I rediscover the current fabric?	13-10
How do I rediscover SCSI Targets?	13-10
Windows Issues	13-11
What do I do when text fields show up too small, and I cannot enter any data?	13-11

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

What do I do when printing causes an application crash?	13-11
What do I do when Windows XP hangs (or I see a blue screen)?	13-11
What do I do when Fabric Manager and Device Manager Icons Disappear?	13-11
What do I do when Device Manager or Fabric Manager window content disappears in Windows XP?	13-11
What do I do when SCP/SFTP fails when a file is copied from local machine to the switch?	13-12
UNIX Issues	13-12
What do I do when the parent Menus Disappear?	13-12
What do I do when the web browser cannot find web server even it is running?	13-12
How do I fix a "too many open files" error?	13-12
Other	13-13
How do I set the map layout so it stays after Fabric Manager restarted?	13-13
What do I do when two switches show on the map, but there is only one switch?	13-13
What does a red/orange/dotted line through the switch mean?	13-13
How do I upgrade without losing map settings?	13-19
How do I preserve historical data when moving Fabric Manager server to new host?	13-19
Are there restrictions when using Fabric Manager across FCIP?	13-19
How do I fix a "Please insure that FM server is running on localhost" message?	13-20
How do I run Cisco Fabric Manager with multiple interfaces?	13-20
Manually specifying an interface for Fabric Manager Server	13-20
Manually specifying an interface for Fabric Manager Client or Device Manager	13-21
How do I configure an HTTP proxy server?	13-21
How do I clear the topology map?	13-21
How can I use Fabric Manager in a mixed software environment?	13-22
How do I fix a "corrupted jar file" error when Launching Fabric Manager?	13-22
How do I search for Devices in a Fabric?	13-22
How do I search in a table?	13-23
How does Fabric Manager Server licensing work?	13-24
How do I manage Multiple Fabrics?	13-24
How can I clear an Orange X Through a Switch caused by license expiration?	13-24

## APPENDIX A

### Launching Fabric Manager in Cisco SAN-OS Releases Prior to 3.2(1) A-1

Setting the Seed Switch in Cisco SAN-OS Releases 3.1(1) to 3.2(1)	A-1
Setting the Seed Switch in Releases Prior to Cisco SAN-OS Release 3.1(1)	A-3

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

---

APPENDIX B

**Cisco Fabric Manager Unsupported Feature List** B-1

---

APPENDIX C

**Interface Nonoperational Reason Codes** C-1

---

APPENDIX D

**Managing Cisco FabricWare** D-1

Fibre Channel Support D-1

Zone Configuration D-1

Security D-2

Events D-2

Managing Cisco FabricWare with Fabric Manager D-3

---

INDEX



## New and Changed Information

As of Cisco MDS NX-OS Release 4.2(1), software configuration information is available in new feature-specific configuration guides for the following information:

- System management
- Interfaces
- Fabric
- Quality of service
- Security
- IP services
- High availability and redundancy

The information in these new guides previously existed in the *Cisco MDS 9000 Family CLI Configuration Guide* and in the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*. Those configuration guides remain available on Cisco.com and should be used for all software releases prior to MDS NX-OS Release 4.2(1). Each guide addresses the features introduced in or available in a particular release. Select and view the configuration guide that pertains to the software installed in your switch.

To find additional information about Cisco MDS NX-OS Release 4.2(x), see the *Cisco MDS 9000 Family Release Notes* available at the following Cisco Systems website:

[http://www.cisco.com/en/US/products/ps5989/prod\\_release\\_notes\\_list.htm](http://www.cisco.com/en/US/products/ps5989/prod_release_notes_list.htm)

### About this Guide

The information in the new *Cisco Fabric Manager Fundamentals Configuration Guide* previously existed in Part 1: Getting Started, Part 8: Network and Switch Monitoring, and various Appendices of the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.

[Table 1](#) lists the New and Changed features for this guide, starting with MDS NX-OS Release 5.0(1).

**Table 1**      **New and Changed Features for Cisco MDS NX-OS Release 5.0(0)**

Feature	New or Changed Topics	Changed in Release	Where Documented
Integrating FM and DCNM	Integrating Fabric Manager and Data Center Network	5.0(1a)	<a href="#">Chapter 5, “Fabric Manager Client”</a>
Search Engine	Fabric manager Webclient Search Engine	5.0(1a)	<a href="#">Chapter 7, “Fabric Manager Web Client”</a>

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Table 1** *New and Changed Features for Cisco MDS NX-OS Release 5.0(0)*

Feature	New or Changed Topics	Changed in Release	Where Documented
Switch Configuration Management	Configuration Backups using Fabric Manager Webclient	5.0(1a)	<a href="#">Chapter 7, “Fabric Manager Web Client”</a>
Windows 2008 Support	Supported Software	5.0(1a)	<a href="#">Chapter 2, “Installing Cisco MDS NX-OS and Fabric Manager”</a>
SAN Health Analyzer Tool	Analyzing SAN Health	5.0(1a)	<a href="#">Chapter 11, “Performance Monitoring”</a>
Software Upgrade Wizard Enhancement	Using the Software Install Wizard	5.0(1a)	<a href="#">Chapter 12, “Software Images”</a>
Web Client Report Enhancement	Reports	5.0(1a)	<a href="#">Chapter 7, “Fabric Manager Web Client”</a>
Scoped Discovery	VSAN Scoped Discovery	5.0(1a)	<a href="#">Chapter 5, “Fabric Manager Client”</a>
Federated Server	Server Federation	4.2(1)	<a href="#">Chapter 3, “Fabric Manager Server”</a>
Cisco Discovery Protocol - FM - DM Enhancements	Launching Fabric Manager Client	4.2(1)	<a href="#">Chapter 5, “Fabric Manager Client”</a>
FM Web Client: Report Enhancements	Viewing Custom Reports by Template. Generating Custom Reports by Template.	4.2(1)	<a href="#">Chapter 7, “Fabric Manager Web Client”</a>
Fabric Manager Launch Pad	Launching Fabric Manager Client Using Launch Pad.	4.2(1)	<a href="#">Chapter 5, “Fabric Manager Client”</a>
Populate Device Alias to Device Description	Using Alias Names as Descriptions.	4.2(1)	<a href="#">Chapter 5, “Fabric Manager Client”</a>
FM Historical and Real Time Charts	Viewing Statics Using Fabric Manager	4.2(1)	<a href="#">Chapter 11, “Performance Monitoring”</a>





## Preface

This preface describes the audience, organization, and conventions of the *Cisco MDS 9000 Family Fabric Manager Fundamentals Configuration Guide*. It also provides information on how to obtain related documentation.

## Audience

This guide is for experienced network administrators who are responsible for configuring and maintaining the Cisco MDS 9000 Family of multilayer directors and fabric switches.

## Organization

This Guide is organized as follows:

Chapter	Title	Description
<a href="#">Chapter 1</a>	<a href="#">Cisco Fabric Manager Fundamentals Overview</a>	Provides a brief overview of Fabric Manager components and capabilities.
<a href="#">Chapter 2</a>	<a href="#">Installing Cisco MDS NX-OS and Fabric Manager</a>	Provides information on installation and launching the applications.
<a href="#">Chapter 3</a>	<a href="#">Fabric Manager Server</a>	Provides in-depth descriptions of GUI and capabilities for the Fabric Manager Server.
<a href="#">Chapter 4</a>	<a href="#">Authentication in Fabric Manager</a>	Describes the authentication schemes between Fabric Manager components and fabric switches.
<a href="#">Chapter 5</a>	<a href="#">Fabric Manager Client</a>	Provides in-depth descriptions of GUI and capabilities for the Fabric Manager.
<a href="#">Chapter 6</a>	<a href="#">Device Manager</a>	Provides in-depth descriptions of GUI and capabilities for the Device Manager.
<a href="#">Chapter 7</a>	<a href="#">Fabric Manager Web Client</a>	Provides in-depth descriptions of GUI and capabilities for the Fabric Manager Web Client.
<a href="#">Chapter 8</a>	<a href="#">Performance Manager</a>	Provides overview of Performance Manager architecture.
<a href="#">Chapter 9</a>	<a href="#">Cisco Traffic Analyzer</a>	Describes installing and launching Cisco Traffic Analyzer from Performance Manager.

[Send documentation comments to fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)

Chapter	Title	Description
<a href="#">Chapter 11</a>	<a href="#">Performance Monitoring</a>	Provides details on using Performance Manager.
<a href="#">Chapter 12</a>	<a href="#">Software Images</a>	Provides details on installing and upgrading software on switches.
<a href="#">Chapter 13</a>	<a href="#">Management Software FAQ</a>	Provides answers to some of the most frequently asked questions about Cisco Fabric Manager and Device Manager.
<a href="#">Appendix A</a>	<a href="#">Launching Fabric Manager in Cisco SAN-OS Releases Prior to 3.2(1)</a>	Provides instructions for launching Fabric Manager Client in Cisco SAN-OS releases prior to 3.2(1).
<a href="#">Appendix B</a>	<a href="#">Cisco Fabric Manager Unsupported Feature List</a>	Provides a list of features and functions not supported by Cisco Fabric Manager or Device Manager.
<a href="#">Appendix C</a>	<a href="#">Interface Nonoperational Reason Codes</a>	Provides the nonoperational reason codes for why an interface is up and the operational state is down.
<a href="#">Appendix D</a>	<a href="#">Managing Cisco FabricWare</a>	Provides information on the Cisco FabricWare software running on the MDS 9020 Switch which offers Fibre Channel switching services that realize maximum performance.

## Document Conventions

Command descriptions use these conventions:

<b>boldface font</b>	Commands and keywords are in boldface.
<i>italic font</i>	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
[ x   y   z ]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Screen examples use these conventions:

<code>screen font</code>	Terminal sessions and information the switch displays are in screen font.
<b>boldface screen font</b>	Information you must enter is in boldface screen font.
<i>italic screen font</i>	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

This document uses the following conventions:

**Note**

Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

## Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the following documents. To find a document online, use the Cisco MDS NX-OS Documentation Locator at:

[http://www.cisco.com/en/US/docs/storage/san\\_switches/mds9000/roadmaps/doclocator.htm](http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/roadmaps/doclocator.htm)

## Release Notes

- *Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Releases*
- *Cisco MDS 9000 Family Release Notes for MDS SAN-OS Releases*
- *Cisco MDS 9000 Family Release Notes for Storage Services Interface Images*
- *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images*
- *Release Notes for Cisco MDS 9000 Family Fabric Manager*

## Regulatory Compliance and Safety Information

- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*

## Compatibility Information

- *Cisco Data Center Interoperability Support Matrix*
- *Cisco MDS 9000 NX-OS Hardware and Software Compatibility Information and Feature Lists*
- *Cisco MDS NX-OS Release Compatibility Matrix for Storage Service Interface Images*
- *Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*
- *Cisco MDS NX-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000*
- *Cisco MDS SAN-OS Release Compatibility Matrix for VERITAS Storage Foundation for Networks Software*

*[Send documentation comments to fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Hardware Installation

- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9124 and Cisco MDS 9134 Multilayer Fabric Switch Quick Start Guide*

## Software Installation and Upgrade

- *Cisco MDS 9000 NX-OS Release 4.1(x) and SAN-OS 3(x) Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family Storage Services Interface Image Install and Upgrade Guide*
- *Cisco MDS 9000 Family Storage Services Module Software Installation and Upgrade Guide*

## Cisco NX-OS

- *Cisco MDS 9000 Family NX-OS Licensing Guide*
- *Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide*
- *Cisco MDS 9000 Family NX-OS System Management Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Security Configuration Guide*
- *Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Intelligent Storage Services Configuration Guide*
- *Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide*

## Cisco Fabric Manager

- *Cisco Fabric Manager Fundamentals Configuration Guide*
- *Cisco Fabric Manager System Management Configuration Guide*
- *Cisco Fabric Manager Interfaces Configuration Guide*
- *Cisco Fabric Manager Fabric Configuration Guide*
- *Cisco Fabric Manager Quality of Service Configuration Guide*
- *Cisco Fabric Manager Security Configuration Guide*
- *Cisco Fabric Manager IP Services Configuration Guide*
- *Cisco Fabric Manager Intelligent Storage Services Configuration Guide*
- *Cisco Fabric Manager High Availability and Redundancy Configuration Guide*
- *Cisco Fabric Manager Inter-VSAN Routing Configuration Guide*

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- *Cisco Fabric Manager Online Help*
- *Cisco Fabric Manager Web Services Online Help*

## Command-Line Interface

- *Cisco MDS 9000 Family Command Reference*

## Intelligent Storage Networking Services Configuration Guides

- *Cisco MDS 9000 I/O Acceleration Configuration Guide*
- *Cisco MDS 9000 Family SANTap Deployment Guide*
- *Cisco MDS 9000 Family Data Mobility Manager Configuration Guide*
- *Cisco MDS 9000 Family Storage Media Encryption Configuration Guide*
- *Cisco MDS 9000 Family Secure Erase Configuration Guide*
- *Cisco MDS 9000 Family Cookbook for Cisco MDS SAN-OS*

## Troubleshooting and Reference

- *Cisco NX-OS System Messages Reference*
- *Cisco MDS 9000 Family NX-OS Troubleshooting Guide*
- *Cisco MDS 9000 Family NX-OS MIB Quick Reference*
- *Cisco MDS 9000 Family NX-OS SMI-S Programming Reference*
- *Cisco MDS 9000 Family Fabric Manager Server Database Schema*

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*



# CHAPTER 1

## Cisco Fabric Manager Fundamentals Overview

---

This chapter provides an overview of the basic Cisco Fabric Manager components and includes the following sections:

- [Fabric Manager Server, page 1-1](#)
- [Authentication in Fabric Manager, page 1-3](#)
- [Fabric Manager Client, page 1-1](#)
- [Device Manager, page 1-2](#)
- [Fabric Manager Web Client, page 1-2](#)
- [Performance Manager, page 1-3](#)
- [Cisco Traffic Analyzer, page 1-3](#)
- [Network Monitoring, page 1-4](#)
- [Performance Monitoring, page 1-4](#)

### Fabric Manager Server

Fabric Manager Server is a platform for advanced MDS monitoring, troubleshooting, and configuration capabilities. Fabric Manager Server provides centralized MDS management services and performance monitoring. SNMP operations are used to efficiently collect fabric information. The Cisco Fabric Manager software, including the server components, requires about 60 MB of hard disk space on your workstation. Cisco Fabric Manager Server runs on Windows 2000, Windows 2003, Windows XP, Solaris 9 and 10, and Red Hat Enterprise Linux AS Release 5.

Each computer configured as a Cisco Fabric Manager Server can monitor multiple Fibre Channel SAN fabrics. Up to 16 clients (by default) can connect to a single Cisco Fabric Manager Server concurrently. The Cisco Fabric Manager Clients can also connect directly to an MDS switch in fabrics that are not monitored by a Cisco Fabric Manager Server, which ensures that you can manage any of your MDS devices from a single console.

### Fabric Manager Client

Cisco Fabric Manager Client is a Java and SNMP-based network fabric and device management tool with a GUI that displays real-time views of your network fabric, including Cisco Nexus 5000 Series switches, Cisco MDS 9000 Family switches and third-party switches, hosts, and storage devices.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

Fabric Manager Client provides Fibre Channel troubleshooting tools, in addition to complete configuration and status monitoring capabilities for Cisco MDS 9000 Family switches and Cisco Nexus 5000 Series switches. You can use these health and configuration analysis tools on the MDS 9000 Family switch or Cisco Nexus 5000 Series switch to perform Fibre Channel ping and traceroute.

Fabric Manager Release 4.1(1b) and later releases provide a multilevel security system by adding a server admin role that allows access to limited features. The configuration capabilities of a server admin is limited to configuring FlexAttach and relevant data. Advanced mode option is available only for network administrators and provides all of the Fabric Manager features, including security, IVR, iSCSI, and FICON.

## Device Manager

Device Manager provides a graphical representation of a Cisco MDS 9000 Family switch chassis or Cisco Nexus 5000 Series switch chassis, including the installed switching modules, the supervisor modules, the status of each port within each module, the power supplies, and the fan assemblies.

The tables in the Fabric Manager Information pane basically correspond to the dialog boxes that appear in Device Manager. However, while Fabric Manager tables show values for one or more switches, a Device Manager dialog box shows values for a single switch. Device Manager also provides more detailed information for verifying or troubleshooting device-specific configuration than Fabric Manager.

Device Manager provides two views: Device View and Summary View. Use Summary View to monitor interfaces on the switch. Use Device View to perform switch-level configurations including the following configurations:

- Configuring virtual Fibre Channel interfaces
- Configuring Fibre Channel over Ethernet (FCoE) features
- Configuring zones for multiple VSANs
- Managing ports, PortChannels, and trunking
- Managing SNMPv3 security access to switches
- Managing CLI security access to the switch
- Managing alarms, events, and notifications
- Saving and copying configuration files and software image
- Viewing hardware configuration
- Viewing chassis, module, port status, and statistics

## Fabric Manager Web Client

With Fabric Manager Web Client you can monitor Cisco MDS switch events, performance, and inventory from a remote location using a web browser.

- **Performance Manager Summary reports**—The Performance Manager summary report provides a high-level view of your network performance. These reports list the average and peak throughput and provides hot-links to additional performance graphs and tables with additional statistics. Both tabular and graphical reports are available for all interconnections monitored by Performance Manager.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- **Performance Manager drill-down reports**—Performance Manager can analyze daily, weekly, monthly and yearly trends. You can also view the results for specific time intervals using the interactive zooming functionality. These reports are only available if you create a collection using Performance Manager and start the collector.
- **Zero maintenance database for statistics storage**—No maintenance is required to maintain Performance Manager's round-robin database, because its size does not increase over time. At prescribed intervals the oldest samples are averaged (rolled-up) and saved. A full two days of raw samples are saved for maximum resolution. Gradually the resolution is reduced as groups of the oldest samples are rolled up together.

## Performance Manager

The primary purpose of Fabric Manager is to manage the network. A key management capability is network performance monitoring. Performance Manager gathers network device statistics historically and provides this information graphically using a web browser. Performance Manager presents recent statistics in detail and older statistics in summary. Performance Manager also integrates with external tools such as Cisco Traffic Analyzer.

Performance Manager has three operational stages:

- **Definition**—The Flow Wizard sets up flows in the switches.
- **Collection**—The Web Server Performance Collection screen collects information on desired fabrics.
- **Presentation**—Generates web pages to present the collected data through Fabric Manager Web Server.

Performance Manager can collect statistics for ISLs, hosts, storage elements, and configured flows. Flows are defined based on a host-to-storage (or storage-to-host) link. Performance Manager gathers statistics from across the fabric based on collection configuration files. These files determine which SAN elements and SAN links Performance Manager gathers statistics for. Based on this configuration, Performance Manager communicates with the appropriate devices (switches, hosts, or storage elements) and collects the appropriate information at fixed five-minute intervals.

## Authentication in Fabric Manager

Administrators launch Fabric Manager Client and select the seed switch that is used to discover the fabric. The user name and password are passed to Fabric Manager Server and are used to authenticate to the seed switch. If this user name and password are not a recognized SNMP user name and password, either Fabric Manager Client or Fabric Manager Server opens a CLI session to the switch (SSH or Telnet) and retries the user name and password pair. If the user name and password are recognized by the switch in either the local switch authentication database or through a remote AAA server, then the switch creates a temporary SNMP user name that is used by Fabric Manager Client and Fabric Manager Server.

## Cisco Traffic Analyzer

Cisco Traffic Analyzer provides real-time analysis of SPAN traffic or analysis of captured traffic through a Web browser user interface. Traffic encapsulated by one or more Port Analyzer Adapter products can be analyzed concurrently with a single workstation running Cisco Traffic Analyzer, which is based on ntop, a public domain software enhanced by Cisco for Fibre Channel traffic analysis.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

Cisco Traffic Analyzer monitors round-trip response times, SCSI I/Os per second, SCSI read or traffic throughput and frame counts, SCSI session status, and management task information. Additional statistics are also available on Fibre Channel frame sizes and network management protocols.

## Network Monitoring

Fabric Manager provides extensive SAN discovery, topology mapping, and information viewing capabilities. Fabric Manager collects information on the fabric topology through SNMP queries to the switches connected to it. Fabric Manager recreates a fabric topology, presents it in a customizable map, and provides inventory and configuration information in multiple viewing options such as fabric view, device view, summary view, and operation view.

Once Fabric Manager is invoked, a SAN discovery process begins. Using information polled from a seed Cisco MDS 9000 Family switch, including Name Server registrations, Fibre Channel Generic Services (FC-GS), Fabric Shortest Path First (FSPF), and SCSI-3, Fabric Manager automatically discovers all devices and interconnects on one or more fabrics. All available switches, host bus adapters (HBAs), and storage devices are discovered. The Cisco MDS 9000 Family switches use Fabric-Device Management Interface (FMDI) to retrieve the HBA model, serial number and firmware version, and host operating-system type and version discovery without host agents. Fabric Manager gathers this information through SNMP queries to each switch. The device information discovered includes device names, software revision levels, vendor, ISLs, PortChannels, and VSANs.

## Performance Monitoring

Fabric Manager and Device Manager provide multiple tools for monitoring the performance of the overall fabric, SAN elements, and SAN links. These tools provide real-time statistics as well as historical performance monitoring.

Real-time performance statistics are a useful tool in dynamic troubleshooting and fault isolation within the fabric. Real-time statistics gather data on parts of the fabric in user-configurable intervals and display these results in Fabric Manager and Device Manager.

Device Manager provides an easy tool for monitoring ports on the Cisco MDS 9000 Family switches. This tool gathers statistics at a configurable interval and displays the results in tables or charts. These statistics show the performance of the selected port in real-time and can be used for performance monitoring and troubleshooting. For a selected port, you can monitor any of a number of statistics including traffic in and out, errors, class 2 traffic, and FICON data. You can set the polling interval from ten seconds to one hour, and display the results based on a number of selectable options including absolute value, value per second, and minimum or maximum value per second.



## CHAPTER 2

# Installing Cisco MDS NX-OS and Fabric Manager

---

The Cisco Fabric Manager is a set of network management tools that supports Secure Simple Network Management Protocol version 3 (SNMPv3). It provides a graphical user interface (GUI) that displays real-time views of your network fabrics, and lets you manage the configuration of Cisco MDS 9000 Family devices and third-party switches. The Cisco Fabric Manager provides an alternative to the command-line interface (CLI) for most switch configuration commands.

In addition to complete configuration and status monitoring capabilities for Cisco MDS 9000 switches, Fabric Manager provides powerful Fibre Channel troubleshooting tools. These in-depth health and configuration analysis capabilities leverage unique MDS 9000 switch capabilities: Fibre Channel Ping and Traceroute.

This chapter contains the following sections:

- [Starting a Switch in the Cisco MDS 9000 Family, page 2-1](#)
- [Initial Setup Routine, page 2-2](#)
- [Accessing the Switch, page 2-13](#)
- [Where Do You Go Next?, page 2-13](#)
- [About Cisco Fabric Manager, page 2-14](#)
- [Installing the Management Software, page 2-18](#)
- [Upgrading the Management Software, page 2-40](#)
- [Upgrading Fabric Manager Server and Fabric Manager Standalone Version Using the Fabric Manager Update Installer, page 2-41](#)
- [Integrating Cisco Fabric Manager with Other Management Tools, page 2-42](#)
- [Running Fabric Manager Behind a Firewall, page 2-42](#)
- [Uninstalling the Management Software, page 2-45](#)

## Starting a Switch in the Cisco MDS 9000 Family

The following procedure is a review of the tasks you should have completed during hardware installation, including starting up the switch. These tasks must be completed before you can configure the switch.



**Note**


---

You must use the CLI for initial switch start up.

---

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

Before you can configure a switch, follow these steps:

- 
- Step 1** Verify the following physical connections for the new Cisco MDS 9000 Family switch:
- The console port is physically connected to a computer terminal (or terminal server).
  - The management 10/100 Ethernet port (mgmt0) is connected to an external hub, switch, or router.
- Refer to the *Cisco MDS 9000 Family Hardware Installation Guide* (for the required product) for more information.
-  **Tip** Save the host ID information for future use (for example, to enable licensed features). The host ID information is provided in the Proof of Purchase document that accompanies the switch.
- 
- Step 2** Verify that the default console port parameters are identical to those of the computer terminal (or terminal server) attached to the switch console port:
- 9600 baud
  - 8 data bits
  - 1 stop bit
  - No parity
- Step 3** Power on the switch. The switch boots automatically and the switch# prompt appears in your terminal window.
- 

## Initial Setup Routine

The first time you access a switch in the Cisco MDS 9000 Family, it runs a setup program that prompts you for the IP address and other configuration information necessary for the switch to communicate over the supervisor module Ethernet interface. This information is required to configure and manage the switch. The IP address can only be configured from the CLI. All Cisco MDS 9000 Family switches have the network administrator as a default user (admin). You cannot change the default user at any time. You must explicitly configure a strong password for any switch in the Cisco MDS 9000 Family. The setup scenario differs based on the subnet to which you are adding the new switch:

- Out-of-band management—This feature provides a connection to the network through a supervisor module front panel Ethernet port.
- In-band management—This feature provides IP over Fibre Channel (IPFC) to manage the switches. The in-band management feature is transparent to the network management system (NMS).

The first time that you access a switch in the Cisco MDS 9000 Family using the CLI, it runs a setup program that prompts you for the IP address and other configuration information necessary for the switch to communicate over the supervisor module Ethernet interface. This information is required to configure and manage the switch.



### Note

The IP address can only be configured from the CLI. When you power up the switch for the first time, assign the IP address. After you perform this step, the Cisco MDS 9000 Family Fabric Manager can reach the switch through the management port.

---

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Preparing to Configure the Switch

Before you configure a switch in the Cisco MDS 9000 Family for the first time, you need the following information:

- Administrator password, including:
  - Creating a password for the administrator (required).
  - Creating an additional login account and password (optional).
- IP address for the switch management interface—The management interface can be an out-of-band Ethernet interface or an in-band Fibre Channel interface (recommended).
- Subnet mask for the switch's management interface (optional).
- IP addresses, including:
  - Destination prefix, destination prefix subnet mask, and next hop IP address, if you want to enable IP routing. Also, provide the IP address of the default network (optional).
  - Otherwise, provide an IP address of the default gateway (optional).
- SSH service on the switch—To enable this optional service, select the type of SSH key (dsa/rsa/rsa1) and number of key bits (768 to 2048).
- DNS IP address (optional).
- Default domain name (optional).
- NTP server IP address (optional).
- SNMP community string (optional).
- Switch name—This is your switch prompt (optional).



### Note

Be sure to configure the IP route, the IP default network address, and the IP default gateway address to enable SNMP access. If IP routing is enabled, the switch uses the IP route and the default network IP address. If IP routing is disabled, the switch uses the default gateway IP address.



### Note

You should verify that the Fabric Manager Server hostname entry exists on the DNS server, unless the Fabric Manager Server is configured to bind to a specific interface during installation.

## Default Login

All Cisco MDS 9000 Family switches have the network administrator as a default user (admin). You cannot change the default user at any time (see the *Cisco Fabric Manager Security Configuration Guide*).

You have an option to enforce secure password for any switch in the Cisco MDS 9000 Family. If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a secure password (see the *Cisco Fabric Manager Security Configuration Guide*). If you configure and subsequently forget this new password, you have the option to recover this password (see the *Cisco Fabric Manager Security Configuration Guide*).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Setup Options

The setup scenario differs based on the subnet to which you are adding the new switch. You must configure a Cisco MDS 9000 Family switch with an IP address to enable management connections from outside of the switch.

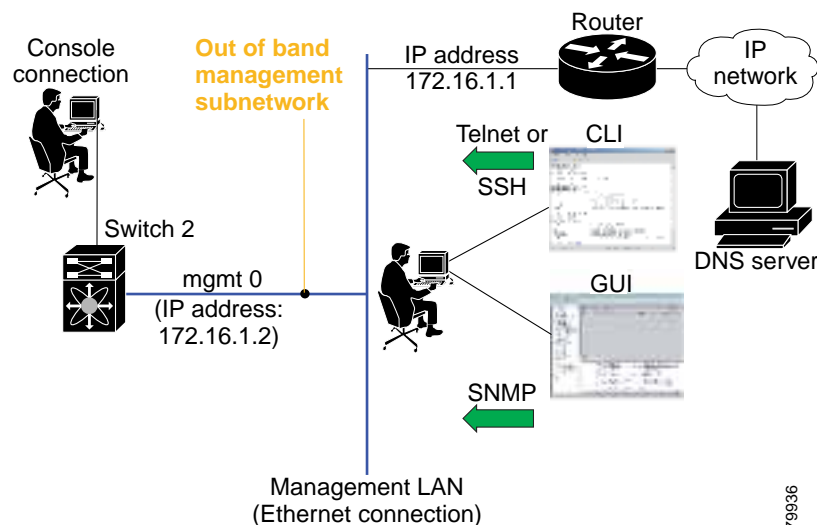


### Note

Some concepts such as out-of-band management and in-band management are briefly explained here. These concepts are explained in more detail in subsequent chapters.

- Out-of-band management—This feature provides a connection to the network through a supervisor module front panel Ethernet port (see [Figure 2-1](#)).
- In-band management—This feature provides IP over Fibre Channel (IPFC) to manage the switches. The in-band management feature is transparent to the network management system (NMS). Instead of conventional Ethernet physical media, switches in the Cisco MDS 9000 Family use IPFC as the transport mechanism. see *Cisco Fabric Manager IP Services Configuration Guide*.

**Figure 2-1** Management Access to Switches



## Assigning Setup Information

This section describes how to initially configure the switch for both out-of-band and in-band management.



### Note

Press **Ctrl-C** at any prompt to skip the remaining configuration options and proceed with what is configured until that point. Entering a new password for the administrator is a requirement and cannot be skipped.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Tip**

If you do not wish to answer a previously configured question, or if you wish to skip answers to any questions, press **Enter**. If a default answer is not available (for example, switch name), the switch uses what was previously configured and skips to the next question.

## Configuring Out-of-Band Management

**Note**

You can configure both in-band and out-of-band configuration together by entering **Yes** in both [Step 11c](#) and [Step 11d](#) in the following procedure.

To configure the switch for first time out-of-band access, follow these steps:

**Step 1** Power on the switch. Switches in the Cisco MDS 9000 Family boot automatically.

Do you want to enforce secure password standard (Yes/No)?

**Step 2** Enter **Yes** to enforce secure password.

a. Enter the administrator password

Enter the password for admin: **2008asdf\*1kjh17**

b. Confirm the administrator password.

Confirm the password for admin: **2008asdf\*1kjh17**

**Tip**

If a password is trivial (short, easy to decipher), your password configuration is rejected. Be sure to configure a secure password as shown in the sample configuration. Passwords are case-sensitive. You must explicitly configure a password that meets the requirements listed in the *Cisco Fabric Manager Security Configuration Guide*.

**Step 3** Enter **yes** to enter the setup mode.

**Note**

This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

Please register Cisco MDS 9000 Family devices promptly with your supplier. Failure to register may affect response times for initial service calls. MDS devices must be registered to receive entitled support services.

Press Enter anytime you want to skip any dialog. Use ctrl-c at anytime to skip away remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): **yes**

The setup utility guides you through the basic configuration process. Press **Ctrl-C** at any prompt to end the configuration process.

**Step 4** Enter the new password for the administrator (admin is the default).

Enter the password for admin: **admin**

**Step 5** Enter **yes** (no is the default) to create additional accounts.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

Create another login account (yes/no) [n]: **yes**

While configuring your initial setup, you can create an additional user account (in the network-admin role) besides the administrator's account. See the *Cisco Fabric Manager Security Configuration Guide* for information on default roles and permissions.



**Note** User login IDs must contain non-numeric characters.

- a. Enter the user login ID [administrator].

Enter the user login ID: *user\_name*

- b. Enter the user password.

Enter the password for user\_name: *user-password*

- c. Confirm the user password for

Confirm the password for user\_name: *user-password*

- Step 6** Enter **yes** (no is the default) to create an SNMPv3 account.

Configure read-only SNMP community string (yes/no) [n]: **yes**

- a. Enter the user name (admin is the default).

SNMPv3 user name [admin]: **admin**

- b. Enter the SNMPv3 password (minimum of eight characters). The default is **admin123**.

SNMPv3 user authentication password: *admin\_pass*

- Step 7** Enter **yes** (no is the default) to configure the read-only or read-write SNMP community string.

Configure read-write SNMP community string (yes/no) [n]: **yes**

- a. Enter the SNMP community string.

SNMP community string: *snmp\_community*

- Step 8** Enter a name for the switch.

## Assigning a Switch Name

Each switch in the fabric requires a unique name. You can assign names to easily identify the switch by its physical location, its SAN association, or the organization to which it is deployed. The assigned name is displayed in the command-line prompt. The switch name is limited to 20 alphanumeric characters.



**Note** The switch name is limited to 32 alphanumeric characters. The default is **switch**.

Enter the switch name: *switch\_name*

- Step 9** Enter **yes** (yes is the default) to configure out-of-band management.

Continue with Out-of-band (mgmt0) management configuration? [yes/no]: **yes**

- a. Enter the mgmt0 IP address.

Mgmt0 IPv4 address: *ip\_address*



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- b. Enter the mgmt0 subnet mask.

Mgmt0 IPv4 netmask: *subnet\_mask*

- Step 10** Enter **yes** (yes is the default) to configure the default gateway (recommended).

Configure the default-gateway: (yes/no) [y]: **yes**

- a. Enter the default gateway IP address.

IPv4 address of the default gateway: *default\_gateway*

- Step 11** Enter **yes** (**no** is the default) to configure advanced IP options such as in-band management, static routes, default network, DNS, and domain name.

Configure Advanced IP options (yes/no)? [n]: **yes**

- a. Enter **no** (no is the default) at the in-band management configuration prompt.

Continue with in-band (VSAN1) management configuration? (yes/no) [no]: **no**

- b. Enter **yes** (no is the default) to enable IP routing capabilities.

Enable the ip routing? (yes/no) [n]: **yes**

- c. Enter **yes** (no is the default) to configure a static route (recommended).

Configure static route: (yes/no) [n]: **yes**

Enter the destination prefix.

Destination prefix: *dest\_prefix*

Type the destination prefix mask.

Destination prefix mask: *dest\_mask*

Type the next hop IP address.

Next hop ip address: *next\_hop\_address*



**Note** Be sure to configure the IP route, the default network IP address, and the default gateway IP address to enable SNMP access. If IP routing is enabled, the switch uses the IP route and the default network IP address. If IP routing is disabled, the switch uses the default gateway IP address.

- d. Enter **yes** (no is the default) to configure the default network (recommended).

Configure the default network: (yes/no) [n]: **yes**

Enter the default network IP address.



**Note** The default network IP address is the destination prefix provided in [Step 11c](#).

Default network IP address [dest\_prefix]: *dest\_prefix*

- e. Enter **yes** (no is the default) to configure the DNS IP address.

Configure the DNS IPv4 address? (yes/no) [n]: **yes**

Enter the DNS IP address.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

DNS IPv4 address: *name\_server*

- f. Enter **yes** (default is no) to configure the default domain name.

Configure the default domain name? (yes/no) [n]: **yes**

Enter the default domain name.

Default domain name: *domain\_name*

- Step 12** Enter **yes** (no is the default) to enable Telnet service.

Enable the telnet server? (yes/no) [n]: **yes**

- Step 13** Enter **yes** (no is the default) to enable the SSH service.

Enabled SSH server? (yes/no) [n]: **yes**

- Step 14** Enter the SSH key type.

Type the SSH key you would like to generate (dsa/rsa)? **dsa**

- Step 15** Enter the number of key bits within the specified range.

Enter the number of key bits? (768 to 2048): **768**

- Step 16** Enter **yes** (no is the default) to configure the NTP server.

Configure NTP server? (yes/no) [n]: **yes**

Configure clock? (yes/no) [n] :**yes**

Configure clock? (yes/no) [n] :**yes**

Configure timezone? (yes/no) [n] :**yes**

Configure summertime? (yes/no) [n] :**yes**

Configure the ntp server? (yes/no) [n] : **yes**

- a. Enter the NTP server IP address.

NTP server IP address: *ntp\_server\_IP\_address*

- Step 17** Enter **noshut** (shut is the default) to configure the default switch port interface to the shut state.

Configure default switchport interface state (shut/noshut) [shut]: **noshut**

- Step 18** Enter **on** (on is the default) to configure the switch port trunk mode.

Configure default switchport trunk mode (on/off/auto) [on]: **on**

- Step 19** Enter **no** (no is the default) to configure switchport port mode F.

Configure default switchport port mode F (yes/no) [n] : **no**

- Step 20** Enter **permit** (deny is the default) to deny a default zone policy configuration.

Configure default zone policy (permit/deny) [deny]: **permit**

Permits traffic flow to all members of the default zone.

- Step 21** Enter **yes** (no is the default) to disable a full zone set distribution (see the *Cisco Fabric Manager Fabric Configuration Guide*). Disables the switch-wide default for the full zone set distribution feature.

Enable full zoneset distribution (yes/no) [n]: **yes**

You see the new configuration. Review and edit the configuration that you have just entered.

- Step 22** Enter **no** (no is the default) if you are satisfied with the configuration.

The following configuration will be applied:

username admin password admin\_pass role network-admin

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

```
username user_name password user_pass role network-admin
snmp-server community snmp_community ro
switchname switch
interface mgmt0
    ip address ip_address subnet_mask
    no shutdown
ip routing
ip route dest_prefix dest_mask dest_address
ip default-network dest_prefix
ip default-gateway default_gateway
ip name-server name_server
ip domain-name domain_name
telnet server enable
ssh key dsa 768 force
ssh server enable
ntp server ipaddr ntp_server
system default switchport shutdown
system default switchport trunk mode on
system default port-channel auto-create
zone default-zone permit vsan 1-4093
zoneset distribute full vsan 1-4093
```

Would you like to edit the configuration? (yes/no) [n]: **no**

**Step 23** Enter **yes** (yes is default) to use and save this configuration:

Use this configuration and save it? (yes/no) [y]: **yes**



#### Caution

If you do not save the configuration at this point, none of your changes are updated the next time the switch is rebooted. Type **yes** to save the new configuration. This ensures that the kickstart and system images are also automatically configured.

## Configuring In-Band Management

The in-band management logical interface is VSAN 1. This management interface uses the Fibre Channel infrastructure to transport IP traffic. An interface for VSAN 1 is created on every switch in the fabric. Each switch should have its VSAN 1 interface configured with an IP address in the same subnetwork. A default route that points to the switch providing access to the IP network should be configured on every switch in the Fibre Channel fabric (see *Cisco Fabric Manager Fabric Configuration Guide*)



#### Note

You can configure both in-band and out-of-band configuration together by entering **Yes** in both [Step 9c](#) and [Step 9d](#) in the following procedure.

To configure a switch for first time in-band access, follow these steps:

**Step 1** Power on the switch. Switches in the Cisco MDS 9000 Family boot automatically.

**Step 2** Enter the new password for the administrator.

Enter the password for admin: **2004asdf\*1kjh18**

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Tip**

If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password as shown in the sample configuration. Passwords are case-sensitive. You must explicitly configure a password that meets the requirements listed in the *User Accounts* section in *Cisco Fabric Manager Security Configuration Guide*.

**Step 3** Enter **yes** to enter the setup mode.

This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

Please register Cisco MDS 9000 Family devices promptly with your supplier. Failure to register may affect response times for initial service calls. MDS devices must be registered to receive entitled support services.

Press Enter incase you want to skip any dialog. Use ctrl-c at anytime to skip away remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): **yes**

The setup utility guides you through the basic configuration process. Press **Ctrl-C** at any prompt to end the configuration process.

**Step 4** Enter **no** (no is the default) if you do not wish to create additional accounts.

Create another login account (yes/no) [no]: **no**

**Step 5** Configure the read-only or read-write SNMP community string.

- a. Enter **no** (no is the default) to avoid configuring the read-only SNMP community string.

Configure read-only SNMP community string (yes/no) [n]: **no**

**Step 6** Enter a name for the switch.**Note**

The switch name is limited to 32 alphanumeric characters. The default is **switch**.

Enter the switch name: *switch\_name*

**Step 7** Enter **no** (yes is the default) at the configuration prompt to configure out-of-band management.

Continue with Out-of-band (mgmt0) management configuration? [yes/no]: **no**

**Step 8** Enter **yes** (yes is the default) to configure the default gateway.

Configure the default-gateway: (yes/no) [y]: **yes**

- a. Enter the default gateway IP address.

IP address of the default gateway: *default\_gateway*

**Step 9** Enter **yes** (no is the default) to configure advanced IP options such as in-band management, static routes, default network, DNS, and domain name.

Configure Advanced IP options (yes/no)? [n]: **yes**

- a. Enter **yes** (no is the default) at the in-band management configuration prompt.

Continue with in-band (VSAN1) management configuration? (yes/no) [no]: **yes**

Enter the VSAN 1 IP address.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

VSAN1 IP address: *ip\_address*

Enter the subnet mask.

VSAN1 IP net mask: *subnet\_mask*

- b. Enter **no** (yes is the default) to enable IP routing capabilities.

Enable ip routing capabilities? (yes/no) [y]: **no**

- c. Enter **no** (yes is the default) to configure a static route.

Configure static route: (yes/no) [y]: **no**

- d. Enter **no** (yes is the default) to configure the default network.

Configure the default-network: (yes/no) [y]: **no**

- e. Enter **no** (yes is the default) to configure the DNS IP address.

Configure the DNS IP address? (yes/no) [y]: **no**

- f. Enter **no** (no is the default) to skip the default domain name configuration.

Configure the default domain name? (yes/no) [n]: **no**

- Step 10** Enter **no** (yes is the default) to disable Telnet service.

Enable the telnet service? (yes/no) [y]: **no**

- Step 11** Enter **yes** (no is the default) to enable the SSH service.

Enabled SSH service? (yes/no) [n]: **yes**

- Step 12** Enter the SSH key type (see the *Cisco Fabric Manager Security Configuration Guide*) that you would like to generate.

Type the SSH key you would like to generate (dsa/rsa/rsa1)? **rsa**

- Step 13** Enter the number of key bits within the specified range.

Enter the number of key bits? (768 to 1024): **1024**

- Step 14** Enter **no** (no is the default) to configure the NTP server.

Configure NTP server? (yes/no) [n]: **no**

- Step 15** Enter **shut** (shut is the default) to configure the default switch port interface to the shut state.

Configure default switchport interface state (shut/noshut) [shut]: **shut**



**Note**

The management Ethernet interface is not shut down at this point—only the Fibre Channel, iSCSI, FCIP, and Gigabit Ethernet interfaces are shut down.

- Step 16** Enter **auto** (off is the default) to configure the switch port trunk mode.

Configure default switchport trunk mode (on/off/auto) [off]: **auto**

- Step 17** Enter **deny** (deny is the default) to deny a default zone policy configuration.

Configure default zone policy (permit/deny) [deny]: **deny**

Denies traffic flow to all members of the default zone.

- Step 18** Enter **no** (no is the default) to disable a full zone set distribution.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

Enable full zoneset distribution (yes/no) [n]: **no**

Disables the switch-wide default for the full zone set distribution feature.

You see the new configuration. Review and edit the configuration that you have just entered.

**Step 19** Enter **no** (no is the default) if you are satisfied with the configuration.

```
The following configuration will be applied:
username admin password admin_pass role network-admin
snmp-server community snmp_community rw
switchname switch
interface vsan1
  ip address ip_address subnet_mask
  no shutdown
ip default-gateway default_gateway
no telnet server enable
ssh key rsa 1024 force
ssh server enable
no system default switchport shutdown
system default switchport trunk mode auto
no zone default-zone permit vsan 1-4093
no zoneset distribute full vsan 1-4093
```

Would you like to edit the configuration? (yes/no) [n]: **no**

**Step 20** Enter **yes** (yes is default) to use and save this configuration.

Use this configuration and save it? (yes/no) [y]: **yes**



#### Caution

If you do not save the configuration at this point, none of your changes are updated the next time the switch is rebooted. Type **yes** to save the new configuration. This ensures that the kickstart and system images are also automatically configured.

## Using the setup Command

To make changes to the initial configuration at a later time, you can issue the **setup** command in EXEC mode.

```
switch# setup
---- Basic System Configuration Dialog ----
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup always assumes a predefined defaults irrespective
of the current system configuration when invoked from CLI.

Press Enter incase you want to skip any dialog. Use ctrl-c at anytime
to skip away remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes
```

The setup utility guides you through the basic configuration process.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Accessing the Switch

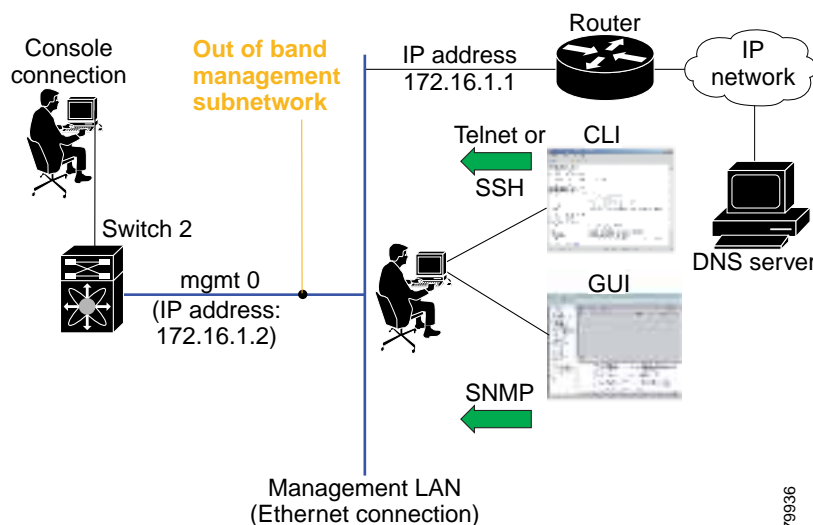
After initial configuration, you can access the switch in one of the three ways:

- Serial console access—You can use a serial port connection to access the CLI.
- In-band IP (IPFC) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use SNMP to connect to a Cisco MDS 9000 Fabric Manager application.
- Out-of-band (10/100BASE-T Ethernet) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use SNMP to connect to a Cisco MDS 9000 Fabric Manager application.

After initial configuration, you can access the switch in one of three ways (see [Figure 2-2](#)):

- Serial console access—You can use a serial port connection to access the CLI.
- In-band IP (IPFC) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use Cisco MDS 9000 Fabric Manager to access the switch.
- Out-of-band (10/100BASE-T Ethernet) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use Cisco MDS 9000 Fabric Manager to access the switch.

**Figure 2-2** Switch Access Options



79936

## Where Do You Go Next?

After reviewing the default configuration, you can change it or perform other configuration or management tasks. The initial setup can only be performed at the CLI. However, you can continue to configure other software features, or access the switch after initial configuration by using either the CLI or the Device Manager and Fabric Manager applications.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## About Cisco Fabric Manager

The Cisco Fabric Manager provides an alternative to the command-line interface (CLI) for most switch configuration commands. For information on using the CLI to configure a Cisco MDS 9000 Family switch, refer to the *Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide* or the *Cisco MDS 9020 Switch Configuration Guide* and *Cisco MDS 9000 Family Command Reference Guide*. For details on managing switches running Cisco FabricWare, see the [“Managing Cisco FabricWare with Fabric Manager” section on page D-3](#).

In addition to complete configuration and status monitoring capabilities for Cisco MDS 9000 switches, Fabric Manager provides powerful Fibre Channel troubleshooting tools. These in-depth health and configuration analysis capabilities leverage unique MDS 9000 switch capabilities: Fibre Channel Ping and Traceroute.

The Cisco Fabric Manager includes these management applications:

- Fabric Manager (client and server)
- Device Manager
- Performance Manager
- Fabric Manager Web Server

## Fabric Manager Server

The Fabric Manager Server component must be started before running Fabric Manager. On a Windows PC, the Fabric Manager Server is installed as a service. This service can then be administered using the Windows Services in the Control Panel. Fabric Manager Server is responsible for discovery of the physical and logical fabric, and for listening for SNMP traps, syslog messages, and Performance Manager threshold events. For more information, see [Chapter 3, “Fabric Manager Server.”](#)

## Fabric Manager Client

The Fabric Manager Client component displays a map of your network fabrics, including Cisco MDS 9000 Family switches, third-party switches, hosts, and storage devices. The Fabric Manager Client provides multiple menus for accessing the features of the Fabric Manager Server. For more information, see [Chapter 5, “Fabric Manager Client.”](#)

## Fabric Manager Server Proxy Services

The Fabric Manager Client and Device Manager use SNMP to communicate with the Fabric Manager Server. In typical configurations, the Fabric Manager Server may be installed behind a firewall. The SNMP proxy service available in Cisco Fabric Manager Release 2.1(1a) or later provides a TCP-based transport proxy for these SNMP requests. The SNMP proxy service allows you to block all UDP traffic at the firewall and configure Fabric Manager Client to communicate over a configured TCP port.

Fabric Manager uses the CLI for managing some features on the switches. These management tasks are used by Fabric Manager and do not use the proxy services. Your firewall must remain open for CLI access for the following features:

- External and internal loopback test
- Flash files



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Create CLI user
- Security - ISCSI users
- Show image version
- Show tech
- Switch resident reports (syslog, accounting)
- Zone migration
- Show cores

If you are using the SNMP proxy service and another application on your server is using port 9198, you need to modify your workstation settings.

**Note**

The MDS switch always checks the local SNMP users before the remote AAA users, unlike the CLI.

To modify a Windows workstation, follow these steps:

- 
- Step 1** Open Internet Explorer and select **Tools > Internet Options**.  
You see the Internet Options dialog box.
- Step 2** Select the **Connections** tab and click **LAN Settings**.  
You see the LAN Settings dialog box.
- Step 3** Check the **Use a Proxy Server for your LAN** check box and click **Advanced**.
- Step 4** Add your server IP Address or local host under the Exceptions section.
- Step 5** Click **OK** to save your changes.
- 

See the [“Running Fabric Manager Behind a Firewall”](#) section on page 2-42.

## Device Manager

The Device Manager provides two views of a single switch:

- Device View displays a graphic representation of the switch configuration and provides access to statistics and configuration information.
- Summary View displays a summary of xE ports (Inter-Switch Links), Fx ports (fabric ports), and Nx ports (attached hosts and storage) on the switch, as well as Fibre Channel and IP neighbor devices. Summary or detailed statistics can be charted, printed, or saved to a file in tab-delimited format. See [Chapter 6, “Device Manager.”](#)

## Performance Manager

Performance Manager presents detailed traffic analysis by capturing data with SNMP. This data is compiled into various graphs and charts that can be viewed with any web browser.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Fabric Manager Web Server

The Fabric Manager Web Server allows operators to monitor and obtain reports for MDS events, performance, and inventory from a remote location using a web browser. For information on installing and using Fabric Manager Web Server, see [Chapter 7, “Fabric Manager Web Client.”](#)

## Cisco MDS 9000 Switch Management

The Cisco MDS 9000 Family of switches can be accessed and configured in many different ways and supports standard management protocols. [Table 2-1](#) lists the management protocols that Fabric Manager supports to access, monitor, and configure the Cisco MDS 9000 Family of switches.

**Table 2-1**      *Supported Management Protocols*

Management Protocol	Purpose
Telnet/SSH	Provides remote access to the CLI for a Cisco MDS 9000 switch.
FTP/SFTP/TFTP, SCP	Copies configuration and software images between devices.
SNMPv1, v2c, and v3	Includes over 80 distinct Management Information Bases (MIBs). Cisco MDS 9000 Family switches support SNMP version 1, 2, and 3 and RMON V1 and V2. RMON provides advanced alarm and event management, including setting thresholds and sending notifications based on changes in device or network behavior.  By default, the Cisco Fabric Manager communicates with Cisco MDS 9000 Family switches using SNMPv3, which provides secure authentication using encrypted user names and passwords. SNMPv3 also provides the option to encrypt all management traffic.
HTTP/HTTPS	Includes HTTP and HTTPS for web browsers to communicate with Fabric Manager Web Services and for the distribution and installation of the Cisco Fabric Manager software. It is not used for communication between the Cisco Fabric Manager Server and Cisco MDS 9000 Family switches.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Table 2-1 Supported Management Protocols (continued)**

Management Protocol	Purpose
XML/CIM over HTTP/HTTPS	Includes CIM server support for designing storage area network management applications to run on Cisco SAN-OS and NX-OS.
ANSI T11 FC-GS-3	Provides Fibre Channel-Generic Services (FC-GS-3) in the defining management servers in the Fabric Configuration Server (FCS). Fabric Manager uses the information provided by FCS on top of the information contained in the Name Server database and in the Fibre Channel Shortest Path First (FSPF) topology database to build a detailed topology view and collect information for all the devices building the fabric.

## Storage Management Solutions Architecture

Management services required for the storage environment can be divided into five layers, with the bottom layer being closest to the physical storage network equipment, and the top layer managing the interface between applications and storage resources.

Of these five layers of storage network management, Cisco Fabric Manager provides tools for device (element) management and fabric management. In general, the Device Manager is most useful for device management (a single switch), while Fabric Manager is more efficient for performing fabric management operations involving multiple switches.

Tools for upper-layer management tasks can be provided by Cisco or by third-party storage and network management applications. The following summarizes the goals and function of each layer of storage network management:

- Device management provides tools to configure and manage a device within a system or a fabric. You use device management tools to perform tasks on one device at a time, such as initial device configuration, setting and monitoring thresholds, and managing device system images or firmware.
- Fabric management provides a view of an entire fabric and its devices. Fabric management applications provide fabric discovery, fabric monitoring, reporting, and fabric configuration.
- Resource management provides tools for managing resources such as fabric bandwidth, connected paths, disks, I/O operations per second (IOPS), CPU, and memory. You can use Fabric Manager to perform some of these tasks.
- Data management provides tools for ensuring the integrity, availability, and performance of data. Data management services include redundant array of independent disks (RAID) schemes, data replication practices, backup or recovery requirements, and data migration. Data management capabilities are provided by third-party tools.
- Application management provides tools for managing the overall system consisting of devices, fabric, resources, and data from the application. Application management integrates all these components with the applications that use the storage network. Application management capabilities are provided by third-party tools.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## In-Band Management and Out-of-Band Management

Cisco Fabric Manager requires an out-of-band (Ethernet) connection to at least one Cisco MDS 9000 Family switch. You need either mgmt0 or IP over Fibre Channel (IPFC) to manage the fabric.

### mgmt0

The out-of-band management connection is a 10/100 Mbps Ethernet interface on the supervisor module, labeled mgmt0. The mgmt0 interface can be connected to a management network to access the switch through IP over Ethernet. You must connect to at least one Cisco MDS 9000 Family switch in the fabric through its Ethernet management port. You can then use this connection to manage the other switches using in-band (Fibre Channel) connectivity. Otherwise, you need to connect the mgmt0 port on each switch to your Ethernet network.

Each supervisor module has its own Ethernet connection; however, the two Ethernet connections in a redundant supervisor system operate in active or standby mode. The active supervisor module also hosts the active mgmt0 connection. When a failover event occurs to the standby supervisor module, the IP address and media access control (MAC) address of the active Ethernet connection are moved to the standby Ethernet connection.

### IPFC

You can also manage switches on a Fibre Channel network using an in-band IP connection. The Cisco MDS 9000 Family supports RFC 2625 IP over Fibre Channel, which defines an encapsulation method to transport IP over a Fibre Channel network.

IPFC encapsulates IP packets into Fibre Channel frames so that management information can cross the Fibre Channel network without requiring a dedicated Ethernet connection to each switch. This feature allows you to build a completely in-band management solution.

## Installing the Management Software

To install the software for the first time, or if you want to update or reinstall the software, access the supervisor module with a web browser. Click the **Install** links on the web page that is displayed. The software running on your workstation is verified to make sure you are running the most current version of the software. If it is not current, the most recent version is downloaded and installed on your workstation.



#### Note

Before upgrading or uninstalling Fabric Manager or Device Manager, make sure any instances of these applications have been shut down.

Installation options include:

- Upgrade—The installer detects your current version of Fabric Manager and Device Manager, and it provides the option to upgrade. The default is to upgrade to the latest version of Fabric Manager or Device Manager.
- Uninstall—If you are downgrading from Fabric Manager 2.x or later to Fabric Manager 1.3x or earlier, use the Uninstall batch file or shell script. Do not delete the MDS 9000 folder as this might prevent your installation from being upgraded in the future.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Note**

We recommend that you install the latest version of the Fabric Manager applications. Fabric Manager is backward-compatible with the Cisco MDS SAN-OS and Cisco FabricWare software running on the switches. When upgrading, upgrade the Fabric Manager software first, and then upgrade the Cisco MDS SAN-OS or NX-OS or Cisco FabricWare software on the switch.

## Before You Install

Before you can access the Cisco Fabric Manager, you must complete the following tasks:

- Install a supervisor module on each switch that you want to manage.
- Configure the supervisor module with the following values using the setup routine or the CLI:
  - IP address assigned to the mgmt0 interface
  - SNMP credentials (v3 user name and password or v1/v2 communities), maintaining the same user name and password for all the switches in the fabric

Cisco MDS SAN-OS Release 2.x, 3.x, and NX-OS Release 4.2(0) and later supports AAA authentication using RADIUS, TACACS, or local SNMP users.

The Cisco Device Manager software executable files reside on each supervisor module of each Cisco MDS 9000 Family switch running Cisco MDS SAN-OS or NX-OS software in your network. The supervisor module provides an HTTP server that responds to browser requests and distributes the software to Windows or UNIX network management stations. You can also find Cisco Fabric Manager software on Cisco.com at the following website:

<http://cisco.com/cgi-bin/tablebuild.pl/mds-fm>

## Supported Software

**Note**

For the latest information on supported software, refer to the *Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Release 4.2(0)*.

Cisco Fabric Manager and Cisco Device Manager have been tested with the following software:

- Operating Systems
  - Windows 2003 SP2, Windows XP SP2, Windows XP SP3, Windows Vista SP1 (Enterprise edition), Windows 2008
  - Red Hat Enterprise Linux AS Release 5
  - Solaris (SPARC) 9 and 10
  - VMWare ESX Server 3.5.0

**Note**

We support only Windows 2003 SP2 VM created on VMWare ESX Server 3.5

- Java
  - Sun JRE and JDK 1.5(x) and 1.6(x) is supported
  - Java Web Start 1.5 and 1.6

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*



**Note** Do not use Java 1.6 Update 13

- Browsers
  - Internet Explorer 6.x and 7.0



**Note** Internet Explorer 7.0 is not supported on Windows 2000 SP4.

- Firefox 1.5, 2.0 and 3.0
- Mozilla 1.7 (packaged with Solaris 9)
- Databases
  - Oracle Database 10g Express, Oracle Enterprise Edition 10g
  - PostgreSQL 8.2 (Windows and Red Hat Enterprise Linux AS Release 5)
  - PostgreSQL 8.1 (Solaris 9 and 10)
- Security
  - Cisco ACS 3.1 and 4.0
  - PIX Firewall
  - IP Tables
  - SSH v2
  - Global Enforce SNMP Privacy Encryption
  - HTTPS

## Java Database Connectivity

Java database connectivity (JDBC) is the JavaSoft specification of a standard application programming interface (API) that allows Java programs to access database management systems.

A JDBC driver is a software component enabling a Java application to interact with a database. Fabric Manager uses Oracle JDBC drivers `ojdbc14.jar` and `ojdbc14.jar` to access the Oracle database and store data.

You can download the recommended version (10.2.0.1.0) of the `ojdbc14.jar` file, from the following link:

[http://www.oracle.com/technology/software/tech/java/sqlj\\_jdbc/htdocs/jdbc\\_10201.html](http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/htdocs/jdbc_10201.html)

Alternatively, if you have access to the system where Oracle is installed in your environment, you can find the jar file in the Oracle installation directory under `ORACLE_HOME\jdbc\lib\`.

## Minimum Hardware Requirements

For a PC running Fabric Manager Server on large fabrics (1000 or more end devices), we recommend you use a Dual Core/Dual CPU high-speed system with 2 GB of RAM and 10 GB of free disk space.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Upgrading Fabric Manager in Cisco SAN-OS Releases Prior to 3.1(2b)

When you install Cisco SAN-OS 3.2(1), data is migrated from the Hypersonic HSQL database to either the PostgreSQL database or Oracle Database 10g Express during the installation. To install the PostgreSQL database on Windows, click the FM Installer link on the CD. To install Oracle Database 10g Express, follow the instructions in the [“Installing Oracle”](#) section on page 2-23.



### Note

If you are upgrading a previous installation of Fabric Manager Server, be sure the previous installation of the database is running. Do not uninstall the previous version. If the previous version is uninstalled, the database will not be migrated and your server settings will not be preserved. After you ensure that the previous installation is running, follow the steps listed in the [“Installing Fabric Manager”](#) section on page 2-26. Before beginning the upgrade, you must close Fabric Manager and Device Manager.

## Upgrading Fabric Manager in Cisco SAN-OS Releases 3.1(2b) and Later to 3.2(1)

When you install Cisco SAN-OS 3.2(1), data is migrated from the Hypersonic HSQL database to either the PostgreSQL database or Oracle Database 10g Express during the installation. Data is also migrated from Oracle to Oracle.



### Note

If you migrate the database from Oracle to Oracle, the schema is updated as required by Cisco SAN-OS 3.2(1).

To install the PostgreSQL database on Windows, click the FM Installer link on the CD. To install Oracle Database 10g Express, follow the instructions in the [“Installing Oracle”](#) section on page 2-23.

## Upgrading Fabric Manager Federated Server

To upgrade Fabric Manager federated server on Linux and Solaris machines, follow these steps:

- 
- Step 1** Log on to the server node in the federation.
  - Step 2** Run `$INSTALLDIR/FMServer.sh stop` to stop the server node.
  - Step 3** Run the `m9000-fm-5.0.1a.jar` (`java -Xmx512m -jar m9000-fm-5.0.1a.jar`) on the first server node to upgrade the first server in the federation.
  - Step 4** Repeat steps 1 through step 3 on all the other servers nodes.
- 

To upgrade Fabric Manager federated server on a Windows machine, follow these steps:

- 
- Step 1** Log on to the server node in the federation.
  - Step 2** Stop the Fabric Manager Server service. To stop the Fabric Manager Server service, click **Start > Control Panel > Administrative Tools > Services**.
  - Step 3** Right-click Cisco Fabric Manager Server services in the services window, and then click **Stop** to stop the services.
  - Step 4** Repeat step 1 through step 3 on all the server nodes.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 5** Run the **m9000-fm-5.0.1a.jar** (`java -Xmx512m -jar m9000-fm-5.0.1a.jar`) on the first server node to upgrade the first server.
- Step 6** Repeat step 5 on all the other server nodes.

## Installing the Database

Before you install Fabric Manager, you must install a database. As of Cisco MDS NX-OS Release 4.1(1) and later, Fabric Manager is packaged with PostgreSQL and Oracle Database 10g Express databases. You can install the database of your choice using Fabric Manager from the CD-ROM or from Cisco.com. If the database is present, the Fabric Manager installer will upgrade it to the latest version.



### Note

If you are installing Cisco SAN-OS Release 3.1(2b) or later, you can also use Oracle Database 10g Express. Your other choice is PostgreSQL.



### Note

Be sure to back up all of the rrd file in \$INSTALL/pm/db before the upgrade.

## Directory Structure

Starting from Cisco MDS NX-OS Release 4.1(3a), the directory structure has changed to accommodate its future integration with Nexus 5000 products. By default, the Fabric Manager components are installed on your computer's hard drive, in the C:\Program Files\ folder. The installation path is the root directory on your computer, such as C:\Program Files\Cisco Systems. Fabric Manager and databases are installed in application directories, such as C:\Program Files\Cisco Systems\DCM\FM. [Table 2-2](#) and [Table 2-3](#) describe the directory structure for Windows, UNIX and Solaris operating systems.

**Table 2-2** *Directory Structure (Windows)*

Directory	Description
C:\Program Files\Cisco Systems\	Home directory for Cisco products.
C:\Program Files\Cisco Systems\DCM\	Home directory for Cisco Data Center Management products.
C:\Program Files\Cisco Systems\DCM\FM	Home directory for Fabric Manager and Device Manager.
C:\Program Files\Cisco Systems\DCM\JBoss-4.2.2.GA	Home directory for JBoss (Fabric Manager Server infrastructure).
C:\Program Files\Cisco Systems\DCM\DB	Home directory for database (Oracle and PostgreSQL).
C:\Program Files\Cisco Systems\DCM\JRE	Home directory for Java Runtime Environment.
C:\Program Files\Cisco Systems\DCM\JBoss-4.2.2.GA\SERVER\FM	Home directory for Fabric Manager Server.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Table 2-3**      *Directory Structure (Unix and Solaris)*

Directory	Description
/usr/local/cisco	Home directory for Cisco products.
/usr/local/cisco/dcm/	Home directory for Cisco Data Center Management products.
/usr/local/cisco/dcm/fm	Home directory for Fabric Manager and Device Manager.
/usr/local/cisco/dcm/jboss-4.2.2.GA	Home directory for JBoss (Fabric Manager Server infrastructure).
/usr/local/cisco/dcm/db	Home directory for database (Oracle and PostgreSQL).
/usr/local/cisco/dcm/jboss-4.2.2.GA/server/fm	Home directory for Fabric Manager Server.

## Installing Oracle



### Note

If you want to use Oracle Database 10g Express, you must install the database and create a user name and password before continuing with the Fabric Manager installation.



### Note

We recommend the Oracle Database 10g Express option for all users who are running Performance Manager on large fabrics (1000 or more end devices).

To install the Oracle database, follow these steps:

- Step 1** Click the following link to install Oracle Database 10g Express.  
<http://www.oracle.com/technology/software/products/database/xe/index.html>



### Note

If you have another instance of Oracle already installed on a PC, we recommend that you do not install the Oracle database on the same PC. In such cases, Fabric Manager can only use the PostgreSQL database.

- Step 2** Run OracleXE.exe to install the Oracle database. Set the password for the system user. The database administrator uses the password to manage and administer Oracle Database 10g Express server, which is installed by the Oracle installer.
- Step 3** Finish the installation and verify that both services (OracleServiceXE and OracleXETNSListener) are running from the Services window.
- Step 4** Run the following script to
- g. Change the default Oracle admin port to 8082, and
  - h. To create a database account. This example creates a new user 'scott' with a password 'tiger'. You need to keep this login credentials as it is required at a later point in the installation process.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

```
C:\> cd c:\oracle\app\oracle\product\10.2.0\server\bin
C:\oracle\app\oracle\product\10.2.0\server\bin>sqlplus / as sysdba
SQL> exec dbms_xdb.sethttpport(8082);
SQL> GRANT CONNECT,RESOURCE,UNLIMITED TABLESPACE TO SCOTT IDENTIFIED BY
TIGER;
SQL> EXIT;
```



**Note** The Oracle Database 10g Express option is supported on Microsoft Windows and UNIX systems.



**Note** For information about backing up the Oracle database, go to this location:  
[http://download.oracle.com/docs/cd/B25329\\_01/doc/admin.102/b25107/backrest.htm#i1004902](http://download.oracle.com/docs/cd/B25329_01/doc/admin.102/b25107/backrest.htm#i1004902).

You can also use the exp/imp utility at this location:  
[http://download.oracle.com/docs/cd/B25329\\_01/doc/admin.102/b25107/impexp.htm#BCEEDCIB](http://download.oracle.com/docs/cd/B25329_01/doc/admin.102/b25107/impexp.htm#BCEEDCIB).



**Note** For information about backing up the PostgreSQL database, run the pg\_dump utility to have a good backup. For more information, go to this location:  
<http://www.postgresql.org/docs/8.1/static/app-pgdump.html>.

If you are using the Oracle database, you need to install the Oracle JDBC (Java Database Connectivity) component for Fabric Manager to connect to the database. For more information refer to the “[Java Database Connectivity](#)” section on page 2-20.

## Increasing UDP Buffer Size

If the Fabric Manager SNMP packet log shows an SNMP VarBind decode error, the UDP buffer size is low and the buffer size needs to be increased.

To increase the UDP buffer size, do the following:

**Step 1** For Solaris, ensure that the UDP buffer size is at least 64 K.

```
ndd -set /dev/udp udp_rcv_hiwat 65535
nnd -set /dev/udp udp_xmit_hiwat 65535
```

**Step 2** Add the following setting in **/etc/system**, so that the buffer size will be in effect even after a reboot.

```
set ndd:udp_rcv_hiwat=65535
set ndd:udp_xmit_hiwat=65535
```



**Note** Before starting the installation, make sure that you have logged in as a Superuser.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Database Backup and Restore-PostgresSQL

The Fabric Manager uses PostgreSQL Database as the default database. The Fabric Manager backup utility uses PostgreSQL `pg_dump` utility to dump all of the database content to an ASCII dump file. Restore utility uses PostgreSQL to recreate data using the dump file.

The dump file represents a snapshot of the database at the time of backup.

### Backup

To perform a backup of the Fabric Manager database, enter these commands on Linux/Solaris. Assume `INSTALLDIR` is the top directory of Fabric Manager installation.

```
cd $INSTALLDIR/bin
/pgbackup.sh 02252008.data
```

The backup file `02252008.data` will be created in `$INSTALLDIR/bin` directory. If you want to create it in a standard backup director provide the full path name of the dump file.

To perform a backup of the Fabric Manager database, enter these commands on Windows. Assume `INSTALLDIR` is the top directory of Fabric Manager installation.

```
cd $INSTALLDIR/bin
/pgbackup.bat 02252008.data
```

The backup file `02252008.data` will be created in `$INSTALLDIR/bin` directory. If you want to create it in a standard backup director provide the full path name of the dump file.

### Restore

To restore Fabric Manager database, you must have a good backup file, and you must stop the Fabric Manager server before restoration. Run restore and enter these commands on Linux Solaris. Assume `INSTALLDIR` is the top directory of the Fabric Manager installation.

```
cd $INSTALLDIR/bin
./FMServer.sh stop
./pgrestore.sh 02252008.data
./FMServer.sh start
```

To restore Fabric Manager database, you must have a good backup file, and you must stop the Fabric Manager server before restoration. Run restore and enter these commands on Windows. Assume `INSTALLDIR` is the top directory of the Fabric Manager installation.

```
cd $INSTALLDIR/bin
./FMServer.bat stop
./pgrestore.bat 02252008.data
./FMServer.bat start
```

## Importing PM Statitics Data to Fabric Manager

To manually import existing Performance Manager statistics data to Fabric Manager, follow these steps:

---

**Step 1** Stop the Fabric Manager Server.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 2 Copy the existing RRD file (from a prior installation) to \$INSTALLDIR/pm/db.
- Step 3 Run the \$INSTALLDIR/bin/pm.bat s.
- Step 4 Restart the Fabric Manager Server.
- Step 5 Add the fabric to the Performance Manager collection using WebClient.

---

The Performance Manager historic statistics are available on WebClient after the application has been running for an hour.

## Installing Fabric Manager

Starting from Cisco MDS NX-OS Release 4.1(3a), Fabric Manager is no longer packaged with a Cisco MDS 9000 Family switch. You must install Fabric Manager from the CD-ROM or from Cisco.com.



### Note

Users installing Fabric Manager must have full administrator privileges to create user accounts and start services. Users should also have access to all ports. These are the ports used by Fabric Manager Server and the PostgreSQL database: 1098, 1099, 4444, 4445, 8009, 8083, 8090, 8092, 8093, 514, 5432.

For switches running Cisco MDS 9000 FabricWare, you must install Fabric Manager from the CD-ROM included with your switch, or you can download Fabric Manager from Cisco.com.

To download the software from Cisco.com, go to the following website:

<http://cisco.com/cgi-bin/tablebuild.pl/mds-fm>

To install Fabric Manager on Solaris, follow these steps:

- 
- Step 1 Set Java 1.5 to the path that is to be used for installing Fabric Manager.
  - Step 2 Copy the Fabric Manager jar file m9000-fm-4.2.0.136.jar from the CD-ROM to a folder on the Solaris workstation.
  - Step 3 Launch the installer using the following command:  

```
java -Xms512m -Xmx512m -jar m9000-fm-4.2.0.136
```
  - Step 4 Follow the on-screen instructions provided in the Fabric Manager management software setup wizard.
- 

When you connect to the server for the first time, Fabric Manager checks to see if you have the correct Sun Java Virtual Machine version installed on your workstation. Fabric Manager looks for version 1.5(x) during installation. If required, install the Sun Java Virtual Machine software.



### Note

You can run CiscoWorks on the same PC as Fabric Manager, even though the Java requirements are different. When installing the later Java version for Fabric Manager, make sure it does not overwrite the earlier Java version required for CiscoWorks. Both versions of Java can coexist on your PC.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Note**

On Windows, remote Fabric Manager installations or upgrades should be done through the console using VNC or through the Remote Desktop Client (RDC) in console mode (ensuring RDC is used with the **/Console** option). This is very important if the default PostgreSQL database is used with Fabric Manager, because this database requires the local console for all installations and upgrades.

**Note**

Before installing Cisco Fabric Manager on a Windows Vista system, turn the User Account Control (UAC) off. To turn off UAC, select **Start > Control Panel > User Accounts > Turn User Account Control on or off**, clear the **Use User Account Control (UAC) to help protect your computer** check box, and then click **OK**. Click **Restart Now** to apply the change.

**Note**

Telnet Client application is not installed by default on Microsoft Windows Vista. To install Telnet Client, select **Start > Programs > Control Panel > Click Turn Windows features on or off** (if you have UAC turned on you will need to give it the permission to continue). Check the **Telnet Client** check box and then click **OK**.

Starting from MDS NX-OS Release 4.1(3a) and later, Fabric Manager has an express installation option. When you select this option, Fabric Manager will be installed on your computer with a set of default user credentials. If the PostgreSQL database is not present on your computer, the installer will install PostgreSQL. If the PostgreSQL database is present, the installer will upgrade it to latest version. You may change the default credentials after the installation is complete.

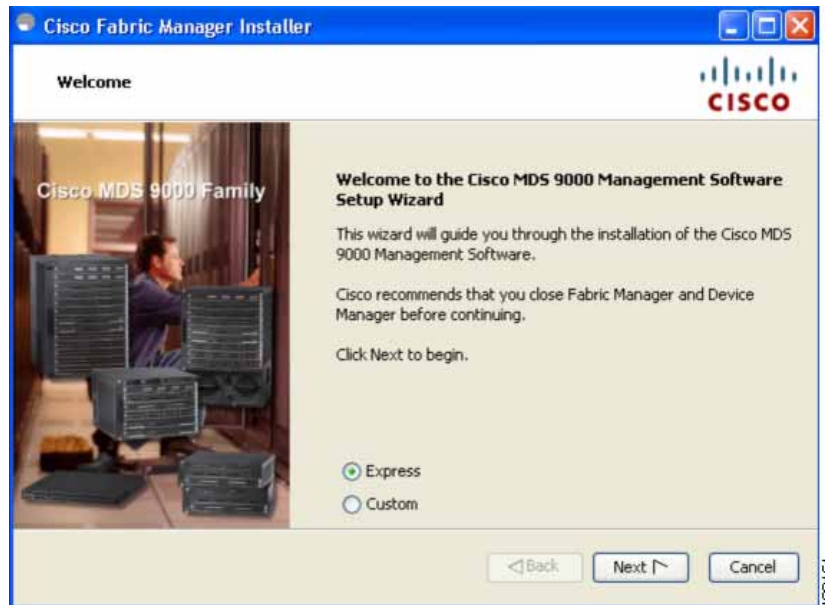
To install (Express) Fabric Manager on Windows, follow these steps:

- 
- Step 1** Click the **Install Management Software** link.
  - Step 2** Choose **Management Software > Cisco Fabric Manager**.
  - Step 3** Click the **Installing Fabric Manager** link.
  - Step 4** Click the **FM Installer** link.

You see the welcome message in the Cisco Fabric Manager Installer window shown in [Figure 2-3](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 2-3** Welcome to the Management Software Setup Wizard



**Step 5** Click the **Express** radio button, and then click **Next** to begin express installation.

**Step 6** Check the **I accept the terms of the License Agreement** check box, and then click **Next**.



**Note**

Fabric Manager express installation option uses *admin* as the user name and *password* as the user password. The user may change the password after the installation is complete.



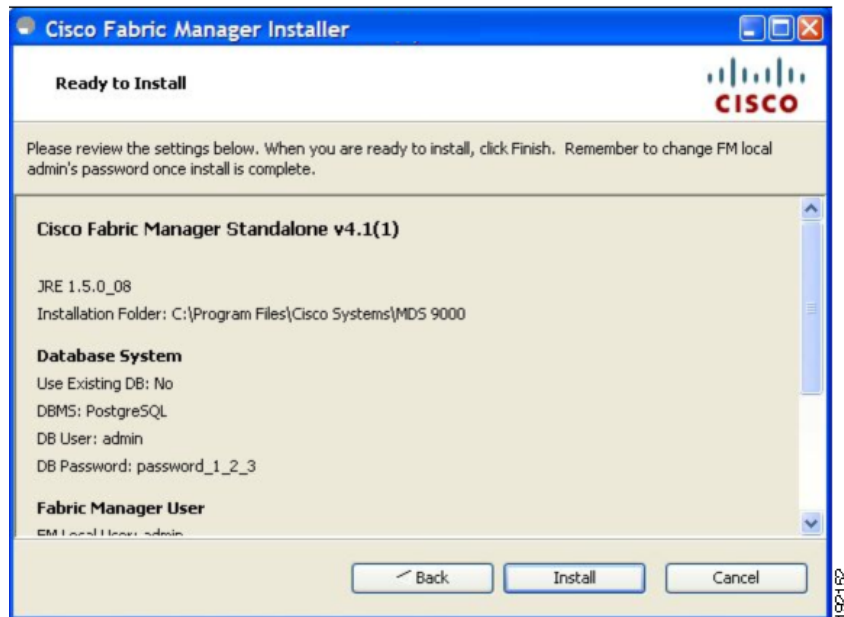
**Note**

Fabric Manager express installation option installs the PostgreSQL database with *admin* as the user name and *password\_1\_2\_3* as the user password. The user may change the password after the installation is complete.

You see the default credentials in the Cisco Fabric Manager Installer window shown in [Figure 2-4](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

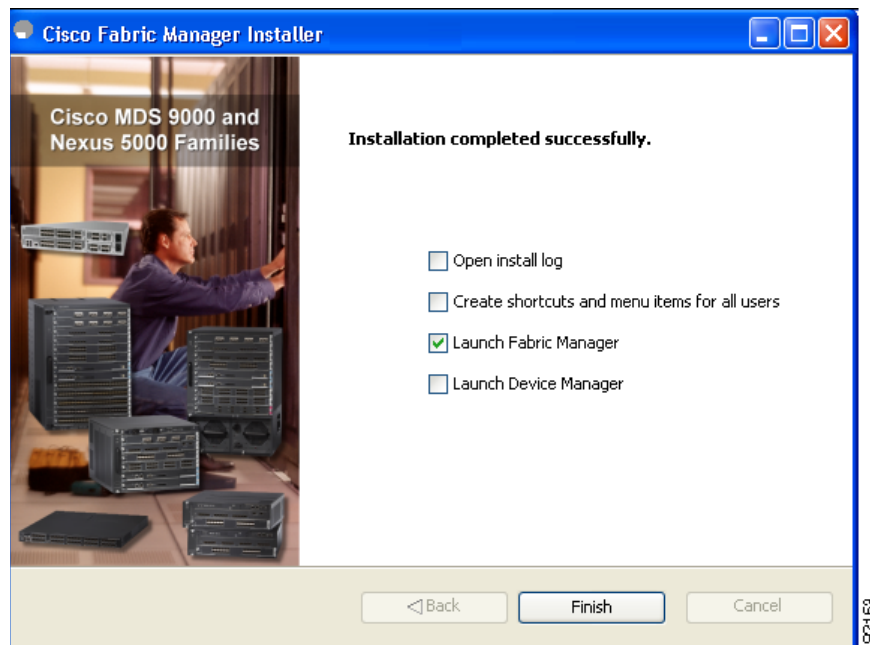
**Figure 2-4** Default User Credentials



**Step 7** Click **Install**.

Once the installation is finished, you see an installation completed message in the Cisco Fabric Manager Installer window shown in Figure 2-5.

**Figure 2-5** Install Complete



**Note**

You can choose to launch Fabric Manager or Device Manager by checking the Launch Fabric Manager or Launch Device Manager check boxes. Icons for Fabric Manager and Device Manager are automatically created on the desktop.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

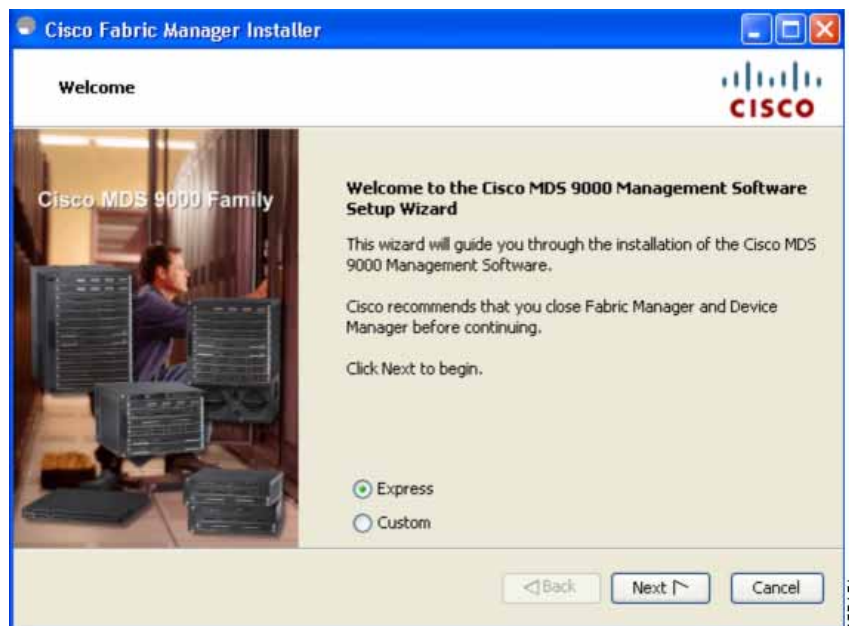
**Step 8** Click **Finish** to close the Cisco Fabric Manager Installer window.

To install (Custom) Fabric Manager on Windows, follow these steps:

- Step 1** Click the **Install Management Software** link.
- Step 2** Choose **Management Software > Cisco Fabric Manager**.
- Step 3** Click the **Installing Fabric Manager** link.
- Step 4** Click the **FM Installer** link.

You see the welcome message in the Cisco Fabric Manager Installer window shown in [Figure 2-6](#).

**Figure 2-6** *Welcome to the Management Software Setup Wizard*



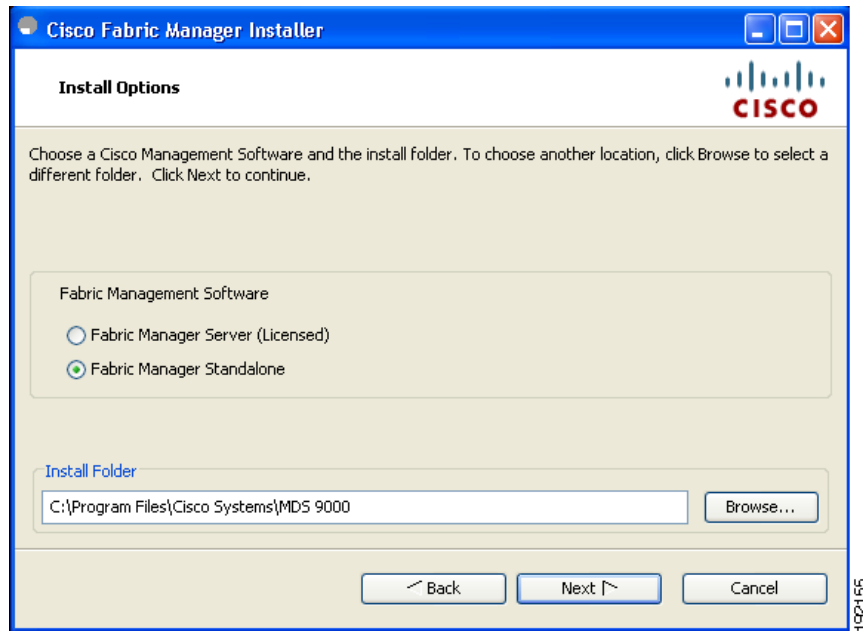
- Step 5** Click the **Custom** radio button, and then click **Next** to begin the installation.
- Step 6** Check the **I accept the terms of the License Agreement** check box, and then click **Next**.

You see the Install Options dialog box shown in [Figure 2-7](#).



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 2-7** *Install Options Dialog Box*



**Step 7** Click the radio button for either:

- a. Fabric Manager Server (Licensed) to install the server components for Fabric Manager Server.
- b. Fabric Manager Standalone to install the standalone version of Fabric Manager.



**Note**

You should verify that the Fabric Manager Server hostname entry exists on the DNS server, unless the Fabric Manager Server is configured to bind to a specific interface during installation.



**Note**

Fabric Manager Standalone is a single application containing Fabric Manager Client and a local version of Fabric Manager Server bundled together. Fabric Manager Standalone allows you to discover and monitor the immediate fabric.

**Step 8** Select an installation folder on your workstation for Fabric Manager.

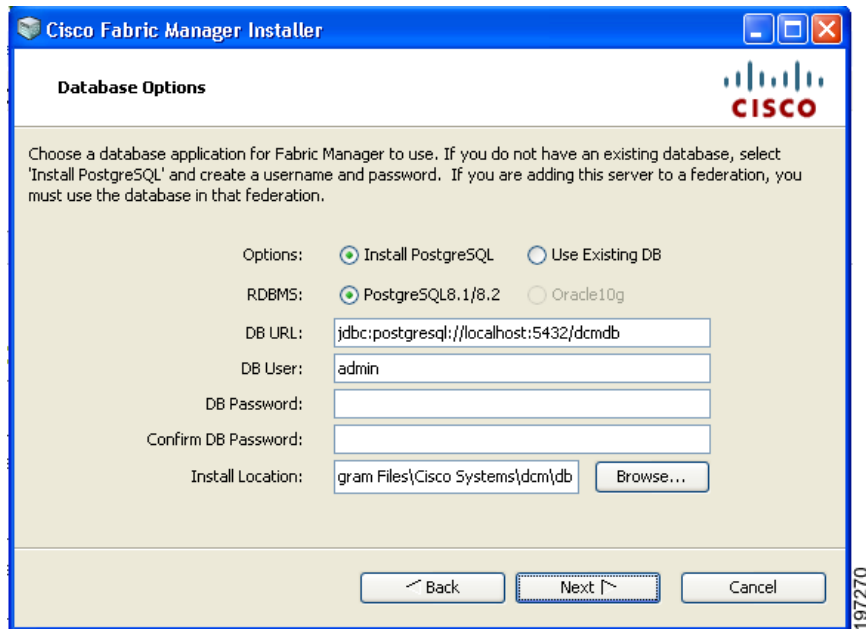
On Windows, the default location is **C:\Program Files\Cisco Systems\MDS 9000**. On a UNIX (Solaris or Linux) machine, the installation path name is **/usr/local/cisco\_mds9000** or **\$HOME/cisco\_mds9000**, depending on the permissions of the user doing the installation.

**Step 9** Click **Next**.

You see the Database Options dialog box shown in [Figure 2-8](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 2-8 Database Options Dialog Box**



- Step 10** Click the radio button for either Install PostgreSQL or Use existing DB to specify which database you want to use.

If you choose Install PostgreSQL, accept the defaults and enter a password. The PostgreSQL database will be installed.



**Note**

If you choose to install PostgreSQL, you must disable any security software you are running, because PostgreSQL may not install certain folders or users.



**Note**

Before you install PostgreSQL, remove the **cygwin/bin** from your environment variable path if Cygwin is running on your system.

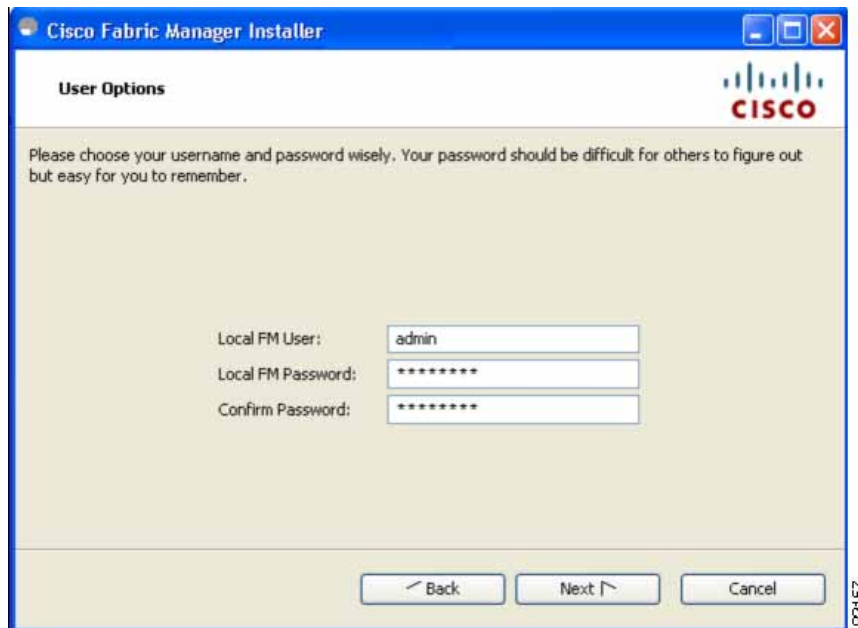
- Step 11** If you select Use existing DB, click the radio button for either PostgreSQL 8.1/8.2 or Oracle10g.

- Step 12** Click **Next** in the Database Options dialog box.

You see the User Options dialog box shown in [Figure 2-9](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 2-9 User Options Dialog Box**

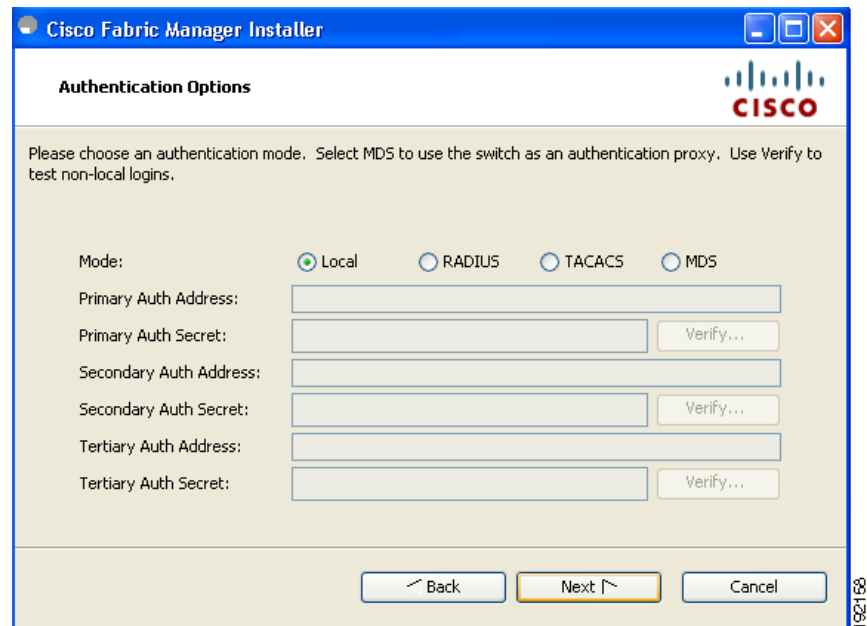


The dialog box is titled "Cisco Fabric Manager Installer" and "User Options". It contains a Cisco logo and a message: "Please choose your username and password wisely. Your password should be difficult for others to figure out but easy for you to remember." Below the message are three input fields: "Local FM User:" with the text "admin", "Local FM Password:" with "\*\*\*\*\*", and "Confirm Password:" with "\*\*\*\*\*". At the bottom are "Back", "Next", and "Cancel" buttons.

**Step 13** Enter a user name and password and click **Next**.

You see the Authentication Options dialog box shown in [Figure 2-10](#).

**Figure 2-10 Authentication Options Dialog Box**



The dialog box is titled "Cisco Fabric Manager Installer" and "Authentication Options". It contains a Cisco logo and a message: "Please choose an authentication mode. Select MDS to use the switch as an authentication proxy. Use Verify to test non-local logins." Below the message are four radio buttons for "Mode": "Local" (selected), "RADIUS", "TACACS", and "MDS". Below the radio buttons are six input fields: "Primary Auth Address:", "Primary Auth Secret:", "Secondary Auth Address:", "Secondary Auth Secret:", "Tertiary Auth Address:", and "Tertiary Auth Secret:". Each secret field has a "Verify..." button to its right. At the bottom are "Back", "Next", and "Cancel" buttons.

**Step 14** Choose an authentication mode (Local, RADIUS, TACACS or MDS) and click **Next**.



**Note**

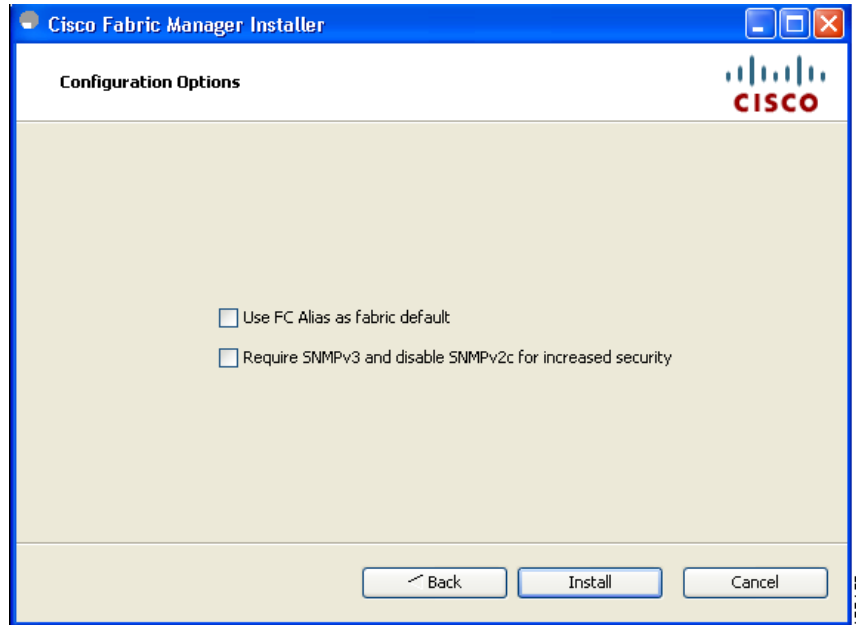
When the MDS radio button is selected, the FM authentication uses the user database in the switch for authentication.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Step 15** Click **Verify** to test your login.

You see the Configuration Options dialog box for Fabric Manager Standalone shown in [Figure 2-11](#).

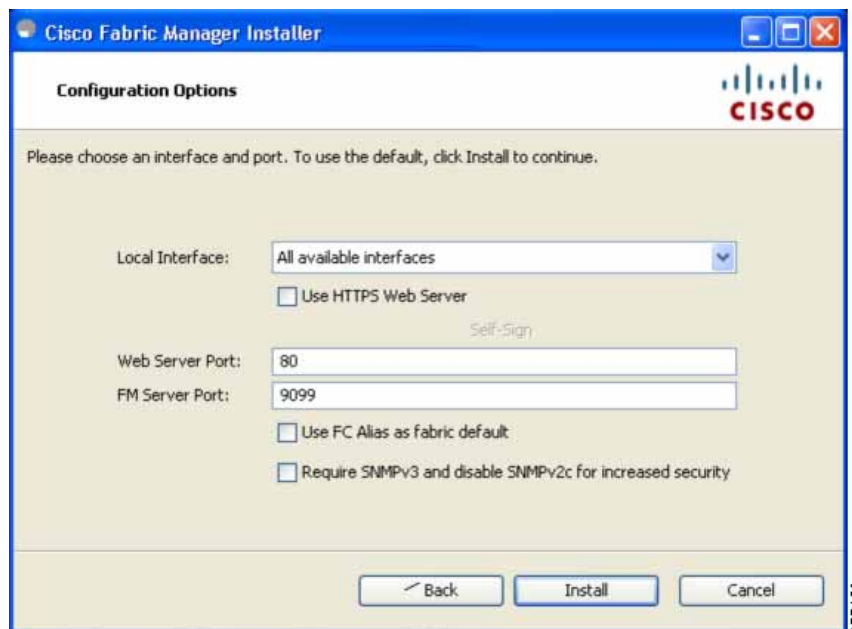
**Figure 2-11** Configuration Options Dialog Box for Fabric Manager Standalone



**Step 16** Check the FC Alias and SNMPv3 check boxes as desired and click **Install** if you are installing Fabric Manager Standalone.

You see the Configuration Options dialog box for Fabric Manager Server shown in [Figure 2-12](#).

**Figure 2-12** Configuration Options Dialog Box for Fabric Manager Server



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 17** Select the local interface, web server port or Fabric Manager server port and check the FC Alias and SNMPv3 check boxes as desired. Click **Install** if you are installing Fabric Manager Server. You see the installation progress in the Cisco Fabric Manager Installer window as shown in [Figure 2-13](#).



**Note** You can change the Fabric Manager Server port number to a port that is not used by any other application.



**Note** You should verify that the Fabric Manager Server hostname entry exists on the DNS server, unless the Fabric Manager Server is configured to bind to a specific interface during installation.

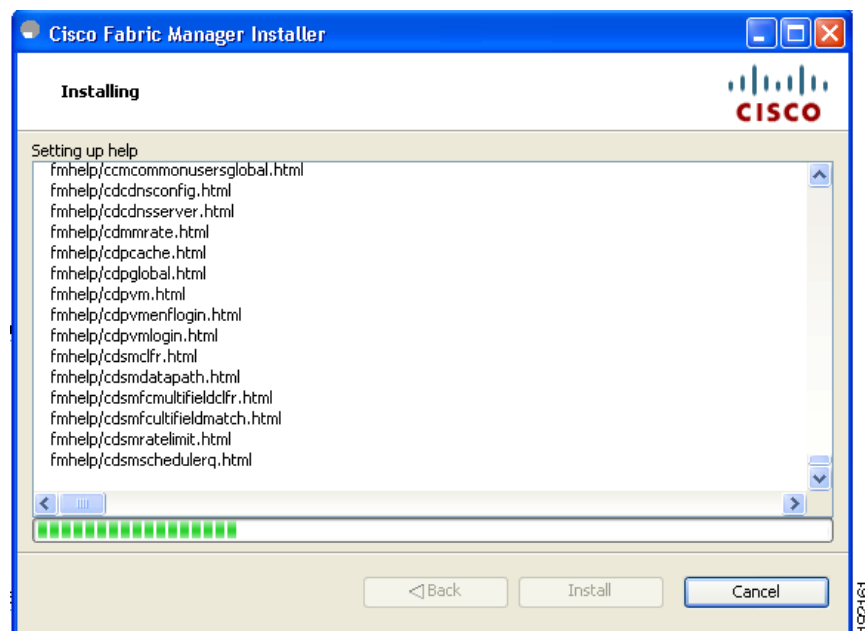


**Note** If you check the **Use HTTPS Web Server** check box, the Web Server Port field is grayed out and the default port is 443.



**Note** If you select a specific IP address during installation and change the server host IP address, you must modify the following two files that are all located in the \$INSTALL/conf directory. Change **server.bindaddrs** to the new IP address in the server.properties file and change **wrapper.app.parameter.4** to the new IP address in the FMServer.conf file.

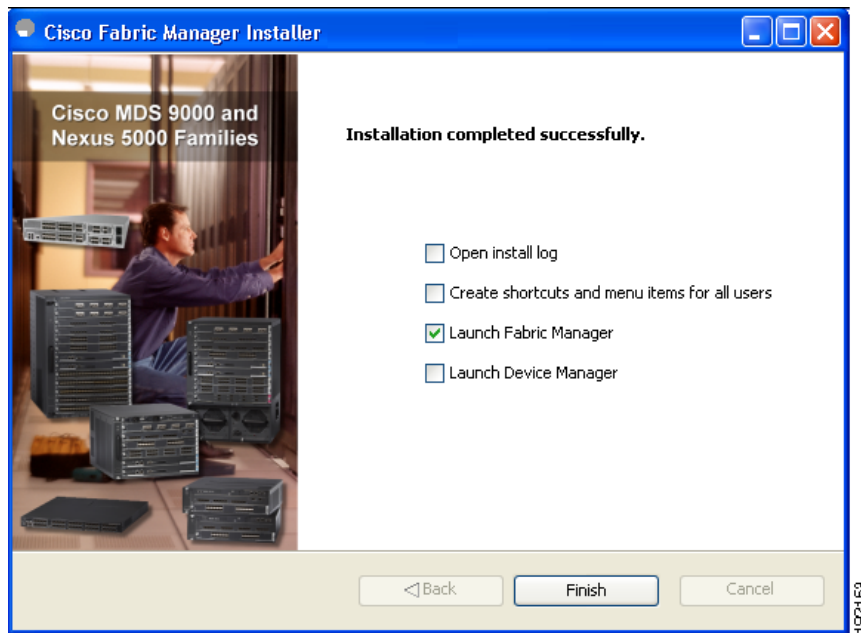
**Figure 2-13** *Progress of Installation*



Once the installation is finished, you see an installation completed message in the Cisco Fabric Manager Installer window shown in [Figure 2-14](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 2-14**      **Install Complete**



**Note**

If you installed Fabric Manager Standalone, you can choose to launch Fabric Manager or Device Manager by checking the **Launch Fabric Manager** or **Launch Device Manager** check boxes. Icons for Fabric Manager and Device Manager are automatically created on the desktop.

**Step 18**      Click **Finish** to close the Cisco Fabric Manager Installer window.

If you installed Fabric Manager Server, icons for Fabric Manager and Device Manager are not created on the desktop until you launch Fabric Manager Client. Follow the instructions in the [“Launching Fabric Manager Client Using Launch Pad”](#) section on page 5-8 to launch Fabric Manager Client.

If you checked the Create shortcuts check box, a Cisco MDS 9000 program group is created under Start > Programs on Windows. This program group contains shortcuts to batch files in the install directory.

On a UNIX (Solaris or Linux) machine, shell scripts are created in the install directory. The shell scripts that run the programs equivalent to the Windows services are FMServer.sh, all the server-side data and Performance Manager data are stored in the install directory.

Fabric Manager Client cannot run without Fabric Manager Server. The server component is downloaded and installed when you download and install Fabric Manager. On a Windows machine you install the Fabric Manager Server as a service. This service can then be administered using Services in the Microsoft Windows Control Panel. The default setting for the Fabric Manager Server service is that the server is automatically started when the machine is rebooted. You can change this behavior by modifying the properties in Services.

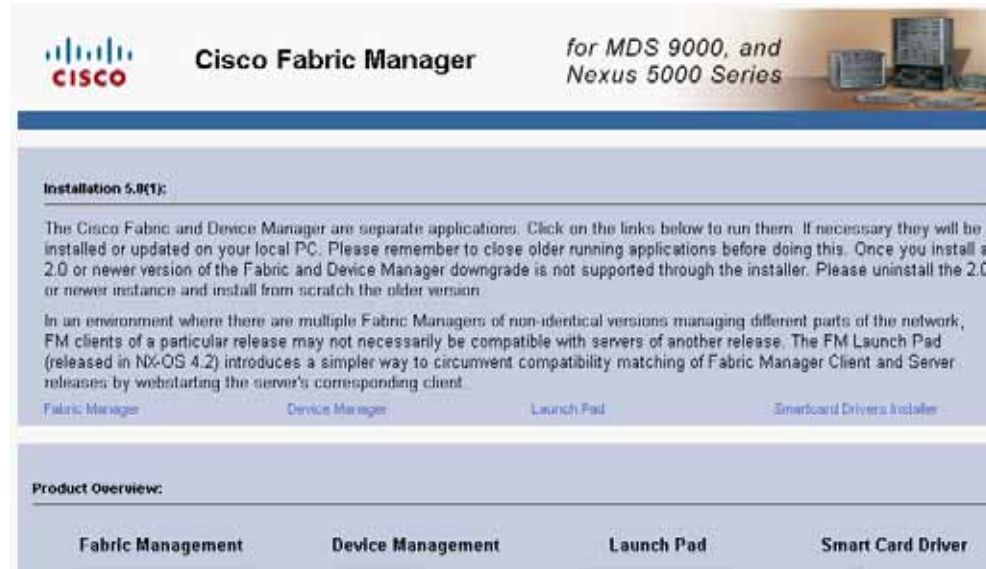
## Installing Device Manager

To install Device Manager on your workstation, follow these steps:

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 1** Enter the IP address of the switch in the Address field of your browser.  
You see the Installation window for Device Manager shown in [Figure 2-15](#).

**Figure 2-15** *Device Manager Installation Window*



- Step 2** Click the **Cisco Device Manager** link.  
You see the welcome to the management software setup wizard message in the Cisco Device Manager Installer window shown in [Figure 2-16](#).

**Figure 2-16** *Welcome to the Management Software Setup Wizard Window*



- Step 3** Click **Next** to begin the Installation.  
**Step 4** Check the **I accept the terms of the License Agreement** check box and click **Next**.

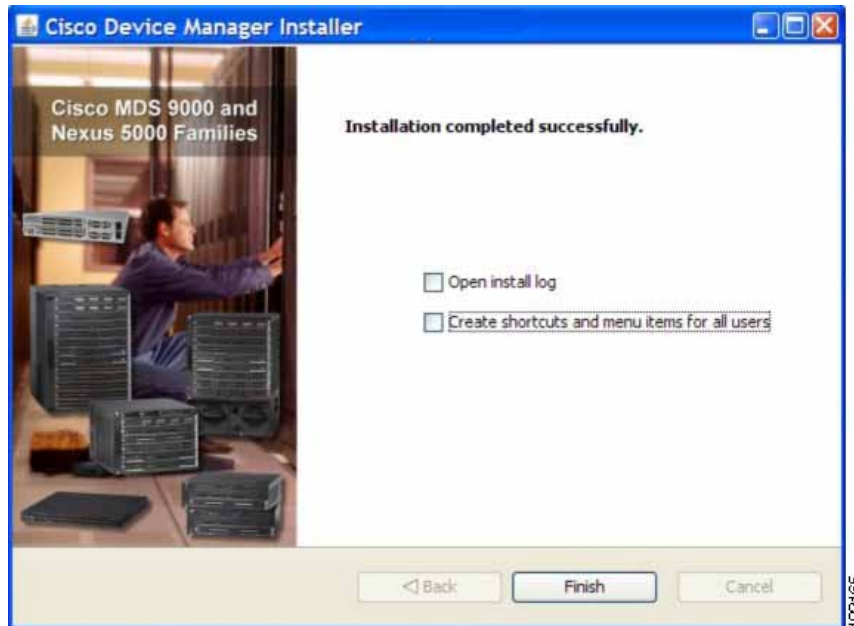
*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 5** Select an installation folder on your workstation for Device Manager. On Windows, the default location is C:\Program Files\Cisco Systems\MDS 9000. On a UNIX (Solaris or Linux) machine, the installation path name is /usr/local/cisco\_mds9000 or \$HOME/cisco\_mds9000, depending on the permissions of the user doing the installation.

- Step 6** Click **Install**.

Once the installation is finished, you see an installation completed message in the Cisco Device Manager Installer window shown in [Figure 2-17](#).

**Figure 2-17** *Install Complete*



- Step 7** Click **Finish** to close the Cisco Device Manager Installer window.

## Creating FM/DM Shortcut Manually

The FM/DM shortcut on the desktop is available only when launching the application for the first time. The shortcut is not offered when you launch Fabric Manager from the FM download page.

To create FM/DM shortcut on the desktop, follow these steps:

- Step 1** Navigate to **Control Panel> Java**.

Double-click Java.

The Java Control Panel displays as shown in the [Figure 2-18](#).



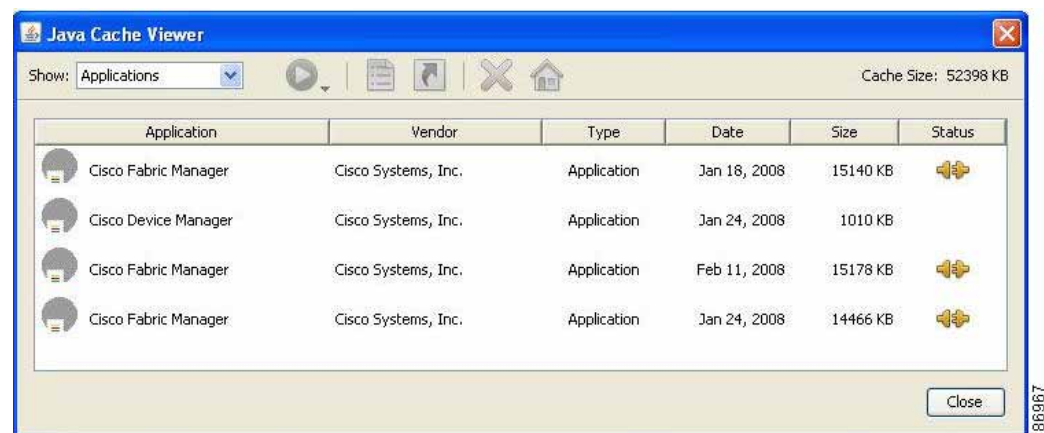
*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 2-18** Java Control Panel Dialog Box



- Step 2** In the **Temporary Internet Files** area, click **View**.  
The **Java Cache Viewer** dialog box displays as shown in [Figure 2-19](#).

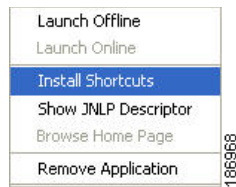
**Figure 2-19** Java Cache Viewer Dialog Box



- Step 3** To recreate the shortcut, right-click on the application, and select **Install Shortcuts** from the shortcut menu, as shown in [Figure 2-20](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 2-20**      **Shortcut Menu**



## Upgrading the Management Software

If you log into a switch running Cisco MDS SAN-OS with Device Manager and that switch has a later version of the management software, you are prompted to install the later version. To upgrade the Cisco MDS Fabric Manager software, follow the instructions described in the [“Installing the Management Software” section on page 2-18](#). You can also upgrade Device Manager at any time by entering the IP address or host name of the supervisor module with the later version of software in the Address field of your browser. You will need a new CD to upgrade Fabric Manager.



### Note

As of Cisco MDS SAN-OS Release 3.x, downgrades are not supported through the installer. To downgrade Fabric Manager or Device Manager to an earlier release, you need to manually uninstall first and then reinstall the previous version of Fabric Manager or Device Manager.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*



# Upgrading Fabric Manager Server and Fabric Manager Standalone Version Using the Fabric Manager Update Installer

As of Release 3.3(1a), you can use the Cisco MDS 9000 Fabric Manager Update Installer to upgrade:

- Fabric Manager Server
- Fabric Manager Standalone



The Fabric Manager Update Installer is smaller in size than the Fabric Manager installer which makes it easier to download. The update Installer has limited capability to upgrade Fabric Manager Server or the Fabric Manager Standalone version and it does not have the capability to install a database or the Fabric Manager Server infrastructure (JBoss). [Table 2-4](#) shows the recommended Fabric Manager upgrade paths.

**Table 2-4**      *Fabric Manager Upgrade Path Using Update Installer*

Current Version	Upgrading To	Upgrade Path
3.0(x) <sup>1</sup>	3.3(1a) or above	<ol style="list-style-type: none"> <li>1. Upgrade to 3.1(x).</li> <li>2. Upgrade to 3.2(x).</li> <li>3. Upgrade to 3.3(x) or above by launching the update installer <b>{java -Xmx512m -jar jar_file_name}</b> and then follow the steps to upgrade Fabric Manager.</li> </ol> <div>  <b>Note</b> Change the server port to 9099 if you are not upgrading from Release 3.2(2c) in Step 2. </div>
3.1(x) <sup>1</sup>	3.3(1a) or above	<ol style="list-style-type: none"> <li>1. Upgrade to 3.2(x).</li> <li>2. Upgrade to 3.3(x) or above by launching the update installer <b>{java -Xmx512m -jar jar_file_name}</b> and then follow the steps to upgrade Fabric Manager.</li> </ol> <div>  <b>Note</b> Change the server port to 9099 if you are not upgrading from Release 3.2(2c) in Step 1. </div>

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Table 2-4** *Fabric Manager Upgrade Path Using Update Installer*

Current Version	Upgrading To	Upgrade Path
3.2(x)	3.3(1a) or above	<p>1. Upgrade to 3.3(x) or above by launching the update installer {<b>java -Xmx512m -jar jar_file_name</b>} and then follow the steps to upgrade Fabric Manager.</p> <p> <b>Note</b> Change the server port to 9099 if you are not upgrading from Release 3.2(2c).</p>
3.3(x)	NX-OS 4.1(1b)	<p>1. Upgrade to 4.1(x) or above by launching the update installer {<b>java -Xmx512m -jar jar_file_name</b>} and then follow the steps to upgrade Fabric Manager.</p> <p> <b>Note</b> Change the server port to 9099 if you are not upgrading from Release 3.4(x).</p>

1. The gateway upgrade needs to be performed as the HSQL database data cannot be migrated to the new database.



**Caution**

You should not discover another fabric, re-discover the upgraded fabric or close the fabric when the upgrade is running.

## Integrating Cisco Fabric Manager with Other Management Tools

You can use Fabric Manager, Device Manager, and Performance Manager with these management tools:

- **Cisco Traffic Analyzer**—Allows you to break down traffic by VSANs and protocols and to examine SCSI traffic at a logical unit number (LUN) level.
- **Cisco Protocol Analyzer**—Enables you to examine actual sequences of Fibre Channel frames easily using the Fibre Channel and SCSI decoders Cisco developed for Ethereal.
- **Cisco Port Analyzer Adapter 2**—Encapsulates SPAN traffic (both Fibre Channel control and data plane traffic) in an Ethernet header for transport to a Windows PC or workstation for analysis. Both the Cisco Traffic Analyzer and Cisco Protocol Analyzer require the PAA to transport MDS SPAN traffic to a Windows PC or workstation.

For more information on these tools and how they work together with the Cisco Fabric Manager management applications, see *Cisco MDS 9000 Family NX-OS Troubleshooting Guide*.

## Running Fabric Manager Behind a Firewall

For Windows PCs running Fabric Manager, Device Manager, and Performance Manager behind a firewall, certain ports need to be available.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

By default, Fabric Manager Client and Device Manager use the first available UDP port for sending and receiving SNMP responses. The UDP SNMP trap local ports are 1162 for Fabric Manager, and 1163 or 1164 for Device Manager. Fabric Manager Server also opens TCP RMI port 9099.

In Fabric Manager Release 2.1(2) or later, you can select the UDP port that Fabric Manager Client or Device Manager uses for SNMP responses by uncommenting the following statement:

- On a Windows desktop, uncomment the following in the FabricManager.bat or DeviceManager.bat file in the C:\Program Files\Cisco Systems\MDS9000\bin directory:

```
rem JVMARGS=%JVMARGS% -Dsnmp.localport=9001
```

- On a UNIX desktop, uncomment the following in the FabricManager.sh or DeviceManager.sh file in the \$HOME/.cisco\_mds9000/bin directory:

```
# JVMARGS=$JVMARGS -Dsnmp.localport=9001
```

In Fabric Manager Release 3.2(1) or later, Fabric Manager Client initiates communication with Fabric Manager Server on the port 9099 for Java Naming Directory and Interface (JNDI) lookup. Fabric Manager Server redirects the client to 1098 and JBoss directs the request to the appropriate service.

Fabric Manager Server proxy services uses a configurable TCP port (9198 by default) for SNMP communications between the Fabric Manager Client or Device Manager and Fabric Manager Server.

The Fabric Manager Server component requires two predictable TCP ports to be opened on the firewall for an incoming connection:

- server.port = 9099
- server.data.port = 9100

As long as these two ports are open, Fabric Manager Client can connect to the server. Other TCP ports connected to Fabric Manager Client are initiated by the server, which is behind the firewall.

The following table lists all ports used by Fabric Manager applications:

Communication Type	Port(s) Used
<b>Used by All Applications</b>	
SSH	Port 22 (TCP)
Telnet	Port 23 (TCP)
HTTP	Port 80 (TCP)
TFTP	Port 69 (UDP)
SNMP	Port 161 (UDP)
Syslog	Port 514 (UDP)
<b>Used by Fabric Manager Server and Performance Manager</b>	
SNMP_TRAP	Port 2162 (UDP)
SNMP	Picks a random free local port (UDP) or 9198 (TCP) if SNMP proxy is enabled. Can be changed in server.properties.
Java RMI	Ports 9099, 9100 (TCP)
<b>Used by Fabric Manager Client</b>	
SNMP	Picks a random free local port (UDP) if SNMP proxy is enabled. Can be changed with the client -Dsnmp.localport option.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

Communication Type	Port(s) Used
Java RMI	Picks a free local port between 19199 and 19399 (TCP). Can be changed with the client <code>-Dclient.portStart</code> and <code>-Dclient.portEnd</code> options. For example, <code>-Dclient.portStart = 19199 -Dclient.portEnd = 19399</code> .
<b>Used by Device Manager</b>	
SNMP_TRAP	Picks a free local port between 1163 and 1170 (UDP).
SNMP	Picks a random free local port (UDP) or 9198 (TCP) if SNMP proxy is enabled. Can be changed in <b>server.properties</b> .

Port(s) Used/Type	Service Descriptor	Service Name	Attribute Name	Description
1098 (TCP)	conf/jboss-service.xml	jboss:service=Naming	RMI Naming Service Port	This port is for JNDI based naming services. The client look up this port for JNDI binding objects and resources.
9099 (TCP)	conf/jboss-service.xml	jboss:service=Naming	Bootstrap JNP Port ( FM changed 1099 to 9099)	This port is for JNDI based naming services. The client look up this port for JNDI binding objects and resources.
4444 (TCP)	conf/jboss-service.xml	jboss:service=invoker,type=jrmp	RMI /JRMP ObjectPort	The org.jboss.invocation.jrmp.server.JRMPInvoker class is an MBean service that provides the RMI/JRMP implementation of the Invoker interface. The JRMPInvoker exports itself as an RMI server so that when it is used as the Invoker in a remote client, the JRMPInvoker stub is sent to the client instead.
4445 (TCP)	conf/jboss-service.xml	jboss:service=invoker,type=pooled	Pooled Invoker	The org.jboss.invocation.pooled.server.PooledInvoker is an MBean service that provides RMI over a custom socket transport implementation of the Invoker interface. The PooledInvoker exports itself as an RMI server so that when it is used as the Invoker in a remote client, the PooledInvoker stub is sent to the client instead and invocations use the a custom socket protocol.
8009 (TCP)	deploy/jbossweb-tomcat41.sar/META-INF/jboss-service.xml	jboss.web:service=WebServer?	AJP Connector	The AJP Connector element represents a Connector component that communicates with a web connector via the AJP protocol. This is used for invisibly integrating JBoss Web into an existing or a new Apache server.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

8083 (TCP)	conf/jboss-service.xml	jboss:service=WebService	RMI dynamic class loader port	The WebService MBean provides dynamic class loading for RMI access to the server EJBs. Used for web service
8092 (TCP)	deploy/jms/oil2-service.xml	jboss.mq:service=InvocationLayer?,type=OIL2	Optimized Invocation Layer for JMS	This port is used for JBossMQ services. JBossMQ is composed of several services working together to provide JMS API level services to client applications. Optimized Invocation Layer is a service used by JMS client.
8093 (TCP)	deploy/jms/uil2-service.xml	jboss.mq:service=InvocationLayer?,type=UIL2	Unified Invocation Layer for JMS	This port is used for JBossMQ services. JBossMQ is composed of several services working together to provide JMS API level services to client applications. Unified Invocation Layer is a service used by JMS client.
3873 (TCP)	Service end point for EJB3 aspect service	JBoss EJB3 Aspect Service Deployer	JBoss EJB3 Invoker	This port used by the client to communicate with EJB3(Enterprise JavaBean 3.0) services on JBoss Server.

## Uninstalling the Management Software

To uninstall the Fabric Manager applications on a Windows PC, follow these steps:

- Step 1** Close all running instances of Fabric Manager and Device Manager.
- Step 2** Select **Start > Programs > Cisco MDS 9000 > Uninstall** to run the uninstall.bat script.
- Step 3** When you are prompted with the following message, type **Y**.
- Are you sure you want to Uninstall? Press 'Y' to uninstall, 'A' to remove all files or 'N' to exit. [Y/A/N]
- You can also run the batch file (located in the C:\Program Files\Cisco Systems\MDS 9000 folder by default) directly from the command line.



**Note** When you uninstall the application, the installer will not remove the database as it is shared with other DCM applications. Option “A” will remove all the log files and client preferences. Option “Y” will not remove the log files and client preferences.



**Note** Starting from NX-OS Release 4.1(3a), when you uninstall Fabric Manager Server, only Fabric Manager is removed. Jboss and the database, either PostgreSQL or Oracle, are not removed because they might be shared with other applications such as Cisco DCNM.



**Note** If you have installed Fabric Manager or Device Manager on Windows Vista, you may see the application shortcuts on your desktop even after uninstalling the application. To remove the shortcuts, you need to refresh the desktop.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Note**

If the Fabric Manager Client fails to uninstall with an error message, you may need to remove the Fabric Manager Client from cache using Java Cache Viewer. To remove Fabric Manager Client from cache, select Start > Run and enter `javaws -viewer`. Select Fabric Manager Client in the java cache viewer and click delete.

**Note**

For older installations, delete the `.cisco_mds9000` folder. Manually delete all desktop icons and program menu items.

On a Windows PC, this folder is created under the Documents and Settings folder (for example, `d:\Documents and Settings\Administrator\.cisco_mds9000` if you had installed it as user Administrator). On a UNIX machine, the default installation folder is `/usr/bin`.

To uninstall the Fabric Manager applications on a UNIX machine, follow these steps:

- 
- Step 1** For all releases starting with Release 2.x, run the shell script `$HOME/cisco_mds9000/Uninstall.sh` or `/usr/local/cisco_mds9000/uninstall.sh`, depending on where Fabric Manager was installed.
  - Step 2** For all releases starting with Release 1.3(1), run the shell script `$HOME/.cisco_mds9000/Uninstall.sh` or `/usr/local/.cisco_mds9000/uninstall.sh`, depending on where Fabric Manager was installed.
  - Step 3** For earlier installations, delete the `$HOME/.cisco_mds9000` folder.

**Note**

To uninstall Fabric Manager Federated Server, on a windows machine, run the batch file `$TOPDIR/Uninstall.bat` on each server node.





## CHAPTER 3

# Fabric Manager Server

---

Fabric Manager Server is a platform for advanced MDS monitoring, troubleshooting, and configuration capabilities. No additional software needs to be installed. The server capabilities are an integral part of the Cisco Fabric Manager software.

This chapter contains the following sections:

- [Fabric Manager Server Overview, page 3-1](#)
- [Fabric Manager Server Features, page 3-1](#)
- [Installing and Configuring Fabric Manager Server, page 3-2](#)
- [Managing a Fabric Manager Server Fabric, page 3-7](#)
- [Fabric Manager Server Properties File, page 3-8](#)
- [Modifying Fabric Manager Server, page 3-10](#)
- [Server Federation, page 3-12](#)

## Fabric Manager Server Overview

Install Cisco Fabric Manager Server on a computer that you want to provide centralized MDS management services and performance monitoring. SNMP operations are used to efficiently collect fabric information. The Cisco Fabric Manager software, including the server components, requires about 60 MB of hard disk space on your workstation. Cisco Fabric Manager Server runs on Windows 2000, Windows 2003, Windows XP, Solaris 9 and 10, and Red Hat Enterprise Linux AS Release 5.

Each computer configured as a Cisco Fabric Manager Server can monitor multiple Fibre Channel SAN fabrics. Up to 16 clients (by default) can connect to a single Cisco Fabric Manager Server concurrently. The Cisco Fabric Manager Clients can also connect directly to an MDS switch in fabrics that are not monitored by a Cisco Fabric Manager Server, which ensures you can manage any of your MDS devices from a single console.

## Fabric Manager Server Features

Cisco Fabric Manager Server has the following features:

- **Multiple fabric management**—Fabric Manager Server monitors multiple physical fabrics under the same user interface. This facilitates managing redundant fabrics. A licensed Fabric Manager Server maintains up-to-date discovery information on all configured fabrics so device status and interconnections are immediately available when you open the Fabric Manager Client.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- **Continuous health monitoring**—MDS health is monitored continuously, so any events that occurred since the last time you opened the Fabric Manager Client are captured.
- **Roaming user profiles**—The licensed Fabric Manager Server uses the roaming user profile feature to store your preferences and topology map layouts on the server, so that your user interface will be consistent regardless of what computer you use to manage your storage networks.



Note

You must have the same release of Fabric Manager Client and Fabric Manager Server.

## Installing and Configuring Fabric Manager Server



Note

Prior to running Fabric Manager Server, you should create a special Fabric Manager administrative user on each switch in the fabric or on a remote AAA server. Use this user to discover your fabric topology. See the [“Best Practices for Discovering a Fabric”](#) section on page 4-3.

To install Fabric Manager Server and set the initial configuration, follow these steps:

- Step 1 Install Fabric Manager and Fabric Manager server on your workstation. See the [“Installing Fabric Manager Server”](#) section on page 3-2.
- Step 2 Log in to Fabric Manager. See the [“Launching Fabric Manager Client Using Launch Pad”](#) section on page 5-8.
- Step 3 Set Fabric Manager Server to continuously monitor the fabric. See the [“Managing a Fabric Manager Server Fabric”](#) section on page 3-7.
- Step 4 Repeat [Step 2](#) through [Step 3](#) for each fabric that you want to manage through Fabric Manager Server.
- Step 5 Install Fabric Manager Web Server. See the [“Verifying Performance Manager Collections”](#) section on page 3-7.
- Step 6 Verify Performance Manager is collecting data. See the [“Verifying Performance Manager Collections”](#) section on page 3-7.

## Installing Fabric Manager Server

When you install Fabric Manager, the basic version of the Fabric Manager Server (unlicensed) is installed with it. After you click the Fabric Manager icon, a dialog box opens and you can enter the IP address of a computer running the Fabric Manager Server component. If you do not see the Fabric Manager Server IP address text box, click **Options** to expand the list of configuration options. If the server component is running on your local machine, leave **localhost** in that field. If you try to run Fabric Manager without specifying a valid server, you are prompted to start the Fabric Manager Server locally.

On a Windows PC, you install the Fabric Manager Server as a service. This service can then be administered using Services in the Administrative Tools. The default setting for the Fabric Manager Server service is that the server is automatically started when the Windows PC is rebooted. You can change this behavior by modifying the properties in Services.

For switches running Cisco MDS 9000 FabricWare, you must install Fabric Manager from the CD-ROM included with your switch, or you can download Fabric Manager from Cisco.com.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Note**

You can have only one instance of Fabric Manager Server running on a computer. If you have a Fabric Manager Standalone version on your computer, you may need to uninstall it before you install Fabric Manager Server.

To download the software from Cisco.com, go to the following website:

<http://cisco.com/cgi-bin/tablebuild.pl/mds-fm>

**Note**

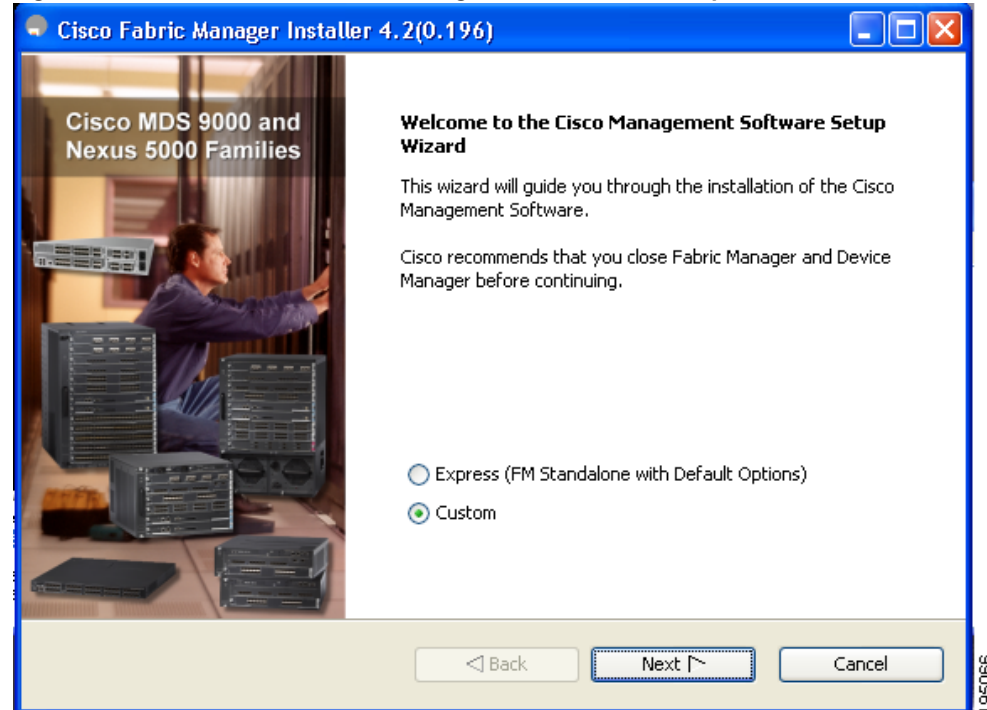
If you are upgrading the Fabric Manager Server to 5.0(1a) that is configured with HTTPS to use your own self-provisioned or 3rd-party issued SSL certificate, make sure that you set the keystore password and then restart the Fabric Manager Server. To set the keystore password, run **\$INSTALLDIR/dcm/fm/bin encrypter.bat ssl**.

To install Fabric Manager Server on windows, follow these steps:

- Step 1** Click the **Install Management Software** link.
- Step 2** Choose **Management Software > Cisco Fabric Manager**.
- Step 3** Click the **Installing Fabric Manager** link.
- Step 4** Click the **FM Installer** link.

You see the welcome message in the Cisco Fabric Manager Installer window shown in [Figure 3-1](#).

**Figure 3-1** Welcome to the Management Software Setup Wizard

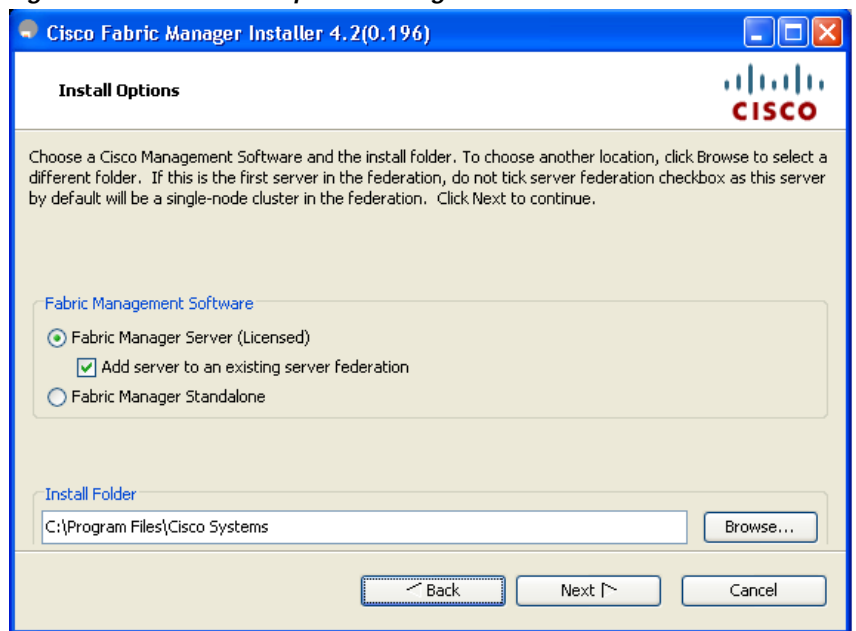


- Step 5** Click the **Custom** radio button, and then click **Next** to begin installation.
- Step 6** Check the **I accept the terms of the License Agreement** check box, and then click **Next**.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

You see the Install Options dialog box as shown in Figure 3-2.

**Figure 3-2 Install Options Dialog Box**



**Step 7** Click the **Fabric Manager Server (Licensed)** radio button to install the server components for Fabric Manager Server.

**Step 8** Click **Add server to an existing server federation** to add the server to a federation.



**Note**

You may need to add the following line in the pg-hba.conf file under **# IPv4 local connections** in order to allow remote hosts to connect to PostgreSQL database:

```
host all all 0.0.0.0/0 md5
```

After adding, save the configuration file, restart the PostgreSQL database before you install the second server node.



**Note**

If you are joining more than three Fabric Manager Servers in a federation, you need to use an Oracle database with the following settings.

```
C:\Documents and Settings\Administrator>sqlplus /nolog
SQL*Plus: Release 10.2.0.1.0 - Production on Wed Jan 6 17:19:32 2010
Copyright (c) 1982, 2005, Oracle. All rights reserved.
SQL> connect / as sysdba;
Connected.

SQL> alter system set processes=100 scope=spfile;
System altered.
SQL> alter system set open_cursors=500 scope=spfile;
System altered.

SQL> shutdown immediately;
SP2-0717: illegal SHUTDOWN option
SQL> shutdown immediate;
Database closed.
Database dismounted.
```

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

```
ORACLE instance shut down.
SQL> startup;
ORACLE instance started.
Total System Global Area  805306368 bytes
Fixed Size                  1453836 bytes
Variable Size              218714356 bytes
Database Buffers           583008256 bytes
Redo Buffers                2129920 bytes
Database mounted.
Database opened.
SQL> show parameter processes;
```

```
Total System Global Area  805306368 bytes
Fixed Size                  1453836 bytes
Variable Size              218714356 bytes
Database Buffers           583008256 bytes
Redo Buffers                2129920 bytes
Database mounted.
Database opened.
SQL> show parameter processes;
```

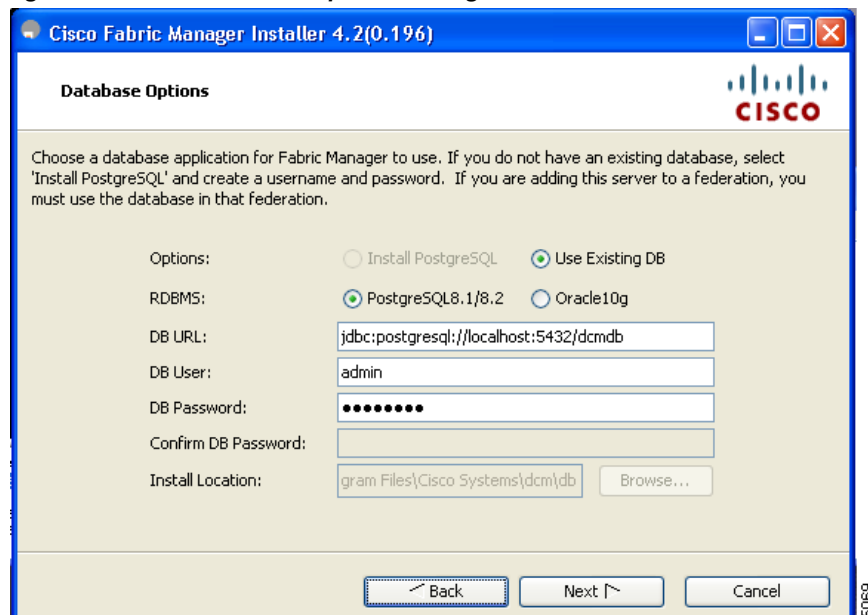
NAME	TYPE	VALUE
aq_tm_processes	integer	0
db_writer_processes	integer	4
gcs_server_processes	integer	0
job_queue_processes	integer	4
log_archive_max_processes	integer	2
processes	integer	100

**Step 9** Select an installation folder on your workstation for Fabric Manager. On Windows, the default location is **C:\Program Files\Cisco Systems**.

**Step 10** Click **Next**.

You see the Database Options dialog box as shown in [Figure 3-3](#).

**Figure 3-3 Database Options Dialog Box**



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 11** Click the radio button for either Install PostgreSQL or Use existing DB to specify which database you want to use.

If you choose Install PostgreSQL, accept the defaults and enter a password. The PostgreSQL database will be installed.



**Note** If you choose to install PostgreSQL, you must disable any security software you are running, because PostgreSQL may not install certain folders or users.



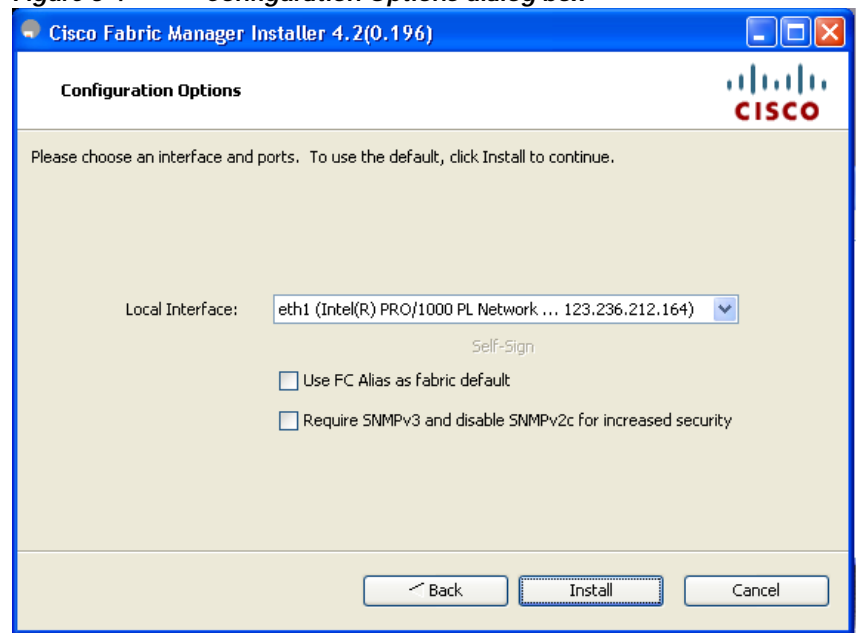
**Note** Before you install PostgreSQL, remove the **cygwin/bin** from your environment variable path if Cygwin is running on your system.

- Step 12** If you select Use existing DB, click the radio button for either PostgreSQL 8.1/8.2 or Oracle10g.

- Step 13** Click **Next** in the Database Options dialog box.

You see the ConfigurationOptions dialog box as shown in [Figure 3-4](#).

**Figure 3-4** Configuration Options dialog box



- Step 14** Click **Install** to install Fabric Manage Server.

## Unlicensed Versus Licensed Fabric Manager Server

When you install Fabric Manager, the basic unlicensed version of Fabric Manager Server is installed with it. To get the licensed features, such as Performance Manager, remote client support, and continuously monitored fabrics, you need to buy and install the Fabric Manager Server package.

However, trial versions of these licensed features are available. To enable the trial version of a feature, you run the feature as you would if you had purchased the license. You see a dialog box explaining that this is a demo version of the feature and that it is enabled for a limited time.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

If you are evaluating one of these Fabric Manager Server features and want to stop the evaluation period for that feature, you can do that using Device Manager.

## Data Migration in Fabric Manager Server

The database migration should be limited to the existing database. Data collision may occur when you merge the data between the several databases.

When you upgrade a non-federation mode database to federation mode database for the first time, we pre-fill the cluster sequence table with the values larger than the corresponding ones in sequence table and conforming to the cluster sequence number format for that server ID.

## Verifying Performance Manager Collections

Once Performance Manager collections have been running for five or more minutes, you can verify that the collections are gathering data by choosing **Performance Manager > Reports** in Fabric Manager. You see the first few data points gathered in the graphs and tables.

## Managing a Fabric Manager Server Fabric

You can continuously manage a Fabric Manager Server fabric, whether or not a client has that fabric open. A continuously managed fabric is automatically reloaded and managed by Fabric Manager Server whenever the server starts.

## Selecting a Fabric to Manage Continuously

To continuously manage a fabric using Fabric Manager, follow these steps:

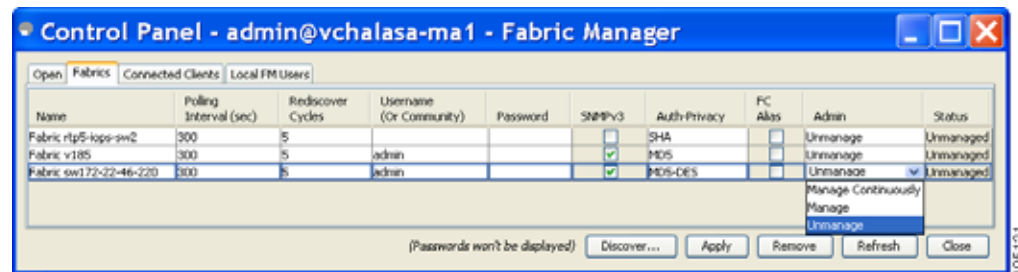
**Step 1** Choose **Server > Admin**.

You see the Control Panel dialog box with the Fabrics tab open as shown in [Figure 3-5](#).



**Note** The Fabrics tab is only accessible to network administrators.

**Figure 3-5** *Fabrics Tab in Control Panel Dialog Box*



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*



**Note** You can pre-configure a user name and password to manage fabrics. In this instance, you should use a local switch account, not a TACACS+ server.

- Step 2** Select one of the following Admin options:
- Manage Continuously**—The fabric is automatically managed when Fabric Manager Server starts and continues to be managed until this option is changed to Unmanage.
  - Manage**—The fabric is managed by Fabric Manager Server until there are no instances of Fabric Manager viewing the fabric.
  - Unmanage**—Fabric Manager Server stops managing this fabric.

**Step 3** Click **Apply**.



**Note** If you are collecting data on these fabrics using Performance Manager, you should now configure flows and define the data collections. These procedures are described in [Chapter 8, “Performance Manager.”](#)

## Fabric Manager Server Properties File

The Fabric Manager Server properties file (**MDS 9000\server.properties**) contains a list of properties that determine how the Fabric Manager Server will function. You can edit this file with a text editor, or you can set the properties through the Fabric Manager Web Services GUI, under the Admin tab.



**Note** As of Cisco NX-OS Release 4.1(1b) and later, you can optionally encrypt the password in the server.properties and the AAA.properties files.

The server properties file contains these nine general sections:

- **GENERAL**—Contains the general settings for the server.
- **SNMP SPECIFIC**—Contains the settings for SNMP requests, responses, and traps.
- **SNMP PROXY SERVER SPECIFIC**—Contains the settings for SNMP proxy server configuration and TCP port designation.
- **GLOBAL FABRIC**—Contains the settings for fabrics, such as discovery and loading.
- **CLIENT SESSION**—Contains the settings for Fabric Manager Clients that can log into the server.
- **EVENTS**—Contains the settings for syslog messages.
- **PERFORMANCE CHART**—Contains the settings for defining the end time to generate a Performance Manager chart.
- **EMC CALL HOME**—Contains the settings for the forwarding of traps as XML data using e-mail, according to EMC specifications.
- **EVENT FORWARD SETUP**—Contains the settings for forwarding events logged by Cisco Fabric Manager Server through e-mail.

The following are new or changed server properties for Fabric Manager Release 3.x:



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

#### SNMP Specific

- **snmp.preferTCP**—If this option is set to true, TCP will be the default protocol for the Fabric Manager Server to communicate with switches. By default, this setting is true. For those switches that do not have TCP enabled, the Fabric Manager Server uses UDP. The advantage of this setting is the ability to designate one TCP session for each SNMP user on a switch. It also helps to reduce time-outs and increase scalability.



**Note** If you set this option to false, the same choice must be set in Fabric Manager. The default value of **snmp.preferTCP** for Fabric Manager is true.

#### Performance Chart

- **pmchart.currenttime**—Specifies the end time to generate a Performance Manager chart. This should only be used for debugging purposes.

#### EMC Call Home

- **server.callhome.enable**—Enables or disables EMC Call Home. By default, it is disabled.
- **server.callhome.location**—Specifies the Location parameter.
- **server.callhome.fromEmail**—Specifies the 'From Email' list.
- **server.callhome.recipientEmail**—Specifies the 'recipientEmail' list.
- **server.callhome.smtphost**—Specifies the SMTP host address for outbound e-mail.
- **server.callhome.xmlDir**—Specifies the path to store the XML message files.
- **server.callhome.connectType**—Specifies the method to use to remotely connect to the server.
- **server.callhome.accessType**—Specifies the method to use to establish remote communication with the server.
- **server.callhome.version**—Specifies the version number of the connection type.
- **server.callhome.routerIp**—Specifies the public IP address of the RSC router.

#### Event Forwarding

- **server.forward.event.enable**—Enables or disables event forwarding.
- **server.forward.email.fromAddress**—Specifies the 'From Email' list.
- **server.forward.email.mailCC**—Specifies the 'CC Email' list.
- **server.forward.email.mailBCC**—Specifies the 'BCC Email' list.
- **server.forward.email.smtphost**—Specifies the SMTP host address for outbound e-mail.

#### Deactivation

- **deactivate.confirm=deactivate**—Specific Request for User to type a String for deactivation.

For more information on setting the server properties, read the `server.properties` file or see the [“Configuring Fabric Manager Server Preferences”](#) section on page 7-57.



**Note** In a federated server environment, you should not change Fabric Manager Server properties by modifying `server.properties` file. You must modify the `server.properties` using web client menu **Admin > Configure > Preferences**.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Modifying Fabric Manager Server

Fabric Manager Release 2.1(2) or later allows you to modify certain Fabric Manager Server settings without stopping and starting the server.

- [Adding or Removing Fabric Manager Server Users, page 3-10](#)
- [Changing the Fabric Manager Server User Name and Password, page 3-11](#)
- [Changing the Polling Period and Fabric Rediscovery Time, page 3-11](#)
- [Using Device Aliases or FC Aliases, page 3-12](#)

## Adding or Removing Fabric Manager Server Users

To add a Fabric Manager Server user or to change the password for an existing user using Fabric Manager, follow these steps:

- Step 1** Click the **Local FM Users** tab in the Control Panel dialog box as shown in [Figure 3-5](#). You see a list of Fabric Manager users.



**Note** Only network administrators can manage users.

- Step 2** Click **New** to add a user or click the user name and click **Edit** to change the password for an existing user. You see the FM User dialog box as shown in [Figure 3-6](#).

**Figure 3-6** FM User Dialog Box

- Step 3** Set the user name and password for the new user and then click **Apply**.

To remove a Fabric Manager Server user using Fabric Manager, follow these steps:

- Step 1** Click the **Local FM Users** tab in the Control Panel dialog box as shown in [Figure 3-5](#). You see a list of Fabric Manager users.
- Step 2** Click the user name you want to delete.
- Step 3** Click **Remove** to delete the user.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 4** Click **Yes** to confirm the deletion or **No** to cancel it.
- 

## Changing the Fabric Manager Server User Name and Password

You can modify the user name or password used to access a fabric from Fabric Manager Client without restarting Fabric Manager Server.

To change the user name or password used by Fabric Manager Server, follow these steps:

- 
- Step 1** Choose **Server > Admin**.
- You see the Control Panel dialog box with the Fabrics tab open as shown in [Figure 3-5](#).
- Step 2** Set the Name or Password for each fabric that you are monitoring with Fabric Manager Server.
- Step 3** Click **Apply** to save these changes.
- 

## Changing the Polling Period and Fabric Rediscovery Time

Fabric Manager Server periodically polls the monitored fabrics and periodically rediscovers the full fabric at a default interval of five cycles. You can modify these settings from Fabric Manager Client without restarting Fabric Manager Server.

To change the polling period or full fabric rediscovery setting used by Fabric Manager Server using Fabric Manager, follow these steps:

- 
- Step 1** Choose **Server > Admin**.
- You see the Control Panel dialog box with the Fabrics tab open as shown in [Figure 3-5](#).
- Step 2** For each fabric that you are monitoring with Fabric Manager Server, set the Polling Interval to determine how frequently Fabric Manager Server polls the fabric elements for status and statistics.
- Step 3** For each fabric that you are monitoring with Fabric Manager Server, set the Rediscover Cycles to determine how often Fabric Manager Server rediscovers the full fabric.
- Step 4** Click **Apply** to save these changes.

## Changing the IP Address of the Fabric Manager Server

To change the IP address of a Fabric Manager Server, follow these steps:

- 
- Step 1** Stop the Fabric Manager Server.
- Step 2** Change the following parameter in the \$INSTALLDIR/conf/FMServer.conf file as shown below.
- wrapper.app.parameter.4=127.0.0.1**
- Step 3** Change the following parameter in the \$INSTALLDIR/conf/server.properties file as shown below.
- server.bindaddrs = 127.0.0.1**

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 4** To assign a new IP address, enter the following command. Assume \$INSTALLDIR is the top directory of Fabric Manager installation and this is for single server instance, 0 is the server ID.
- Step 5** Run \$INSTALLDIR/bin/PLMapping.bat -p newipaddress 0
- 

## Using Device Aliases or FC Aliases

You can change whether Fabric Manager uses FC aliases or global device aliases from Fabric Manager Client without restarting Fabric Manager Server.

To change whether Fabric Manager uses FC aliases or global device aliases using Fabric Manager, follow these steps:

- Step 1** Choose **Server > Admin**.
- You see the Control Panel dialog box with the Fabrics tab open as shown in [Figure 3-5](#).
- Step 2** For each fabric that you are monitoring with Fabric Manager Server, check the **Device Alias** check box to use global device aliases, or uncheck to use FC aliases.
- Step 3** Click **Apply** to save these changes.
- 

## Server Federation

Server Federation is a distributed system that includes a collection of intercommunicated servers or computers that is utilized as a single, unified computing resource. With Fabric Manager Server federation, you can communicate with multiple servers together in order to provide scalability and easy manageability of data and programs running within the federation. The core of server federation includes several functional units such as Fabric Manager server, embedded web servers, database and Fabric Manager Client that accesses the servers.

The Fabric Manager Server in the federation uses the same database to store and retrieve data. The database is shared among different servers to share common information. A Fabric Manager client or Fabric Manager web client can open fabrics from the Fabric Manager Server using the mapping table. A fabric can be moved from one logical server to another. A logical server also can be moved from one physical machine to another machine.



### Note

You cannot upgrade more than one Fabric Manager Server in an existing federation. If you choose to do so, you may not be able to migrate the Performance Manager statistics and other information on that server.

---



### Note

You may require to synchronize the time on all the Fabric Manager Servers in a federated server environment.

---

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Note**

Server Federation is a licensed feature. For more information on Fabric Manager Server Licensing, see *Cisco MDS 9000 Family NX-OS Licensing Guide*.

**Note**

For more information on deploying Fabric Manager Server in a federation, see *Cisco Fabric Manager Server Federation Deployment Guide*.

## Mapping Fabric ID to Server ID

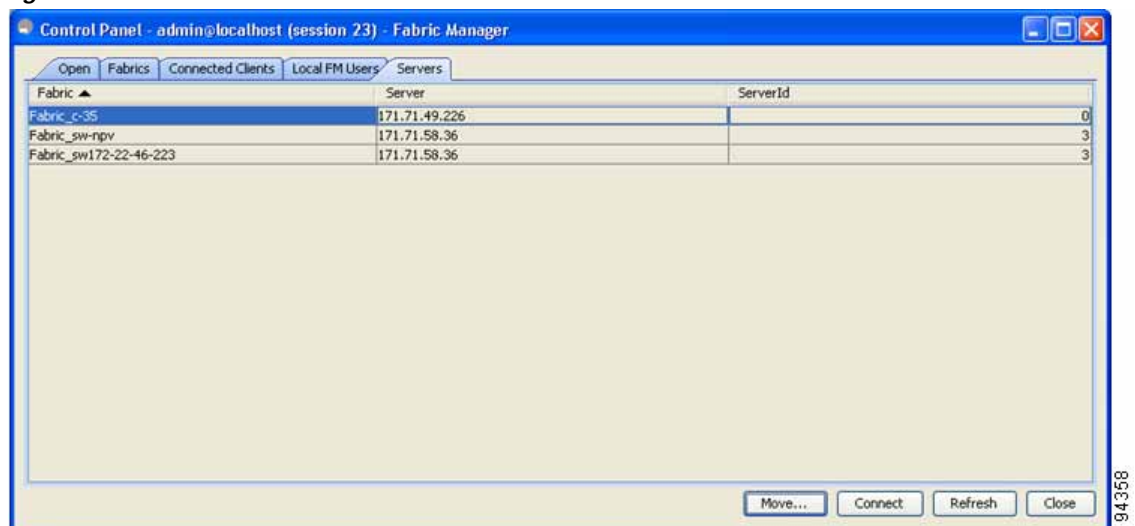
The IP address of the physical server will be mapped to the server ID during the installation of the Fabric Manager Server whenever the IP address of the physical server is changed, you need to map the IP address to the server ID using the PLMapping script provided with the Fabric Manager Server. Whenever the you open or discover a fabric, the fabric ID will be mapped to the server ID . You can move a fabric to a different server ID using the control panel.

To map a fabric to a different server, follow these steps:

**Step 1** Choose **Server > Admin**.

You see the Control Panel as shown in [Figure 3-7](#).

**Figure 3-7 Control Panel**

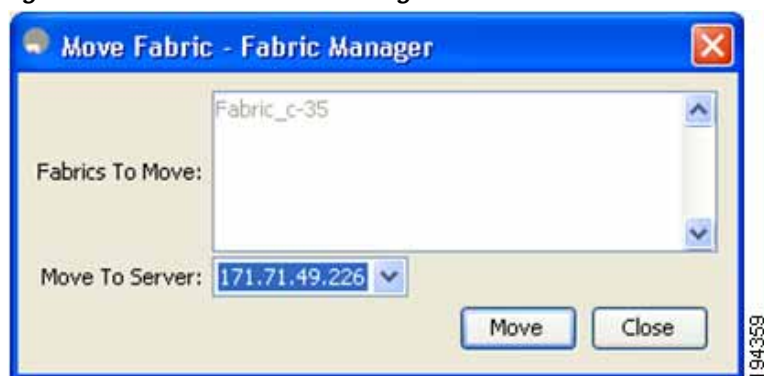


**Step 2** Select the fabric that you want to move to a different server and then click **Move**.

You see the Move Fabric dialog box as shown in [Figure 3-8](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 3-8** Move Fabric Dialog Box



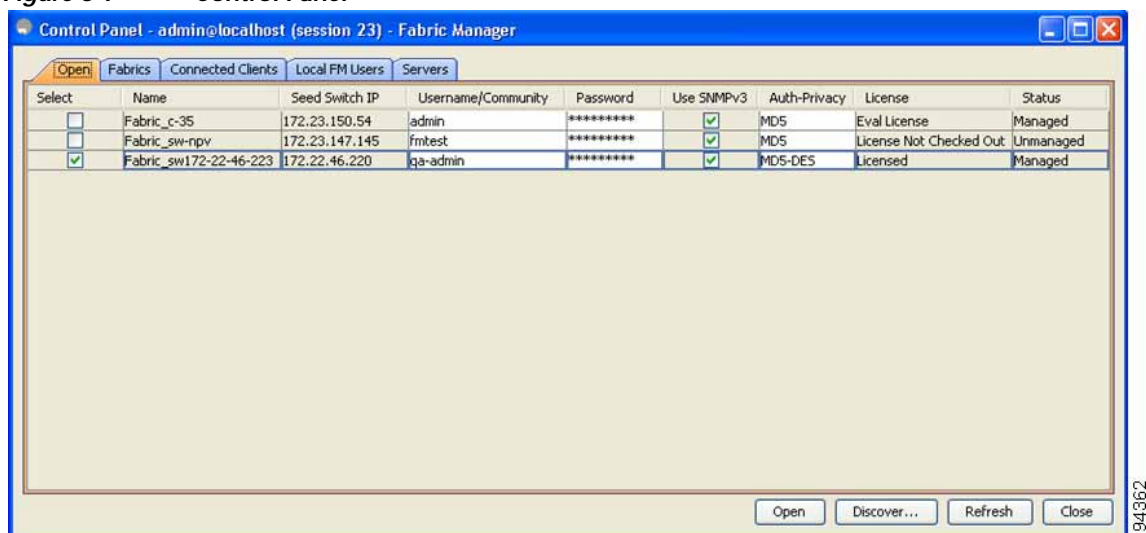
- Step 3** You see the fabrics that you selected in the Fabrics to Move list box. From the **Move To Server** drop-down list select the server you want to move the fabric to.
- Step 4** Click **Move**.

## Opening the Fabric on a Different Server

To open the fabric on a different server follow these steps:

- Step 1** Choose **Server > Admin**.  
You see the Control Panel as shown in Figure 3-9.

**Figure 3-9** Control Panel



- Step 2** Click **Discover**.  
You see the Discover New Fabric dialog box as shown in Figure 3-10.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 3-10** Discover new Fabric



- Step 3** In the Seed Switch list box, enter the IP Address of the seed switch.
- Step 4** In the User Name field, enter the user name.
- Step 5** In the password field, enter the password.
- Step 6** From the Auth-Privacy drop-down list, choose the privacy protocol you want to apply.
- Step 7** To open the selected fabric in a different server, select the server ID from the Server drop-down list.
- Step 8** Click **Discover**.



**Note**

You may receive an error message when you discover a fabric in a federation while another Fabric Manager Server is joining the federation. You can discover the fabric on after the installation or upgradation is complete.

## Viewing the Sessions in a Federation

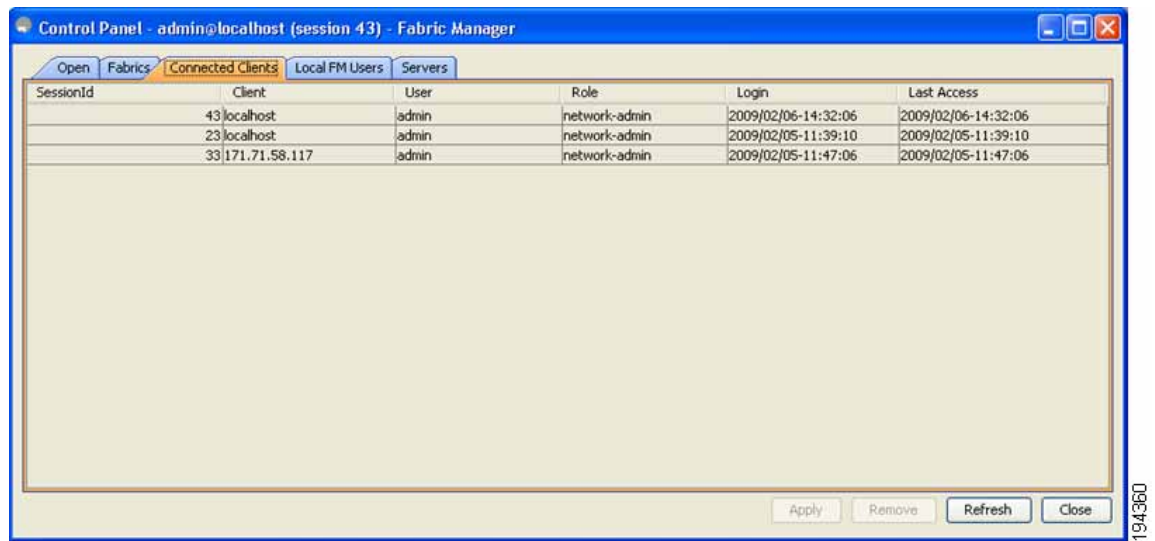
To view all the sessions in a federation, follow these steps:

- Step 1** Choose **Server > Admin**.
- Step 2** Click the **Connected Clients** tab.

You see the Control Panel as shown in [Figure 3-11](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 3-11**      **Connected Clients**



## Viewing the Servers in a Federation

To view all the servers in a federation, follow these steps:

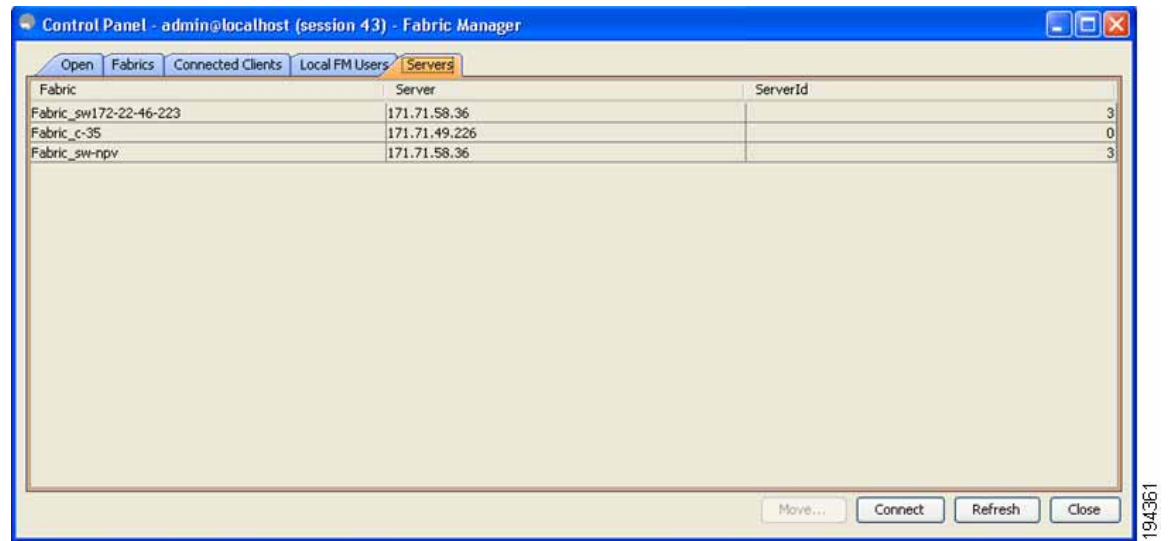
- Step 1 Choose **Server > Admin**.
- Step 2 Click the **Servers** tab.

You see the Control Panel as shown in [Figure 3-12](#).



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 3-12 Servers**



194361

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*



## CHAPTER 4

# Authentication in Fabric Manager

---

Fabric Manager contains interdependent software components that communicate with the switches in your fabric. These components use varying methods to authenticate to other components and switches. This chapter describes these authentication steps and the best practices for setting up your fabric and components for authentication.

This chapter contains the following sections:

- [Fabric Manager Authentication Overview, page 4-1](#)
- [Best Practices for Discovering a Fabric, page 4-3](#)
- [Performance Manager Authentication, page 4-4](#)
- [Fabric Manager Web Server Authentication, page 4-4](#)

## Fabric Manager Authentication Overview

Fabric Manager contains multiple components that interact to manage a fabric.

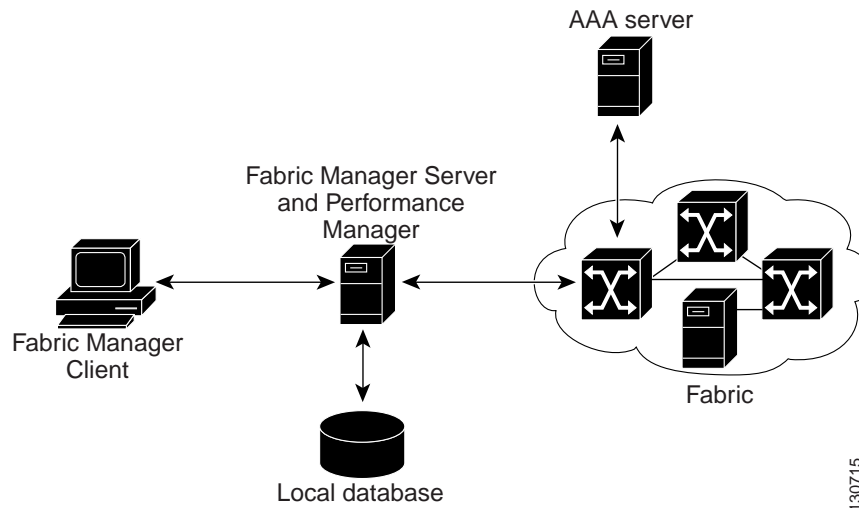
These components include:

- Fabric Manager Client
- Fabric Manager Server
- Performance Manager
- Interconnected fabric of Cisco MDS 9000 switches and storage devices
- AAA server (optional)

[Figure 4-1](#) shows an example configuration for these components.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 4-1 Fabric Manager Authentication Example**



Administrators launch Fabric Manager Client and select the seed switch that is used to discover the fabric. The user name and password used are passed to Fabric Manager Server and used to authenticate to the seed switch. If this user name and password are not a recognized SNMP user name and password, either Fabric Manager Client or Fabric Manager Server opens a CLI session to the switch (SSH or Telnet) and retries the user name and password pair. If the user name and password are recognized by the switch in either the local switch authentication database or through a remote AAA server, then the switch creates a temporary SNMP user name that is used by Fabric Manager Client and server.



**Note**

You may encounter a delay in authentication if you use a remote AAA server to authenticate Fabric Manager or Device Manager.



**Note**

You must allow CLI sessions to pass through any firewall that exists between Fabric Manager Client and Fabric Manager Server. See the [“Running Fabric Manager Behind a Firewall”](#) section on page 2-41.



**Note**

We recommend that you use the same password for the SNMPv3 user name authentication and privacy passwords as well as the matching CLI user name and password.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Best Practices for Discovering a Fabric

Fabric Manager Server monitors multiple physical fabrics under the same user interface. This facilitates managing redundant fabrics. A licensed Fabric Manager Server maintains up-to-date discovery information on all configured fabrics so device status and interconnections are immediately available when you launch Fabric Manager Client.



### Caution

If the Fabric Manager Server's CPU usage exceeds 50 percent, it is recommended that you switch to a higher CPU-class system. For more information on recommended hardware, see the [“Before You Install” section on page 2-19](#).

We recommend you use these best practices for discovering your network and setting up Performance Manager. This ensures that Fabric Manager Server has a complete view of the fabric. Subsequent Fabric Manager Client sessions can filter this complete view based on the privileges of the client logging in. For example, if you have multiple VSANs in your fabric and you create users that are limited to a subset of these VSANs, you want to initiate a fabric discovery through Fabric Manager Server using a network administrator or network operator role so that Fabric Manager Server has a view of all the VSANs in the fabric. When a VSAN-limited user launches Fabric Manager Client, that user sees only the VSANs they are allowed to manage.



### Note

Fabric Manager Server should always monitor fabrics using a local switch account, do not use a AAA (RADIUS or TACACS+) server. You can use a AAA user account to log into the clients to provision fabric services. For more information on Fabric Manager Server fabric monitoring, see the [“Managing a Fabric Manager Server Fabric” section on page 3-7](#).

## Setting Up Discovery for a Fabric

To ensure that Fabric Manager Server discovers your complete fabric, follow these steps:

- Step 1** Create a special Fabric Manager administrative user name in each switch on your fabric with network administrator or network operator roles. Or, create a special Fabric Manager administrative user name in your AAA server and set every switch in your fabric to use this AAA server for authentication.
- Step 2** Verify that the roles used by this Fabric Manager administrative user name are the same on all switches in the fabric and that this role has access to all VSANs.
- Step 3** Launch Fabric Manager Client using the Fabric Manager administrative user. This ensures that your fabric discovery includes all VSANs.
- Step 4** Set Fabric Manager Server to continuously monitor the fabric.  
See the [“Managing a Fabric Manager Server Fabric” section on page 3-7](#).
- Step 5** Repeat [Step 4](#) for each fabric that you want to manage through Fabric Manager Server.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Performance Manager Authentication

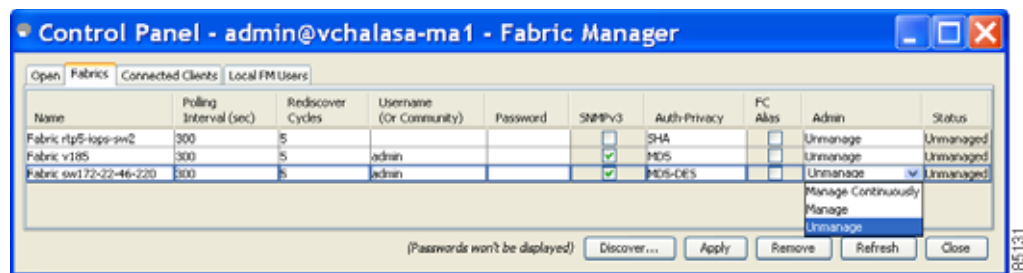
Performance Manager uses the user name and password information stored in the Fabric Manager Server database. If this information changes on the switches in your fabric while Performance Manager is running, you need to update the Fabric Manager Server database and restart Performance Manager. Updating the Fabric Manager Server database requires removing the fabric from Fabric Manager Server and rediscovering the fabric.

To update the user name and password information used by Performance Manager, follow these steps:

**Step 1** Click **Server > Admin** in Fabric Manager.

You see the Control Panel dialog box with the Fabrics tab open (see [Figure 4-2](#)).

**Figure 4-2** Fabrics Tab in Control Panel Dialog Box



**Step 2** Click the fabrics that have updated user name and password information.

**Step 3** From the Admin listbox, select **Unmanage** and then click **Apply**.

**Step 4** Enter the appropriate user name and password and then click **Apply**.

**Step 5** From the Admin listbox, select **Manage** and then click **Apply**.

**Step 6** To rediscover the fabric, click **Open** tab and check the check box(es) next to the fabric(s) you want to open in the Select column.

**Step 7** Click **Open** to rediscover the fabric. Fabric Manager Server updates its user name and password information.

**Step 8** Repeat [Step 3](#) through [Step 7](#) for any fabric that you need to rediscover.

**Step 9** Choose **Performance > Collector > Restart** to restart Performance Manager and use the new user name and password.

## Fabric Manager Web Server Authentication

Fabric Manager Web Server does not communicate directly with any switches in the fabric. Fabric Manager Web Server uses its own user name and password combination that is either stored locally or stored remotely on an AAA server.

We recommend that you use a RADIUS or TACACS+ server to authenticate users in Fabric Manager Web Server.

To configure Fabric Manager Web Server to use RADIUS authentication, follow these steps:

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- 
- Step 1** Launch Fabric Manager Web Server.  
See the [“Launching Fabric Manager Web Client” section on page 7-7](#).
- Step 2** Click the **Admin** tab > **Configure** to update the authentication used by Fabric Manager Web Server.
- Step 3** Click **AAA**.
- Step 4** Set the authentication mode attribute to **radius**.
- Step 5** Set the RADIUS server name, shared secret, authentication method, and ports used for up to three RADIUS servers.
- Step 6** Click **Modify** to save this information.
- 

To configure Fabric Manager Web Server to use TACACS+ authentication, follow these steps:

- 
- Step 1** Launch Fabric Manager Web Server.  
See the [“Launching Fabric Manager Web Client” section on page 7-7](#).
- Step 2** Click **Admin** > **Configure** to update the authentication used by Fabric Manager Web Server.
- Step 3** Click **AAA**.
- Step 4** Set the authentication mode attribute to **tacacs**.
- Step 5** Set the TACACS+ server name, shared secret, authentication method, and port used for up to three TACACS+ servers.
- Step 6** Click **Modify** to save this information.
- 



**Note** Fabric Manager does not support SecureID because it is not compatible with SNMP authentication. Fabric Manager uses the same login credentials for all the switches in a fabric. Since SecureID cannot be used more than once for authentication, Fabric Manager will not be able to establish a connection to the second switch using a SecureID.

---

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*





## CHAPTER 5

# Fabric Manager Client

---

Cisco Fabric Manager Client is a java-based GUI application that provides access to the Fabric Manager applications from a remote workstation.

This chapter contains the following sections:

- [About Fabric Manager Client, page 5-1](#)
- [Launching Fabric Manager Client in Cisco SAN-OS Release 3.2\(1\) and Later, page 5-2](#)
- [Fabric Manager Client Quick Tour: Server Admin Perspective, page 5-10](#)
- [Fabric Manager Client Quick Tour: Admin Perspective, page 5-15](#)
- [Setting Fabric Manager Preferences, page 5-33](#)
- [Network Fabric Discovery, page 5-35](#)
- [Modifying the Device Grouping, page 5-37](#)
- [Controlling Administrator Access with Users and Roles, page 5-40](#)
- [Using Fabric Manager Wizards, page 5-40](#)
- [Fabric Manager Troubleshooting Tools, page 5-41](#)
- [Integrating Fabric Manager and Data Center Network Management Software, page 5-41](#)

## About Fabric Manager Client

Cisco Fabric Manager is a Java and SNMP-based network fabric and device management tool with a GUI that displays real-time views of your network fabric, including Cisco Nexus 5000 Series switches, Cisco MDS 9000 Family and third-party switches, hosts, and storage devices.

In addition to complete configuration and status monitoring capabilities for Cisco MDS 9000 Family switches and Cisco Nexus 5000 Series switches, Fabric Manager Client provides Fibre Channel troubleshooting tools. You can use these health and configuration analysis tools on the MDS 9000 Family switch or Cisco Nexus 5000 Series switch to perform Fibre Channel ping and traceroute.

Fabric Manager Release 4.1(1b) and later provides multilevel security system by adding a server admin role that allows access to limited features. The configuration capabilities of a server admin is limited to FlexAttach and relevant data.



**Note**

You must use the same release of Fabric Manager Client and Fabric Manager Server.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Fabric Manager Advanced Mode

Advanced mode is enabled by default and provides the full suite of Fabric Manager features, including security, IVR, iSCSI, and FICON. To simplify the user interface, from the list box in the upper right corner of the Fabric Manager Client, select **Simple**. In simple mode, you can access basic MDS 9000 features such as VSANs, zoning, and configuring interfaces. Advanced mode option is not available for server admin role.

## Launching Fabric Manager Client in Cisco SAN-OS Release 3.2(1) and Later



### Note

As of Cisco SAN-OS 3.x and NX-OS Release 4.x, the Fabric Manager Client login procedure has changed. If you are running a version of Cisco SAN-OS that is earlier than Cisco SAN-OS 3.2(1), follow the login instructions in the [“Setting the Seed Switch in Cisco SAN-OS Releases 3.1\(1\) to 3.2\(1\)”](#) section on page A-1 or the [“Setting the Seed Switch in Releases Prior to Cisco SAN-OS Release 3.1\(1\)”](#) section on page A-3.



### Note

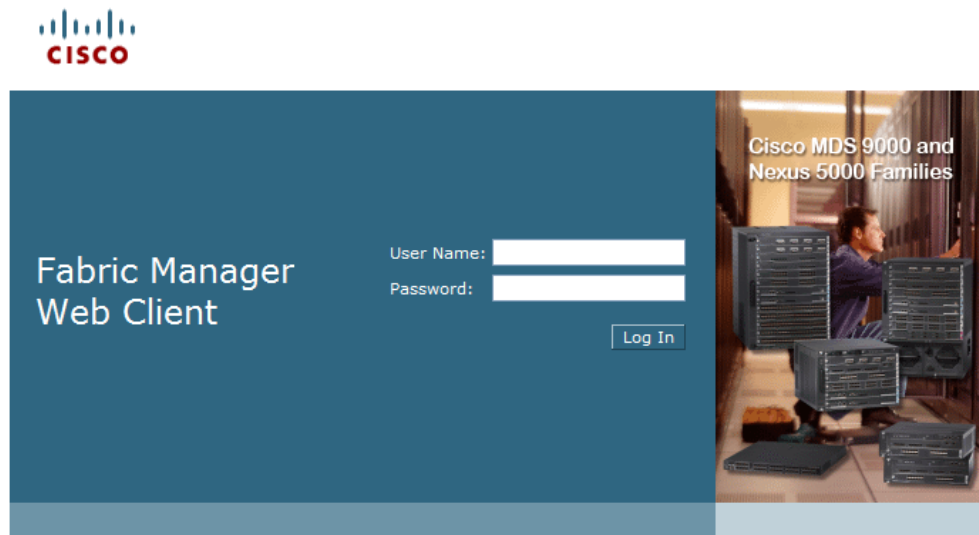
Network administrators must initially launch Fabric Manager Client using Fabric Manager Web Server, as described in the following procedure. Once an administrator has installed the Fabric Manager Client icon on your desktop, you can double-click the icon to launch the Fabric Manager Client.

To launch Fabric Manager Client, follow these steps:

- 
- Step 1** Open your browser and enter the IP address where you installed Fabric Manager Server, or enter localhost if you installed Fabric Manager Server on your local workstation.
- You see the Fabric Manager Web Server Login dialog box shown in [Figure 5-1](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 5-1** Fabric Manager Web Client Login Dialog Box



- Step 2** Enter your user name and password and click **Login**.  
You see the Fabric Manager Web Client Summary page.
- Step 3** Click the **Download** link in the upper right corner of the page.  
You see the Download page for Fabric Manager and Device Manager (see [Figure 5-2](#)).

**Figure 5-2** Download Page for Fabric Manager and Device Manager

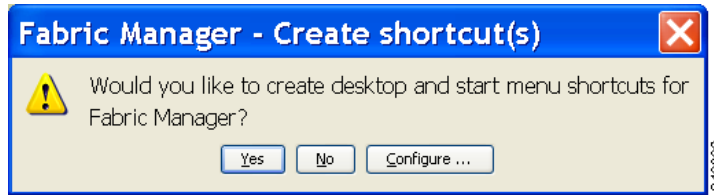


- Step 4** Click the link for **Fabric Manager**.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

If you are launching Fabric Manager Client for the first time, you see a message asking whether you want to create shortcuts for Fabric Manager (see [Figure 5-3](#)).

**Figure 5-3** Fabric Manager Create Shortcut(s) Message



**Step 5** Click **Yes** to create shortcuts for Fabric Manager.



**Note** This message only appears the first time you launch Fabric Manager Client. If you select No, your selection will be remembered and you will not be prompted to make a selection again. In this case, you will need to launch Fabric Manager Client using the Fabric Manager Web Client.

**Step 6** When the software is installed and icons are created on your desktop, double-click the Fabric Manager icon to launch Fabric Manager.

You see the Fabric Manager Login dialog box shown in [Figure 5-4](#).

**Figure 5-4** Fabric Manager Login Dialog Box



**Step 7** Enter the Fabric Manager Server user name and password.

**Step 8** Check the **Use SNMP Proxy** check box if you want Fabric Manager Client to communicate with Fabric Manager Server through a TCP-based proxy server.

**Step 9** Click **Login**. Once you successfully log in to Fabric Manager Server, you can set the seed switch and open the fabrics that you are entitled to access.



**Note** When you launch Fabric Manager Client for the first time or when there are no available fabrics, you see the Discover New Fabric dialog box.

You see the Discover New Fabric dialog box shown in [Figure 5-5](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 5-5 Discover New Fabric Dialog Box**



**Note** Only network administrators can discover new fabrics.

- Step 10** Click the **Ethernet (CDP)** radio button to discover using Cisco Discovery Protocol (CDP).
- Step 11** Starting from NX-OS Release 4.2(0), Fabric Manager uses Cisco Discovery Protocol to discover Ethernet switches such as Nexus 5000, Nexus 7000, Catalyst 4000, and Catalyst 6000 switches. You need to use a CDP seed switch for a CDP discovery.  
Set the fabric seed switch to the Cisco MDS 9000 Family switch or Cisco Nexus 5000 Series that you want Fabric Manager to use.
- Step 12** Choose the Auth-Privacy option according to the privacy protocol you have configured on your switch:
- If you have not configured the switch with a privacy protocol, then choose Auth-Privacy option MD5 (no privacy).
  - If you have configured the switch with your privacy protocol, choose your Auth-Privacy choice.



**Note** You may use SNMP v2 credentials for CDP discovery as the most of the Catalyst switches do not use MD5-DES for configuration.



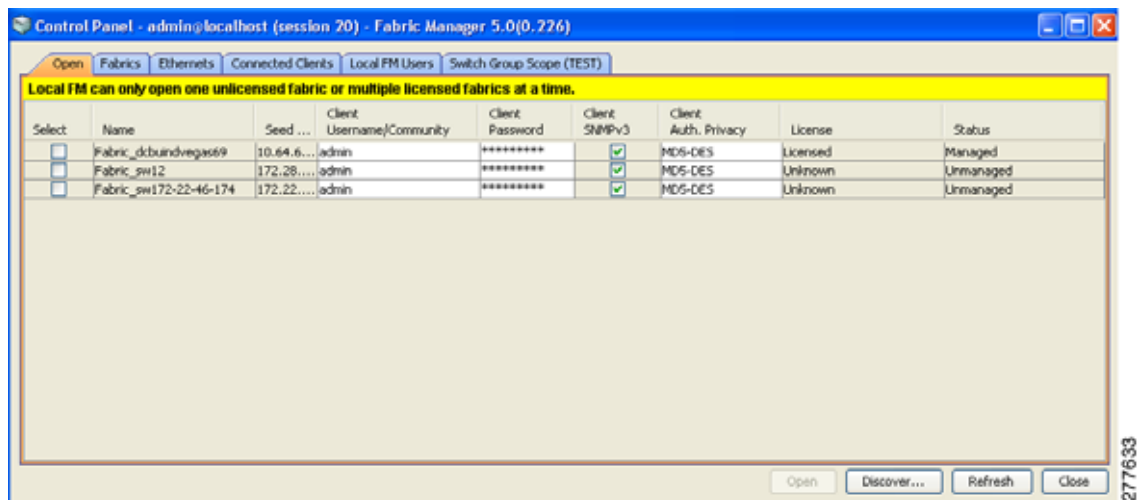
**Note** If you want a clean fabric discovery, remove the fabric and rediscover it. If you want a clean LAN discovery, unmanage LAN, remove the CDP seed switch and then rediscover it.

- Step 13** Enter the user name and password for the switch.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

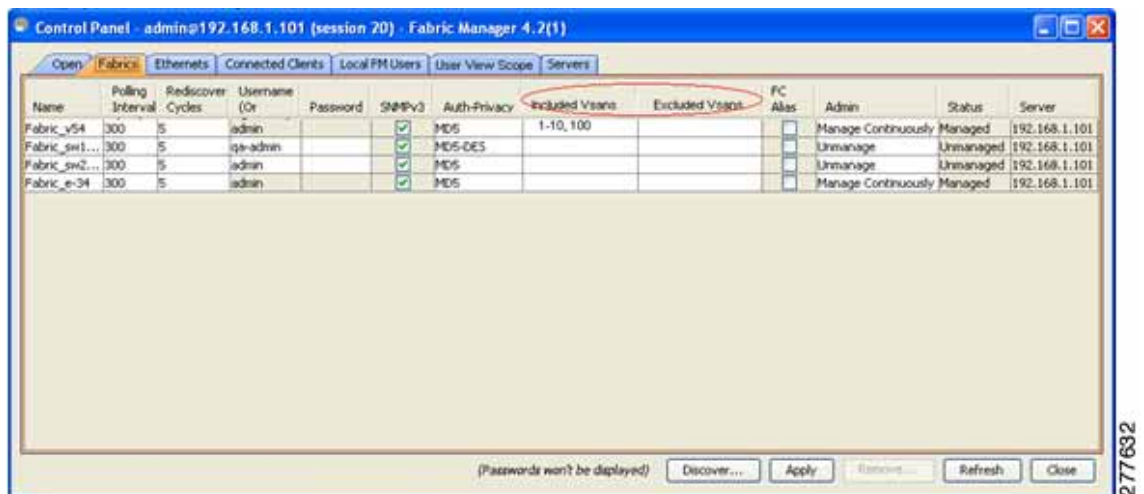
- Step 14** (Options!) To limit the discovery, specify the VSAN range.  
Scoping limits the resources discovered by Fabric Manager client. You can either include a range of VSANs to be discovered or exclude a range of VSANs from being discovered.
- To limit the discovery to a range of VSANs, click **Included VSAN List** radio button. Specify the range of VSANs.
  - To exclude a range of VSANs from being discovered, click **Excluded VSAN List** radio button. Specify the range of VSANs to be excluded.
- Step 15** Click **Discover**.
- You see the Control Panel dialog box shown in [Figure 5-6](#) and [Figure 5-7](#).

**Figure 5-6 Control Panel Dialog Box: Open Tab**



You see the included and excluded VSANs list under the Fabric tab.

**Figure 5-7 Control Panel Dialog Box: Fabrics Tab**



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Note**

You see a message in the dialog box when the server and client are running on the same workstation and there are unlicensed fabrics in the database. You also see a message when there are unmanaged fabrics (the state of the licenses is unknown).

**Note**

In the open tab, you see all the discovered fabrics displayed in the control panel. You need to click on the Open button to see all the discovered Ethernet switches.

- Step 16** Check the check box(es) next to the fabric(s) you want to open in the Select column, or click **Discover** to add a new fabric.

**Note**

Only network administrators can continuously manage or unmanage fabrics. For more information, see the [“Selecting a Fabric to Manage Continuously”](#) section on page 3-7.

- Step 17** Click **Open** to open the selected fabric(s).

**Note**

- If you have an incomplete view of your fabric, rediscover the fabric with a user that has no VSAN restriction.
- If the fabric includes a Cisco Nexus 5000 Series switch, then the Layer 2 node appears under the Switches > Interfaces > Ethernet tree, the VFC (FCoE) node appears under the Switches > Interfaces tree, and the FCoE node appears under the Switches tree in the Physical Attributes pane.
- For Cisco Nexus 5000 Series switches in the fabric, the tooltip for the switch shows the bind information of a virtual Fibre Channel interface to its corresponding Ethernet interface, such as vfc2(eth1/4).

To launch Fabric Manager Client from within a running instance of Fabric Manager, follow these steps:

- Step 1** Choose **File > Open** or click the **Open Switch Fabric** icon on the Fabric Manager toolbar.

You see the Control Panel dialog box (see [Figure 5-6](#)).

- Step 2** Check the check box(es) next to the fabric(s) you want to open in the Select column and click **Open**.

**Note**

Changes made using Fabric Manager are applied to the running configuration of the switches that you are managing. If you have made changes to the configuration or performed an operation (such as activating zones), Fabric Manager prompts you to save your changes before you exit.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Launching Fabric Manager Client Using Launch Pad

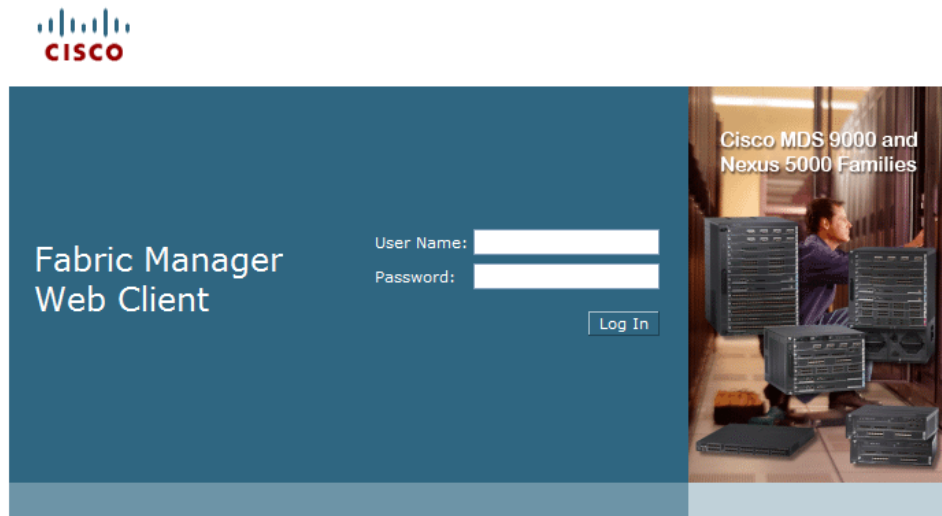
Starting from Cisco NX-OS Release 4.2(0), you can use Fabric Manager launch pad to connect to any server by specifying the IP address of the server. With launch pad, you can connect to any Fabric Manager Server version 3.3(0) and later. Launch pad establishes connection with the server using HTTP protocol.

To launch Fabric Manager Client using launch pad, follow these steps:

- 
- Step 1** Open your browser and enter the IP address where you installed Fabric Manager Server, or enter localhost if you installed Fabric Manager Server on your local workstation.

You see the Fabric Manager Web Server Login dialog box shown in [Figure 5-8](#).

**Figure 5-8** Fabric Manager Web Client Login Dialog Box



- Step 2** Enter your user name and password and click **Login**.  
You see the Fabric Manager Web Client Summary page.
- Step 3** Click the **Download** link in the upper right corner of the page.  
You see the Download page for Fabric Manager and Device Manager (see [Figure 5-9](#)).



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 5-9 Download Page for Fabric Manager and Device Manager**



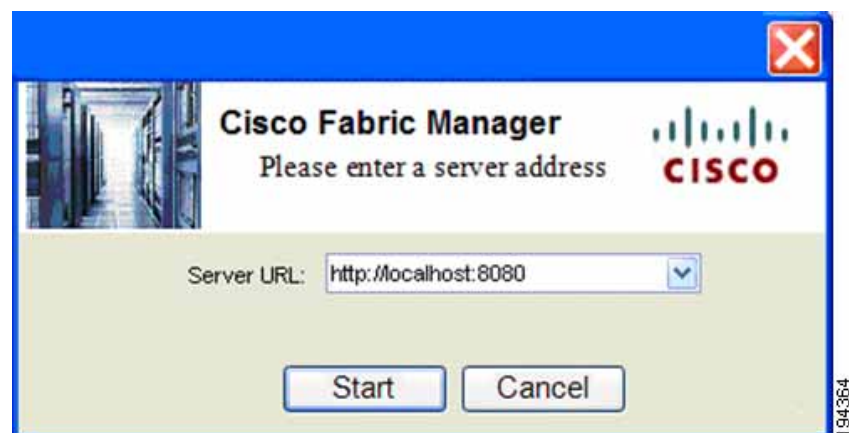
**Step 4** Click the link for **Fabric Manager**.

You see the Fabric Manager Server launch pad as in [Figure 5-10](#).

**Step 5** Enter the host name of the server or IP address in the **Server URL** drop-down list.

**Step 6** Click **Start**.

**Figure 5-10 Fabric Manager Launch Pad**



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Note**

Launch pad retains the history of the server URLs used. You can choose one of the previously user Server URLs from the drop-down list.

## Fabric Manager Client Quick Tour: Server Admin Perspective

Fabric Manager Release 4.1(1b) and later provides a multilevel security system by adding a server admin role that allows access only to limited features. The configuration capabilities of a server admin role is limited to FlexAttach and relevant data. The server admin can pre-configure SAN for new servers, move a server to another port on the same NPV device or another NPV device and replace a failed server onto the same port without involving the SAN administrator. The server role admin will not be able to manage Fabric Manager users or connected clients.

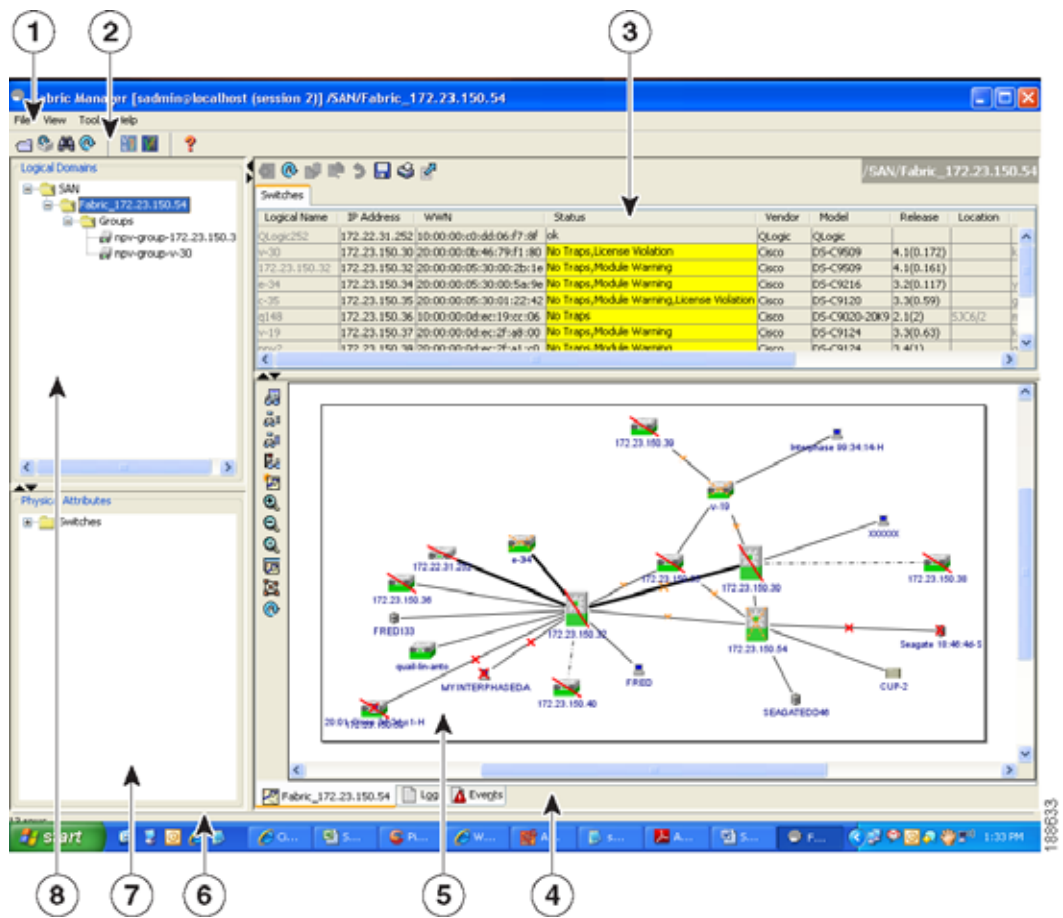
Fabric Manager Release 4.2(0) and later provides a much improved user interface by including movable and dockable panes to let users arrange the Physical Attributes pane, Logical Domains pane, Fabric pane and Information pane according to requirements, making it easier to manage the workflow. The dockable panes are also called as dockable frames. A dockable frame can be standalone (floating), minimized or maximized. The logical, physical, information and the fabric panes can be collapsed and expanded as needed. These panes can also be docked at either the right side left side or to the bottom of the workspace.

## Fabric Manager Main Window

This section describes the Fabric Manager Client interface that is specific to server admin users as shown in [Figure 5-11](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 5-11 Fabric Manager Main Window: Server Admin Perspective**



1	Menu bar—Provides access to options that are organized by menus.
2	Toolbar—Provides icons for direct access to the most commonly used options on the File, Tools, and Help menus.
3	Information pane—Displays information about whatever option is selected in the menu tree.
4	Status Bar (right side)—Shows the last entry displayed by the discovery process and the possible error message.
5	Fabric pane—Displays a map of the network fabric, including switches, hosts, and storage. It also provides tabs for displaying log and event data.
6	Status Bar (left side)—Shows short-term transient messages, such as the number of rows displayed in a table.
7	Physical Attributes pane—Displays a tree of available configuration tasks depending on the fabric, VSAN, or zone selected previously. Lists the switches in the logical selection.
8	Logical Domains pane—Displays a tree of configured SAN, fabrics and user-defined groups.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Menu Bar





The menu bar at the top of the Fabric Manager main window provides options for managing and for controlling the display of information on the Fabric pane. Server admin will not have all the options that are available for SAN admin. The menu bar provides the following menus:

- **File**—Opens a new fabric, rediscovers the current fabric, locates switches, sets preferences, prints the map.
- **View**—Changes the appearance of the map (these options are duplicated on the Fabric pane toolbar).
- **Tools**—Manages the Server and configuration using the FlexAttach virtual pWWN feature.
- **Help**—Displays online help topics for specific dialog boxes in the Information pane.

## Tool Bar

The Fabric Manager main toolbar (specific to server admin) provides icons for accessing the most commonly used menu bar options as shown in [Table 5-1](#).

**Table 5-1**      *Fabric Manager Client Main Toolbar*

Icon	Description
	Opens switch fabric.
	Rediscovers current fabric.
	Finds in the map.
	Shows online help.

## Logical Domains Pane

Use the Logical Domains pane to view fabrics and to access user-defined groups. You can expand the groups to see different user-defined groups. The non-editable groups created for each core switch contains their NPV switches.

## Physical Attributes Pane

Use the Physical Attributes pane to display a tree of the options available for managing the switches in the currently selected fabric or group.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*










To select an option, click a folder to display the options available and then click the option. You see the table with information for the selected option in the Information pane. The Physical Attributes pane provides the following main folders:

- Switches—Views and configures hardware, system, licensing, and configuration files.
- Interfaces—Views and configures FC physical, FC logical, VFC (FCoE), Ethernet, SVC, and PortChannel interfaces.

## Information Pane

Use the Information pane to display tables of information associated with the option selected from the menu tree in the Logical Domains or Physical Attributes panes. The Information pane toolbar provides buttons for performing one or more of the operations shown in Table 5-2.

**Table 5-2** Information Pane Toolbar

Icons	Description
	Applies configuration changes.
	Refreshes table values.
	Copies data from one row to another.
	Pastes the data from one row to another.
	Undoes the most recent change.
	Finds a specified string in the table.
	Exports and saves information to a file.
	Prints the contents of the Information pane.
	Displays a non-editable copy of the table in the Information pane in its own window, which you can move around the screen.

*[Send documentation comments to fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Fabric Pane

Use the Fabric pane to display the graphical representation of your fabric. Table 5-1 explains the graphics you may see displayed, depending on which devices you have in your fabric.

The bottom of the Fabric pane has the following tabs:

- Fabric—When displaying multiple fabrics, each fabric has its own tab. You can switch between fabrics by clicking on their respective tabs.
- Log—Displays messages that describe Fabric Manager operations, such as fabric discovery.
- Events—Displays information about the SNMP traps received by the management station. This includes combination events as detected by discovery and important traps such as license, SNMP, and FICON.



---

**Note**

---

Fabric map display is based on what you select in the logical domain pane. When you select a fabric node, all the switches that belong to that fabric will be enabled. When you select the group node, all the switches that belong to the groups listed under that group node will be enabled. When you select only a group, all the switches that belong to the specific group will be enabled.

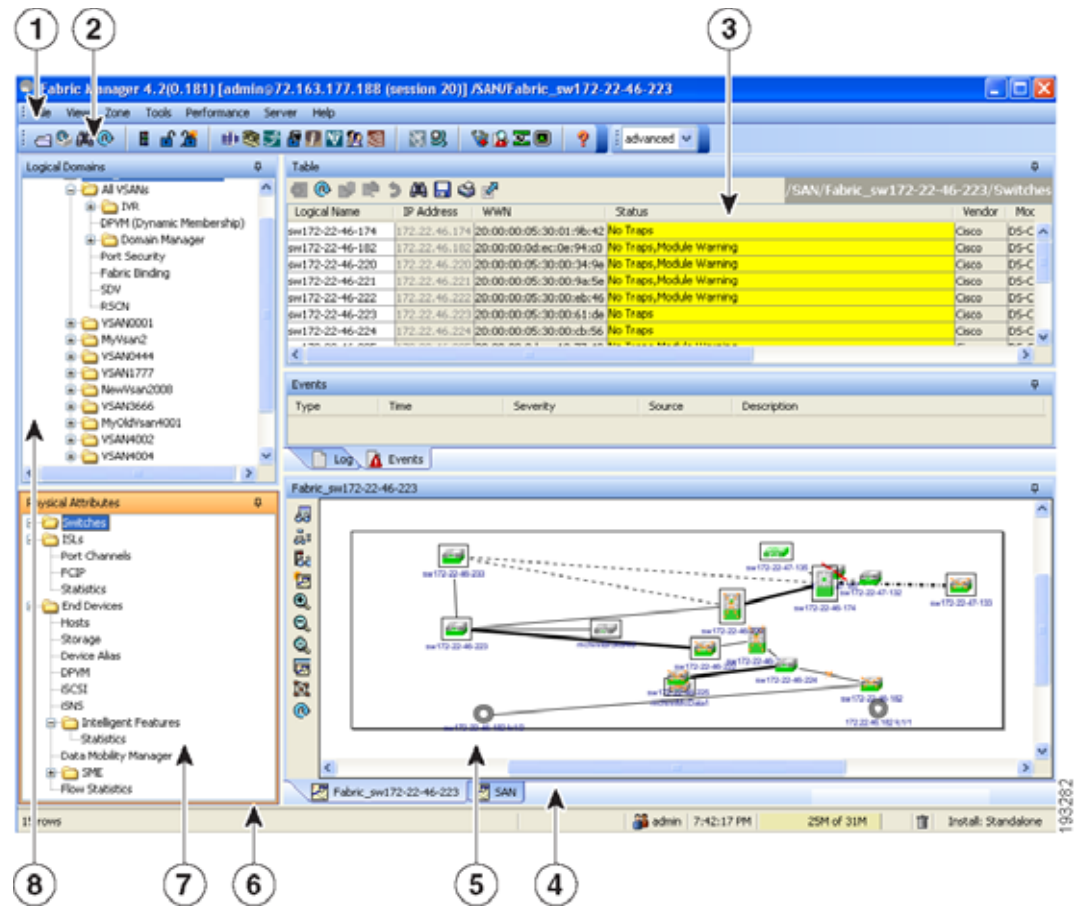
---

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Fabric Manager Client Quick Tour: Admin Perspective

This section describes the Fabric Manager Client interface shown in Figure 5-12.

**Figure 5-12** Fabric Manager Main Window



1	Menu bar—Provides access to options that are organized by menus.
2	Toolbar—Provides icons for direct access to the most commonly used options on the File, Tools, and Help menus.
3	Information pane—Displays information about whatever option is selected in the menu tree.
4	Status Bar (right side)—Shows the last entry displayed by the discovery process and the possible error message.
5	Fabric pane—Displays a map of the network fabric, including switches, hosts, and storage. It also provides tabs for displaying log and event data.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

6	Status Bar (left side)—Shows short-term transient messages, such as the number of rows displayed in a table.
7	Physical Attributes pane—Displays a tree of available configuration tasks depending on the fabric, VSAN, or zone selected previously. Lists the switches and end devices in the logical selection.
8	Logical Domains pane—Displays a tree of configured SAN, fabrics, VSANs, and zones, and provides access to user-defined groups. The label next to the segmented VSAN indicates the number of segments.



#### Note

You can resize each pane by dragging the boundaries between each region or by clicking the **Minimize** or **Maximize** controls.

## Menu Bar

The menu bar at the top of the Fabric Manager main window provides options for managing and troubleshooting the current fabric and for controlling the display of information on the Fabric pane. The menu bar provides the following menus:

- **File**—Opens a new fabric, rediscovers the current fabric, locates switches, sets preferences, prints the map, and exports the Fabric pane log.
- **View**—Changes the appearance of the map (these options are duplicated on the Fabric pane toolbar).
- **Zone**—Manages zones, zone sets, and inter-VSAN routing (IVR).
- **Tools**—Verifies and troubleshoots connectivity and configuration, as described in the “[Fabric Manager Troubleshooting Tools](#)” section on page 5-41.
- **Performance**—Runs and configures Performance Manager and Cisco Traffic Analyzer, and generates reports.
- **Server**—Runs administrative tasks on clients and fabrics. Provides Fabric Manager Server management and a **purge** command. Lists fabrics being managed.
- **Help**—Displays online help topics for specific dialog boxes in the Information pane.

## File

The file menu provides the following options:

- **Open Fabric**—Opens a new switch fabric.
- **Locate Switches and Devices**— Uses the SNMPv2 protocol to discover devices responding to SNMP requests with the read-only community string public. You may use this feature if you want to locate other Cisco MDS 9000 switches in the subnet, but are not physically connected to the fabric.
- **Rediscover**—Initiates an on-demand discovery to learn recent changes from the switches and update the Fabric Manager Client. You may use this option when Fabric Manager Server is not in sync with switches in the fabric and you do not want to wait until the next polling cycle. The rediscover option does not delete the fabric and add it again. You may delete and add the fabric only if the rediscover option fails to update Fabric Manager Server.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Resync All Open Fabrics— Fabric Manager Server forces all the fabrics to close and re-open. You may use this option when Fabric Manager Client is not in sync with Fabric Manager Server.
- Rediscover SCSI Targets— Initiates an on-demand discovery to learn recent changes from the SCSI target switches. You may use this option when Fabric Manager Server is not in sync with SCSI target switches in the fabric and you do not want to wait until the next polling cycle.
- Preferences—Sets your preferences to customize the behavior of the Fabric Manager Client.
- Import Enclosures—Imports saved enclosures.
- Export
  - Map Image—Generates and export the map to a specified location.
  - Visio—Exports the map to a Visio file.
  - Table—Exports the table data to a text file.
  - Log—Exports the log to a text file.
  - Events—Exports the events to a text file.
  - Enclosures—Exports the enclosure values to a text file.
- Print —Prints the map.
- Exit—Exit Fabric Manager.

## View

View menu provides the following options:

- Refresh Map—Refreshes the current map.
- Layout
  - Cancel—Cancels the current layout.
  - Spring—Displays the layout based on spring algorithm.
  - Quick—Quickly displays the layout when the switch has many end devices.
- Zoom
  - In—Zooms in the view.
  - Out—Zooms out the view.
  - Fit—Fits the view in the fabric pane.
- Grid—Enables the grid view.
- Overview Window—Allows you to center the Fabric pane on the area of the fabric that you want to see. This option is useful for large fabrics that cannot be displayed entirely within the Fabric pane.
- Legend—Shows all the legends used in the fabric map.
- Find in Map—Finds a device in the fabric map.

## Zone

The zone menu provides the following options:

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Edit Local Full Zone Database—Allows you to create zones across multiple switches. Zones provide a mechanism for specifying access control. Zone sets are a group of zones to enforce access control in the fabric. All zoning features are available through the Edit Local Full Zone Database dialog box.
- Deactivate Zoneset—Deactivates an active zone set.
- Copy Full Zone Database—Creates a new zone set. On the Cisco MDS Family switches, you cannot edit an active zone set. However, you can copy an active zone set to create a new zone set that you can edit.
- Merge Analysis—Enables you to determine if zones will merge successfully when two Cisco MDS switches are interconnected. If the interconnected switch ports allow VSANs with identical names or contain zones with identical names, then Fabric Manager verifies that the zones contain identical members. You can use merge analysis tool before attempting a merge, or after fabrics are interconnected to determine zone merge failure causes.
- Merge Fail Recovery—Recovers the port from its isolated state either by importing the neighboring switch's active zone set database and replacing the current active or by exporting the current database to the neighboring switch.
- Migrate Non-MDS Database—Migrate a non-MDS database using Fabric Manager (you may need to use the Zone Migration Wizard to accomplish this task).
- IVR
  - Deactivate Zoneset—Deactivates an active zone set.
  - Copy Full Zone Database—Recovers an IVR zone database by copying the IVR full zone database from another switch.
  - Copy Full Topology—Recovers a topology by copying from the active zone database or the full zone database.

## Tools

Tools menu provides the following options:

- Health
  - Switch Health—Determines the status of the components of a specific switch.
  - Fabric Configuration—Analyzes the configuration of a switch by comparing the current configuration to a specific switch or to a policy file. You can save a switch configuration to a file and then compare all switches against the configuration in the file.
  - Show Tech Support—Collects large amount of information about your switch for troubleshooting purposes. When you issue a **show tech support** command from Fabric Manager for one or more switches in a fabric, the results of each command are written to a text file, one file per switch, in a directory you specify. You can then view these files using Fabric Manager.
- Connectivity
  - End to End Connectivity—Determines connectivity and routes among devices with the switch fabric. This tool checks to see that every pair of end devices can talk to each other, using a Ping test and by determining if they are in the same VSAN or in the same active zone.
  - Ping—Determines connectivity from another switch to a port on your switch.
  - Trace Route—Verifies connectivity between two end devices that are currently selected on the Fabric pane.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Compact Flash Report—Automatically scans the fabric and generate a report that shows the status of CompactFlash.
- NPV
  - CFS Static Peer Setup—Manage the peer list used during CFS on NPV-enabled switches. After setting up the static peers list, the CFS discovery on the switches will be changed to static mode for all peers in the list. Fabric Manager does not automatically update static peers list. You may need to update the list using the CFS Static Peer Setup Wizard when a new switch is added to the fabric.
  - Traffic Map Setup—Configures the list of external interfaces to the servers, and enabling or disabling disruptive load balancing. Using Traffic Map Setup you can specify the external ports that a server should use for traffic management.
  - Flex Attach Pre-Configure Server—Sets the port configurations for all the ports in a switch such as enabling or disabling FlexAttach, setting the default VSAN ID, and setting the interface status.
  - Flex Attach Move Server—Moves a server to another port on the same NPV device or another NPV device without changing the SAN.
  - Flex Attach Replace Server—Replaces a failed server with a new server on the same port without changing the SAN.
- Data Mobility Manager
  - Server Based—Performs server-based data migration.
  - Storage based—Performs storage-based data migration.
  - Server LUN Discovery—Performs LUN discovery to select the LUNs available for migration and automates the session creation by matching the LUNs in the existing and new storage.
- FCoE—Launches the FCoE Configuration Wizard to create virtual Fibre Channel interfaces.
- Port Channel—Creates PortChannels from selected ISL either manually or automatically.
- DPVM Setup—Establishes dynamic port VSAN membership, enables autolearning, and activates the DPVM database.
- IP SAN
  - FCIP Tunnel—Creates FCIP links between Gigabit Ethernet ports. Enables Fibre Channel write acceleration and IP compression.
  - iSCSI Setup—Creates zones for iSCSI initiators and adds a VSAN to a target-allowed VSAN list.
  - SAN Extension Tuner—Optimizes FCIP performance by generating either direct access (magnetic disk) or sequential access (magnetic tape) SCSI I/O commands and directing such traffic to a specific virtual target. This option is used to generate SCSI I/O commands (read and write) to the virtual target based on your configured options.
- Security
  - Port Security—Prevents unauthorized access to a switch port in the Cisco MDS 9000 Family, rejects intrusion attempts and reports these intrusions to the administrator.
  - IP ACL—Creates an ordered list of IP filters in a named IPv4-ACL or IPv6-ACL profile using the IPv4-ACL Wizard.
- Install
  - License—Facilitate download and installation of licenses in selected switches in the fabric.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Software—Verifies image compatibility and installs software images on selected switches in the fabric.
- Flow Load Balance Calculator—Allows you to get the best load-balancing configuration for your FICON flows. The calculator does not rely on any switch or flow discovery in the fabric.
- Device Manager—Invokes Device Manager for a switch.
- Command Line Interface —Enables command-line operations.
- Run CLI Commands—Runs command-line operations on more than one switch at a time.

## Performance

The performance menu provides the following options:

- Create Flows—Creates host-to-storage, storage-to-host, or bidirectional flows. You can add these flows to a collection configuration file to monitor the traffic between a host or storage element pair.

## Server

The server menu provides the following options:

- Admin—Opens the control panel.
- Purge Down Elements—Purges all down elements in the fabric.

## Help




The help menu provides the following options:

- Contents —Launches the online help contents.
- Config Guide—Launches the Fabric Manager Configuration Guide.
- About—Displays information about Fabric Manager.

## Toolbar















The Fabric Manager main toolbar provides icons for accessing the most commonly used menu bar options as shown in [Table 5-3](#).

**Table 5-3**      *Fabric Manager Client Main Toolbar*

Icon	Description
	Opens switch fabric.
	Rediscovered current fabric.
	Finds in the map.







*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Table 5-3**      **Fabric Manager Client Main Toolbar (continued)**

Icon	Description
	Creates VSAN.
	Launches DPVM wizard.
	Launches Port Security wizard.
	Edits full zone database.
	Launches IVR zone wizard.
	Launches the FCoE configuration wizard.
	Launches PortChannel wizard.
	Launches FCIP wizard.
	Launches iSCSI wizard.
	Launches NPVM wizard.
	Launches QoS wizard.
	Configures users and roles.
	Launches IP-ACL wizard.
	Launches License Install wizard.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Table 5-3**      *Fabric Manager Client Main Toolbar (continued)*

Icon	Description
	Launches Software Install wizard.
	Performs switch health analysis.
	Performs fabric configuration analysis.
	Performs end-to-end connectivity analysis.
	Monitors ISL performance. Brings up real-time ISL performance information for all interfaces in the fabric, in the Information pane.
	Shows online help.

## Logical Domains Pane

Use the Logical Domains pane to manage attributes for fabrics, VSANs, and zones, and to access user-defined groups. Starting from NX-OS Release 4.2(0), SAN and LAN nodes are listed under Datacenter node and all the fabrics are listed under SAN node. When you select Datacenter node in the tree, Fabric Manager displays all the switches and ISLs. When you select LAN node, Fabric Manager displays only Ethernet switches and Ethernet links. Under the fabric node, VSANs are ordered by a VSAN ID. The segmented VSANs are placed under the fabric node. The label next to the segmented VSAN indicates the number of segments. You can expand a segmented VSAN and the segments under that VSAN. Right-click one of the folders in the tree and click a menu item from the pop-up menu. You see the appropriate configuration dialog box.

The default name for the fabric is the name, IP address, or WWN for the principal switch in VSAN 1. If VSAN 1 is segmented, the default name is chosen from a principal switch with the smallest WWN. The fabric names you see are as follows:

- Fabric <sysName>
- Fabric <ipAddress>
- Fabric <sWWN>

To change the fabric name using Fabric Manager, follow these steps:

---

**Step 1**      Choose **Server > Admin**.

You see the Control Panel dialog box.

**Step 2**      Double-click the fabric name and enter the new name of the fabric.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Step 3** Click **Apply** to change the name.

---

## Filtering

Fabric Manager has a filtering mechanism that displays only the data that you are interested in. To filter, first select the fabric and VSAN from the Logical Domains pane. This action narrows the scope of what is displayed in the Fabric pane. Any information that does not belong to the selected items is dimmed. Also, any information that does not belong to the selected items is not displayed in the tables in the Information pane. As shown in [Figure 5-13](#), the filter that you select is displayed at the top right of the Fabric Manager window.

To further narrow the scope, select attributes from the Physical Attributes pane. The Fabric Manager table, display, and filter criteria change accordingly.

## Physical Attributes Pane

Use the Physical Attributes pane to display a tree of the options available for managing the switches in the currently selected fabric, VSAN, or zone.

To select an option, click a folder to display the options available and then click the option. You see the table with information for the selected option in the Information pane. The Physical Attributes pane provides the following main folders:

- Switches—Views and configures hardware, system, licensing, and configuration files.
- Interfaces—Views and configures FC physical, FC logical, VFC (FCoE), Ethernet, SVC, and PortChannel interfaces.
- FC Services—Views and configures Fibre Channel network configurations.
- IP—Views and configures IP storage and IP services.
- Events—Views and configures events, alarms, thresholds, notifications, and informs.
- Security—Views and configures MDS management and FC-SP security.
- FCoE—Views and configures FCoE interfaces.
- ISLs—Views and configures Inter-Switch Links.
- End Devices—Views and configures end devices.



### Note

You cannot view the detailed physical attributes of the data center switches or monitor the connections. When you select either a data center node or a LAN node the physical attributes pane will be blank.

## Context Menu for Tables

When you right-click in the table, you see a pop-up menu with options that vary depending on the type of option you selected in the Physical Attributes pane. You can perform various operations by right-clicking the device listed in the table. To view various options available for switches, ISLs, and end devices, refer to the procedures in the sections that follows:

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Switch Options

When you select the datacenter node, the switch table displays all the switches that are discovered. When you select the SAN node or the fabric node, the switch table displays all the Fibre Channel switches and when you select the LAN node, the switch table displays all the Ethernet switches.

To view the options for the switch table, follow these steps:

---

**Step 1** Click **Switches** in the Physical Attributes pane.

**Step 2** Right-click the device in the table.

The pop-up menu provides the following options:

- Apply Changes—Applies the changes to the switch.
  - Refresh Values—Refreshes the current values.
  - Undo Changes—Undoes modifications to the switch.
  - Export to File—Export the values to a file.
  - Print Table—Prints the table.
  - Detach Table—Detaches the table.
  - Switch Attributes—Changes the switch properties.
  - Interface Attributes—Changes the interface properties.
  - Element Manager—Manages this switch.
  - Command Line Interface—Enables to perform command line operations.
  - Copy—Copies the switch.
  - Purge—Purges the switch.
  - Fix Location—Fixes the switch in the current location.
  - Align—Aligns the switch.
  - Show End Devices—Shows the end devices.
  - Expand Multiple Links—Expands the links to this switch.
  - Other—Other options.
  - Group—Groups switches.
- 

## ISL Options

When you select the data center node, the ISLs table displays all of the Fibre Channel and Ethernet links. When you select the LAN node, the ISLs table displays all the Ethernet links.

To view the options for the ISLs table, follow these steps:

---

**Step 1** In the Physical Attributes pane, click **ISLs** and then click **Summary** tab.

**Step 2** Right-click the device in the table.

The pop-up menu provides the following options:

- Refresh Values—Refreshes the current values.
- Copy—Copies information from a specific field.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Find—Conducts search based on the input string.
- Export to File—Exports the values to a file.
- Print Table—Prints the table.
- Detach Table—Detaches the table.
- Interface Attributes—Changes the interface properties.
- Element Manager—Manages the device.
- FCIP Tunnel Attributes—Changes FCIP tunneling properties.
- Create Port Channel—Creates port channel.
- Re-enable—Reenables a disabled device.
- Enable FC-SP—Enables FC-SP.
- SAN Extention Tuner—Optimizes FCIP performance.
- Purge—Purges the device.

**Note**

When you select a port channel from the table, the pop-up menu will have the following additional options:

- Member Attributes—Changes the member properties.
- Channel Attributes—Changes the port channel properties.
- Edit—Edits the channel properties.

## End Device Options

To view the options for the end devices table, follow these steps:

**Step 1** In the Physical Attributes pane, click **End Devices** and then click the **Summary** tab.

**Step 2** Right-click the device in the table.

The pop-up menu provides the following options:

- Apply Changes—Applies the changes to the device.
- Refresh Values—Refreshes the current values.
- Copy—Copies the information specific to the field.
- Paste—Pastes the copied text.
- Undo Changes—Undoes modifications to the device.
- Find—Searches for information depending on the input string.
- Export to File—Exports the values to a file.
- Print Table—Prints the table.
- Detach Table—Detaches the table.
- Device Attributes—Changes the device properties.
- Interface Attributes—Changes the interface properties.
- Element Manager—Manages this device.









*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Command Line Interface—Enables you to perform command line operations.
- Copy—Copies the switch.
- Purge—Purges the switch.
- Fix Location—Fixes the switch in the current location.
- Align—Aligns the switch.
- Ping—Pings another device.
- Trace Route—Determines the route taken by packets across the network.
- Select Dependent Ports—Selects dependent ports.
- Group—Groups devices.

## Information Pane




Use the Information pane to display tables of information associated with the option selected from the menu tree in the Logical Domains or Physical Attributes panes. The Information pane toolbar provides buttons for performing one or more of the operations shown in [Table 5-4](#).

**Table 5-4** Information Pane Toolbar

Icon	Description
	Applies configuration changes.
	Refreshes table values.
	Opens the appropriate dialog box to make a new row in the table.
	Deletes the currently highlighted rows from the table.
	Copies data from one row to another.
	Pastes the data from one row to another.
	Undoes the most recent change.
	Finds a specified string in the table.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Table 5-4 Information Pane Toolbar (continued)**

Icon	Description
	Exports and saves information to a file.
	Prints the contents of the Information pane.
	Displays a non-editable copy of the table in the Information pane in its own window, which you can move around the screen.



**Note**

After making changes, you must save the configuration or the changes will be lost when the device is restarted.



**Note**

The buttons that appear on the toolbar vary according to the option that you select. They are activated or deactivated (dimmed) according to the field or other object that you select in the Information pane.




## Detachable Tables

Detachable tables in Fabric Manager allow you to detach tables and move them to different areas on your desktop so that you can compare similar tables from different VSANs. You can keep informational tables open from one view while you examine a different area in Fabric Manager. To detach tables, click the **Detach Table** icon in the Information pane in Fabric Manager.

## Fabric Pane















Use the Fabric pane to display the graphical representation of your fabric. [Table 5-5](#) explains the graphics you may see displayed, depending on which devices you have in your fabric.

**Table 5-5 Fabric Manager Graphics**

Icon or Graphic	Description
	Director class MDS 9000 Fibre Channel switch.
	Non-director class MDS 9000 Fibre Channel switch.
	Nexus 7000 switch.







*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Table 5-5**      *Fabric Manager Graphics (continued)*

Icon or Graphic	Description
	Nexus FCoE or Fibre Channel switch.
	Catalyst LAN switch.
	Generic Fibre Channel switch.
	Cisco SN5428.
	Dashed or dotted orange line through a device indicates that the device is manageable but there are operational problems.
	Dashed or dotted orange X through a device or link indicates that the device or ISL is not working properly.
	A red line through a device indicates that the device is not manageable.
	A red X through a device or link indicates that the device is down or that the ISL is down.
	Fibre Channel HBA (or enclosure).
	Fibre Channel target (or enclosure).
	iSCSI host.
	Fibre Channel ISL and edge connection.
	Fibre Channel PortChannel.
	IP ISL and edge connection.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Table 5-5**      *Fabric Manager Graphics (continued)*

Icon or Graphic	Description
	IP PortChannel.
	DWDM connection.
	NPV connection.
	Fibre Channel loop (storage).
	IP cloud (hosts). This icon is also used to represent a fabric when viewing a SAN (multiple fabrics) in the Fabric Manager Fabric pane.
	Any device, cloud, or loop with a box around it means that there are hidden links attached.

If a switch or director is grayed out, Fabric Manager can no longer communicate with it.

The bottom of the Fabric pane has the following tabs:

- **Fabric**—When displaying multiple fabrics, each fabric has its own tab. You can switch between fabrics by clicking on their respective tabs.
- **Log**—Displays messages that describe Fabric Manager operations, such as fabric discovery.
- **Events**—Displays information about the SNMP traps received by the management station. This includes combination events as detected by discovery and important traps such as license, SNMP, and FICON.

When viewing large fabrics in the Fabric pane, it is helpful to do the following tasks:

- Turn off end device labels.
- Collapse loops.
- Collapse expanded multiple links (collapsed multiple links are shown as very thick single lines).
- Dim or hide portions of your fabric by VSAN.



**Note**

When a VSAN, zone, or zone member is selected in the VSAN tree, the map highlighting changes to identify the selected objects. To remove this highlighting, click the **Clear Highlight** button on the Fabric pane toolbar or choose **Clear Highlight** from the pop-up menu.

## Context Menus

When you right-click an icon in the Fabric pane, you see a pop-up menu with options that vary depending on the type of icon selected. The various options available for different objects include the following:

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Open an instance of Device Manager for the selected switch.
- Open a CLI session for the selected switch.
- Copy the display name of the selected object.
- Execute a **ping** or **traceroute** command for the device.
- Show or hide end devices.
- View attributes.
- Quiesce and disable members for PortChannels.
- Set the trunking mode for an ISL.
- Create or add to a PortChannel for selected ISLs.

The Fabric pane has its own toolbar with options for saving, printing, and changing the appearance of the map. When you right-click the map, a pop-up menu appears that provides options (duplicated on the toolbar) for changing the appearance of the map.



#### Note

You can launch web-based or non-web-based applications from the Fabric pane. To do this, you assign an IP address to the storage port or enclosure. Then right-click to bring up the pop-up menu, and select **Device Manager**.

## Saving the Map

You can save the map in the Fabric Pane as an image, or as an editable Visio diagram. You can save the map with or without labels on the links. The created Visio diagram is editable and saved in two layers:

- The default layer includes all switches and links in the fabric.
- The end devices layer includes the end devices and can be turned off to remove end devices from the Visio diagram.

To save the map as a Visio diagram, select **Files > Export > Visio** and choose **Map** or **Map with link labels**. The saved Visio diagram retains the viewing options that you selected from the Fabric pane. For example, if you collapse multiple links in the map and export the links as a Visio diagram, the Visio diagram shows those multiple links as one solid link.

The Show Tech Support option from the Tools menu also supports saving the map as a Visio diagram.

## Purging Down Elements

The Fabric pane allows you to refresh the map at any time by clicking the **Refresh Map** icon. The **Refresh Map** icon redraws the map but does not purge elements that are down. To purge down elements you can:

- Click **Server > Purge Down Elements**. This purges all down elements in the fabric.
- Right-click the **Fabric** pane and select **Purge Down Elements**.
- Right-click a down element and select **Purge**. This action purges only this element from the fabric.



#### Note

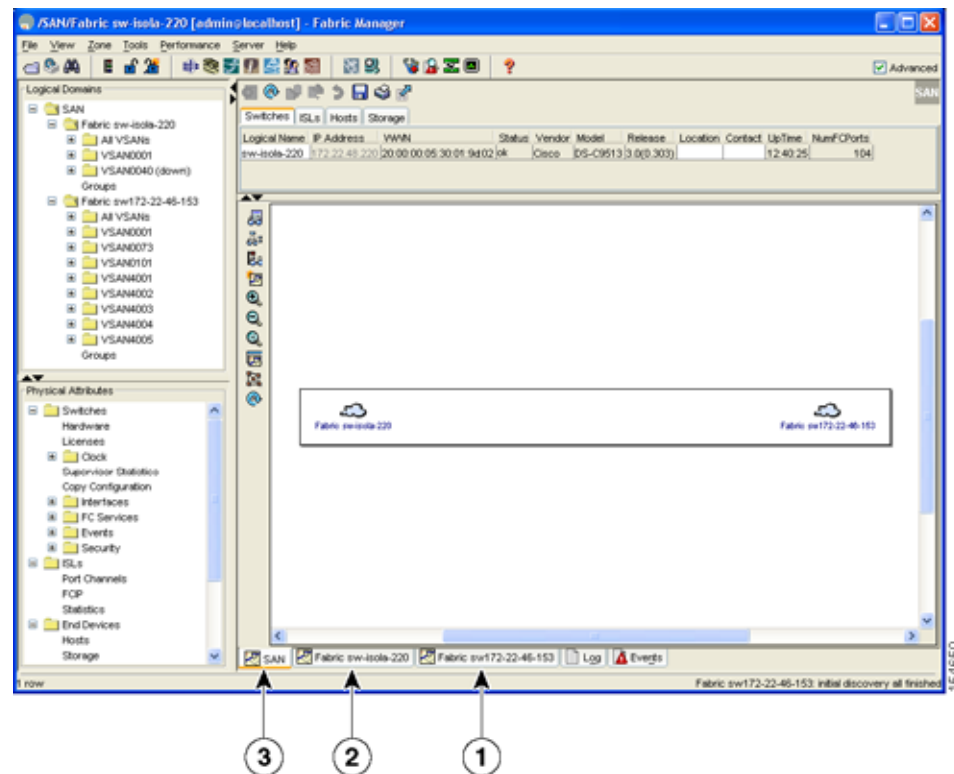
If you select an element that is not down and purge it, that element will reappear on the next fabric discovery cycle.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Multiple Fabric Display

Fabric Manager can display multiple fabrics in the same pane as shown in [Figure 5-13](#).

**Figure 5-13** Fabric Manager's Multiple Fabric Display Window



- |   |   |
|---|---|
| 1 | The Fabric view tab for fabric 172.23.46.152. When selected, the Fabric view displays fabric 172.23.46.152. |
| 2 | The Fabric view tab for fabric 172.23.46.153. When selected, the Fabric view displays fabric 172.23.46.153. |
| 3 | SAN tab (selected), showing two fabrics.  |

The information for both fabrics is displayed; you do not need to select a seed switch. To see details of a fabric, select the tab for that fabric at the bottom of the Fabric pane, or double-click the **Cloud** icon for the fabric in the SAN tab.



### Note

Enclosure names should be unique. If the same enclosure name is used for each port, Fabric Manager shows a host/target enclosure connected to both fabrics. To fix this problem, you can either disable auto-creation or create unique enclosure names.

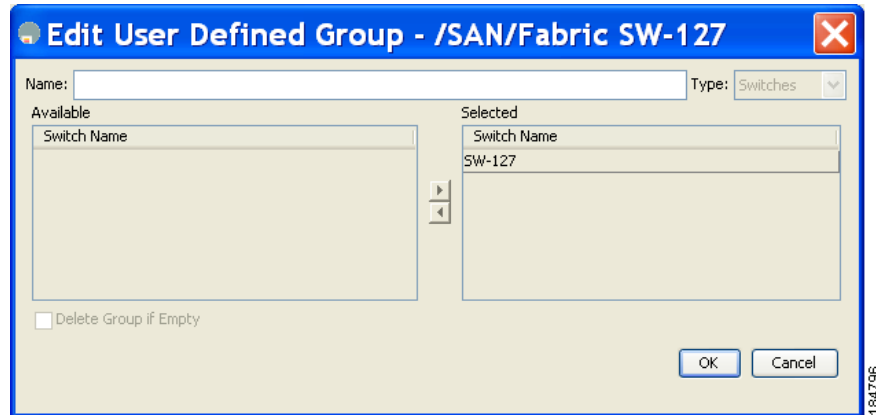
*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Filtering by Groups

You can filter the Fabric pane display by creating groups of switches or end ports. To create a group in Fabric Manager, follow these steps:

- 
- Step 1** Right-click a switch or end port in the Fabric pane map and select **Group > Create**.  
You see the Edit User Defined Group dialog box as shown in [Figure 5-14](#).

**Figure 5-14** Edit User Defined Group Dialog Box



- Step 2** Enter a group name in the Name field.
- Step 3** Use the arrows to move additional switches or end ports from the Available column to the Selected column.
- Step 4** Click **OK** to save the group.
- 

To add a switch or end port to an existing group in Fabric Manager, follow these steps:

- 
- Step 1** Right-click a switch or end device and select **Group > Add To > YourGroupName**.  
You see the Edit User Defined Group dialog box as shown in [Figure 5-14](#).
- Step 2** Use the arrows to move additional switches or end ports from the Available column to the Selected column.
- Step 3** Click **OK** to save the updated group.
- 

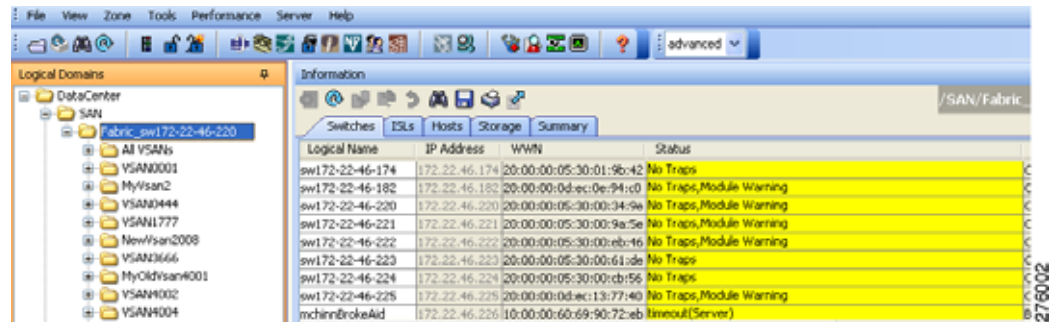
To filter the display by a group you have created, follow these steps:

- 
- Step 1** Expand the **Groups** folder in the Logical Domains pane.  
You see the list of groups that you have created as shown in [Figure 5-15](#).



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 5-15** Group Highlighted in Fabric Pane Map



**Step 2** Click the name of the group that you want to filter.

In the Fabric pane, the switches or end devices in your group are shown normally; all other switches and end devices are shown in gray.

**Step 3** Click the **Groups** folder in the Logical Domains pane to return the display to normal.



**Note** User-defined groups tables are filtered based on switches in the group except for switches where CFS-controlled features are enabled when all CFS member switches are displayed to avoid misconfigurations.

## Status Bar

The status bar at the bottom of the Fabric Manager window shows the last entry displayed by the discovery process, and the possible error message on the right side. The status bar displays a message stating that something has changed in the fabric and a new discovery is needed. The status bar shows both short-term, transient messages (such as the number of rows displayed in the table) and long-term discovery issues.

## Setting Fabric Manager Preferences

To set your preferences for the behavior of the Fabric Manager, choose **File > Preferences** from the Fabric Manager menu bar. You see the Preferences dialog box with the following tabs for setting different components of the application:

- General
- SNMP
- Map

The default General preferences for Fabric Manager are as follows:

- Show Device Name by—Displays the switches in the Fabric pane by IP address, DNS name, or logical name. The default setting for this value is Logical Name.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- **Show WorldWideName (WWN) Vendor**—Displays the world wide name vendor name in any table or listing displayed by Fabric Manager. Check the **Prepend Name** check box to display the name in front of the IP address of the switch. Check the **Replacing Vendor Bytes** check box to display the name instead of the IP address. The default is the Prepend Name option.
- **Show End Device Using**—Displays end devices in the Fabric pane using alias or pWWN alias. The default setting for this value is Alias.
- **Show Shortened iSCSI Names**—Displays the default setting for this value is OFF.
- **Show Timestamps as Date/Time**—Displays timestamps in the date/time format. If this preference is not checked, timestamps are displayed as elapsed time. The default setting is enabled (checked).
- **Telnet Path**—Displays the path for the telnet.exe file on your system. The default is telnet.exe, but you need to browse for the correct location.



**Note** If you browse for a path or enter a path and you have a space in the pathname (for example, c:\program files\telnet.exe), then the path will not work. To get the path to work, you must manually place quotes around it (for example, "c:\program files\telnet.exe").

- **Use Secure Shell instead of Telnet**—Specifies whether to use SSH or Telnet when using the CLI to communicate with the switch. If enabled, you must specify the path to your SSH application. The default setting is disabled.
- **Confirm Deletion**—Displays a confirmation pop-up window when you delete part of your configuration using Fabric Manager. The default setting is enabled (checked).
- **Export Tables with Format**—Specifies the type of file that is created when you export a table using Device Manager. The options are tab-delimited or XML. The default setting is Tab-Delimited.
- **Show CFS Warnings**—Shows warning messages if CFS is not enabled on all switches for a selected feature.

The default SNMP preferences for Fabric Manager are as follows:

- **Retry request 1 time(s) after 5 sec timeout**—You can set the retry value to 0-5, and the timeout value to 3-30.
- **Trace SNMP packets in Log**—The default setting for this value is ON.
- **Enable Audible Alert when Event Received**—The default setting for this value is OFF.

The default Map preferences for Fabric Manager are as follows:

- **Display Unselected VSAN Members**—Displays the unselected VSAN members in the Fabric pane. The default setting for this value is ON.
- **Display End Devices**—Displays the fabric's end devices in the Fabric pane. The default setting for this value is ON.
- **Display End Device Labels**—Displays the fabric's end device labels in the Fabric pane. The default setting for this value is OFF.
- **Expand Loops**—Displays the loops in the fabric as individual connections in the Fabric pane. The default setting for this value is OFF.
- **Expand Multiple Links**—Displays multiple links in the Fabric pane as separate lines instead of one thick line. The default setting for this value is OFF.
- **Open New Device Manager Each Time**—Opens a new instance of Device Manager each time that you invoke it from a switch in your fabric. The default value is OFF, which means that only one instance of Device Manager is open at a time.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- **Select Switch or Link from Table**—Allows you to select a switch or link in the Fabric pane by clicking the switch or link in a table in the Information pane. The default setting for this value is disabled (unchecked), which means clicking a switch or link in the table does not change the switch or link selection in the Fabric pane.
- **Layout New Devices Automatically**—Automatically places new devices in the Fabric pane in an optimal configuration. The default setting for this value is OFF. In this mode, when you add a new device, you must manually reposition it if the initial position does not suit your needs.
- **Use Quick Layout when Switch has 30 or more End Devices**—Displays the default setting for this value (30). You can enter any number in this field. Enter **0** to disable Quick Layout.
- **Override Preferences for Non-default Layout**—Displays the default setting for this value (ON).
- **Automatically Save Layout**—If this option is enabled, any changes in the layout are automatically saved. The default setting for this value is ON.
- **Detach Overview Window**—Allows you to easily center the Fabric pane on the area of the fabric that you want to see. (This feature is useful for large fabrics that cannot be displayed entirely within the Fabric pane.) Bring up the overview window by clicking the **Show/Hide Overview Window** button. It overlays the fabric window and remains there until you click the **Show/Hide Overview Window** button again. If you enable this preference, you can detach the overview window and move it to one side while you access the Fabric pane. The default setting for this value is disabled (unchecked).

## Network Fabric Discovery

Cisco Fabric Manager collects information about the fabric topology through SNMP queries to the switches that are connected to Fabric Manager. The switch replies after having discovered all devices connected to the fabric by using the information from its FSPF technology database and the Name Server database and collected using the Fabric Configuration Server's request/response mechanisms that are defined by the FC-GS-3/4 standard. When you start Fabric Manager, you enter the IP address (or host name) of a seed switch for discovery.

After you start Fabric Manager and the discovery completes, Fabric Manager presents you with a view of your network fabric, including all discovered switches, hosts, and storage devices.

## Network LAN Discovery

Starting from NX-OS Release 4.2(0), you can discover Nexus and Catalyst Ethernet switches using Cisco Discovery Protocol (CDP). DataCenter 3(DC3) switches are displayed under Datacenter and LAN nodes. Fabric Manager displays basic information about DC3 switches and its ISLs.

## Viewing Ethernet Switches

To view information about Ethernet switches, follow these steps:

---

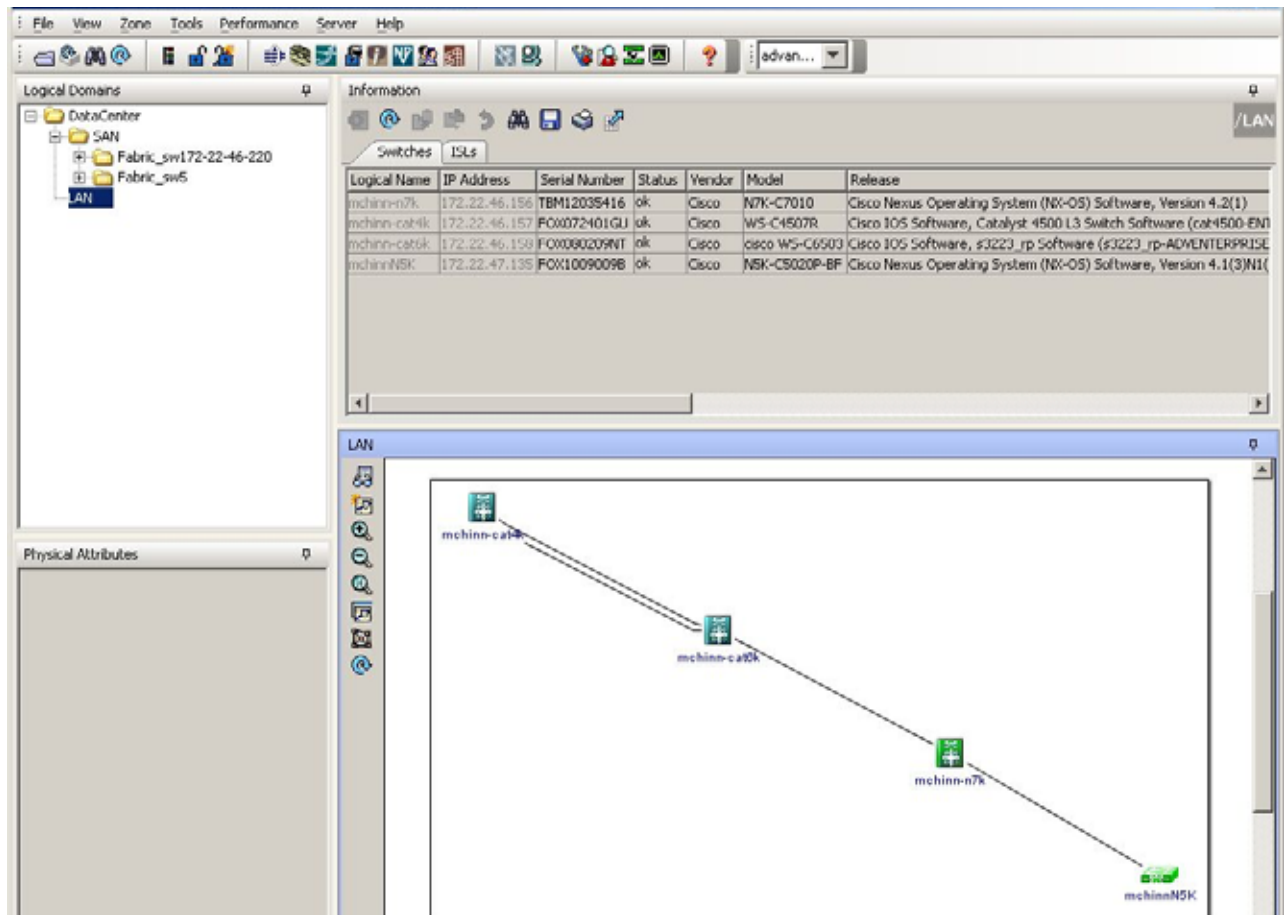
**Step 1** Click the **LAN** node under **Datacenter** node.


**Step 2** Click **Switches** tab in the Information pane.

You can see the switch information as shown in [Figure 5-16](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

Figure 5-16 Ethernet Switch Information



 **Note** Datacenter is the parent node of SAN and LAN nodes. The SAN node remains in the tree as the parent for all the fabrics.

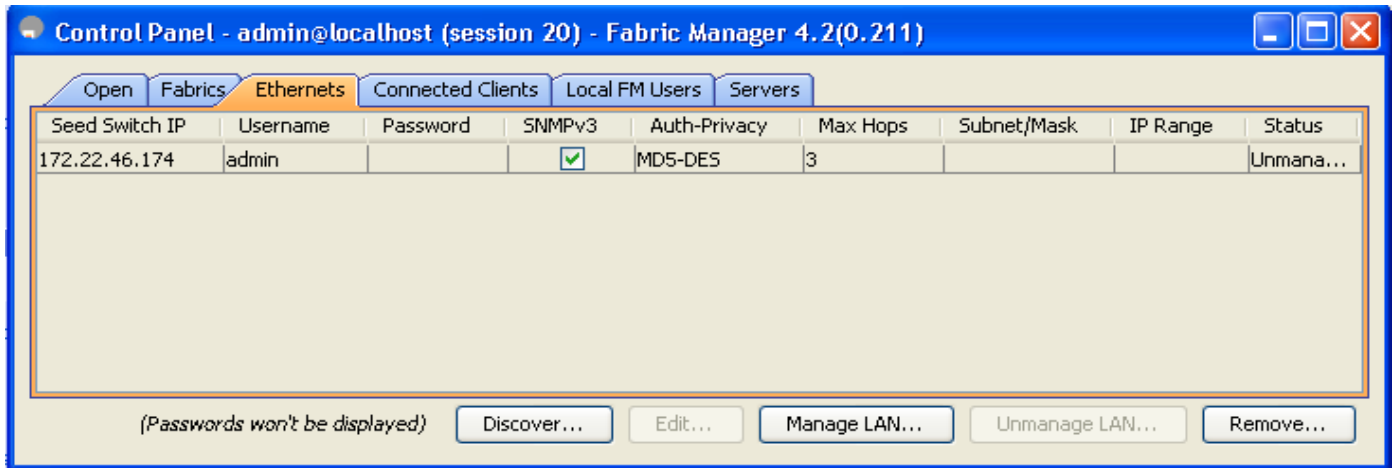
## Removing a LAN

To remove a discovered LAN from the server, follow these steps:

- Step 1** Choose **Server > Admin**.  
You can see the switch information as shown in [Figure 5-17](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

Figure 5-17 Control Panel



- Step 2** Click to select the switch IP of the LAN you want to remove.
- Step 3** Click **Remove**.

## Modifying the Device Grouping

Because not all devices are capable of responding to FC-GS-3 requests, different ports of a single server or storage subsystem may be displayed as individual end devices on the Fabric Manager map.

To group end devices in a single enclosure to have them represented by a single icon on the map, Fabric Manager, follow these steps:

- Step 1** Expand **End Devices** and then select **Storage** or **Hosts** in the Physical Attributes pane. You see the end devices displayed in the Information pane.
- Step 2** Click one of the devices in the Fabric pane, or click the **Enclosures** tab of the Information pane, and then click the device name (in the Name field) that you want to include in the enclosure.
- Step 3** Enter a name to identify the new enclosure in the Fabric pane map.
- Step 4** Click once on the device name in the Name field. To select more than one name, press the **Shift** key and click each of the other names.
- Step 5** Press **Ctrl-C** to copy the selected name(s).
- Step 6** Press **Ctrl-V** to paste the device name into the Name field.



**Note** To remove devices from an enclosure, triple click the device name and press **Delete**. To remove an enclosure, repeat this step for each device in the enclosure.

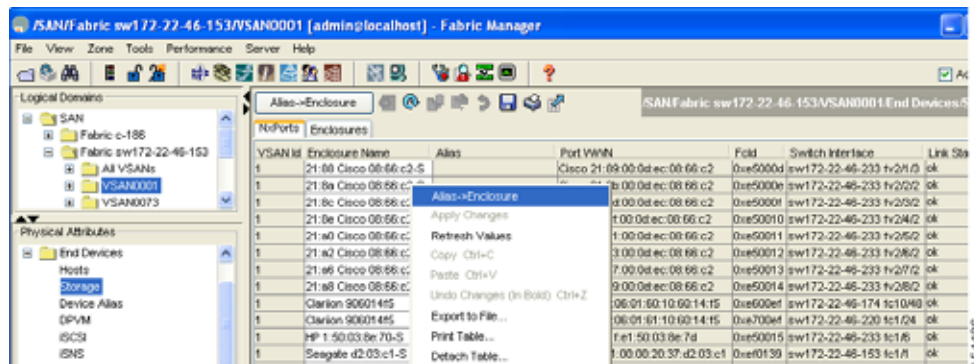
*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Using Alias Names as Enclosures

To create an enclosure that uses the alias name as the name of the enclosure using Fabric Manager, follow these steps:

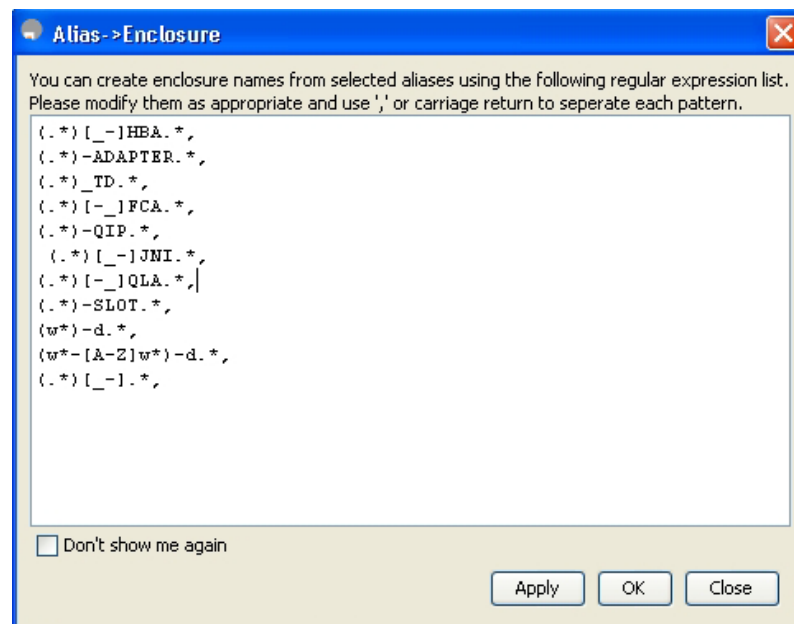
- Step 1 Expand End Devices and select **Hosts** or **Storage** from the Physical Attributes pane. You see the list of devices in the Information pane. The NxPorts tab is the default.
- Step 2 Right-click the enclosure names that you want to convert to alias names and select **Alias > Enclosure** as shown in [Figure 5-18](#).

**Figure 5-18** Alias Enclosure



The Alias > Enclosures window appears as shown in [Figure 5-19](#). It contains a list of expressions. You can also add expressions to the list and modify expressions in the current list.

**Figure 5-19** List of Expressions



- Step 3 Click the **Apply Changes** icon to save the changes and then click **Close**.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Note**

Fabric Manager uses the regular expressions to convert multiple alias names into one enclosure. The alias names should be in the same expression pattern rule. You can create enclosure names from selected aliases using the regular expressions list.

## Using Alias Names as Descriptions

To create descriptions that uses alias names as the name of the description using Fabric Manager, follow these steps:

- Step 1** Select **End Devices** and from the Physical Attributes pane.
- Step 2** Click the **General** tab.  
You see the list of devices in the Information pane.
- Step 3** Select the device names that you want to populate the description with alias names and then click **Alias > Enclosure** button as shown in Figure 5-20.  
You see the alias names are copied to corresponding rows in the description column.

**Figure 5-20 Data Population: Alias to Description**

The screenshot shows the Fabric Manager client interface. At the top, there's a menu bar with 'Server' and 'Help'. Below it is a toolbar with various icons and a dropdown menu set to 'advanced'. The main window is titled 'Information' and contains a tabbed interface. The 'Alias->Description' button is highlighted. The table below shows the data for the selected devices.

Switch	Interface	Mode Admin	Mode Oper	Port VSAN	Dynamic VSAN	Description	Alias	Speed Admin
sw172-22-46-...	fc1/2	TL	TL	2	n/a	Symbios 20:02:00:a0:b8:0c:0a:e3	SymBios 20:02:00:a0:b8:0c:0a:e3	auto
sw172-22-46-...	fc1/10	FX	F	1	n/a	Emulex 10:00:00:00:c9:73:2a:f2	Emulex 10:00:00:00:c9:73:2a:f2	auto
sw172-22-46-...	fc10/20	FX	F	2	n/a	10:00:00:00:00:01:00:00	10:00:00:00:00:01:00:00	auto
sw172-22-46-...	fc10/46	FX	F	2	n/a	LSI 2f:ff:00:06:2b:10:c1:53	LSI 2f:ff:00:06:2b:10:c1:53	auto
sw172-22-46-...	fc10/48	FX	F	2	n/a	myCLRDA	Clariion 906014f5-SPA0	auto
sw172-22-46-...	fc1/3	F	F	1	n/a	Emulex 10:00:00:00:c9:2e:31:37	Emulex 10:00:00:00:c9:2e:31:37	auto

Below the table, the selected device 'Fabric\_sw172-22-46-220' is listed.

**Note**

Fabric Manager does not parse or format the alias name while copying.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Controlling Administrator Access with Users and Roles

Cisco MDS 9000 Family switches support role-based management access whether using the CLI or Cisco Fabric Manager. This lets you assign specific management privileges to particular roles and then assign one or more users to each role.

The default-role contains the access permissions needed by a user to access the GUI (Fabric Manager and Device Manager). These access permissions are automatically granted to all users in order for them to use the GUI.

Cisco Fabric Manager uses SNMPv3 to establish role-based management access. After completing the setup routine, a single role, user name, and password are established. The role assigned to this user allows the highest level of privileges, which includes creating users and roles. Use the Cisco Fabric Manager to create roles and users and to assign passwords as required for secure management access in your network.

## Using Fabric Manager Wizards

Fabric Manager Client provides the following wizards to facilitate common configuration tasks:

- VSAN—Creates VSANs on multiple switches in the fabric and sets VSAN attributes including interop mode, load balancing, and FICON.
- Zone Edit Tool—Creates zone sets, zones, and aliases. Adds members to zones and edits the zone database.
- IVR Zone—Creates IVR zone sets, zones, and aliases. Enables IVR NAT and auto-topology. Adds members to IVR zones, and edits the IVR zone database.
- FCoE—Creates virtual Fibre Channel (FC) interfaces and VLAN to VSAN mappings, and binds virtual FC interfaces to Ethernet interfaces or PortChannels.
- PortChannel—Creates PortChannels from selected ISLs either manually or automatically. Sets PortChannel attributes such as channel ID and trunking mode.
- FCIP—Creates FCIP links between Gigabit Ethernet ports. Enables Fibre Channel write acceleration and IP compression.
- DPVM—Establishes dynamic port VSAN membership, enables autolearning, and activates the DPVM database.
- Port Security—Prevents unauthorized access to Cisco MDS switches and reports these intrusions to the administrator.
- iSCSI—Creates zones for iSCSI initiators and adds a VSAN to a target-allowed VSAN list.
- NPV—Reduces the number of Fibre Channel domain IDs in SANs.
- QoS—Sets QoS attributes for zones in the selected VSAN.
- IP ACL—Creates ordered IP access control lists and distributes to selected switches in the fabric.
- License Install—Facilitates download and installation of licenses in selected switches in the fabric.
- Software Install—Verifies image compatibility and installs software images on selected switches in the fabric.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Fabric Manager Troubleshooting Tools

Fabric Manager has several troubleshooting tools available from the toolbar or Tools menu

- **Zone Merge Analysis**—The zone merge analysis tool (available from the Zone menu) enables you to determine if zones will merge successfully when two Cisco MDS switches are interconnected. If the interconnected switch ports allow VSANs with identical names or contain zones with identical names, then Fabric Manager verifies that the zones contain identical members. The merge analysis tool can be run before attempting a merge or after fabrics are interconnected to determine zone merge failure causes.
- **End-to-End Connectivity**—Fabric Manager's end-to-end connectivity analysis tool uses FC Ping to verify interconnections between Cisco MDS switches and end-device (HBAs and storage devices) in a particular VSAN. In addition to basic connectivity, Fabric Manager can optionally verify the following:
  - Paths are redundant.
  - Zones contain at least two members.

End devices are connected to a manageable switch (have a currently active in-band or out-of-band management path.)

- **Switch Health Analysis**—You can run an in-depth switch health analysis with Fabric Manager. It verifies the status of all critical Cisco MDS switches, modules, ports, and Fibre Channel services. Over 40 conditions are checked. This tool provides a very fast, simple, and thorough way to assess Cisco MDS switch health.
- **Fabric Configuration Analysis**—Fabric Manager includes a fabric configuration analysis tool. It compares the configurations of all Cisco MDS switches in a fabric to a reference switch or a policy file. You can define what functions to check and what type of checks to perform. The analysis can look for mismatched values, and missing or extra values. If all configuration checking is performed for all functions, over 200 checks are performed for each Cisco MDS switch.

After the analysis is run, the results are displayed with details about the issues that were discovered. You can automatically resolve configuration differences by selecting them and clicking the **Resolve** button. Fabric Manager automatically changes the configuration to match the reference switch or policy file.

## Integrating Fabric Manager and Data Center Network Management Software

Fabric Manager and Data Center Network Management (DCNM) software are the two major components in the Cisco next-generation data center environment. Fabric Manager configures Cisco Nexus 5000 Series switches and Cisco MDS 9000 Series switches. DCNM software configures Cisco Nexus 5000 and Cisco Nexus 7000 Series switches. The Scope of the Fabric Manager software is confined to SAN while the scope of the DCNM software is limited to the LAN network.

In a typical data center environment, the mixture of SAN and LAN topology are becoming increasingly common. Since the two management software are not designed to work across their topology limits, users are not able to navigate to Fabric Manager from DCNM software and vice versa.

Integrating Fabric Manager and DCNM provides a single platform to manage the networks in data center 3.0 and it provides seamless user experience under specific configuration. Starting from Cisco MDS NX-OS Release 4.2, the directory structure has changed to accommodate the integration of Fabric Manager with Cisco Nexus 5000 Series products.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

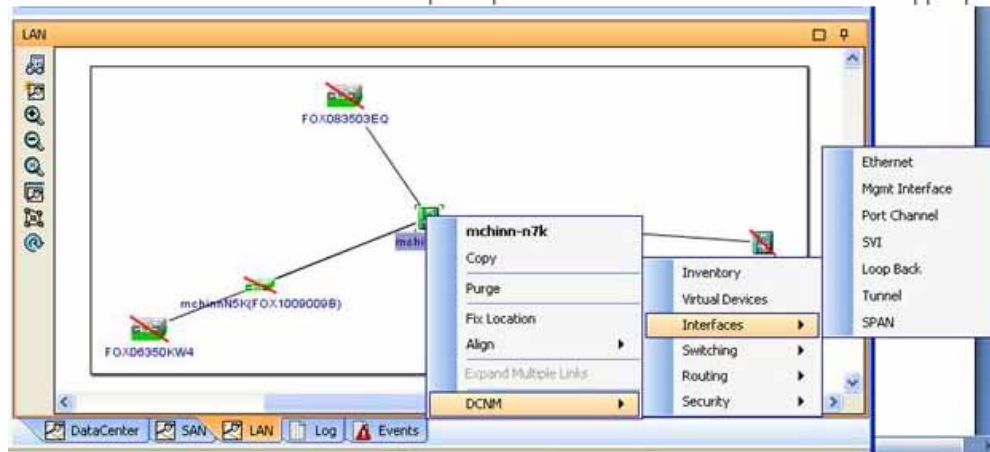
## Launching a Switch from the Topology Map

To launch a switch in DCNM from Fabric Manager, follow these steps:

- Step 1** In the Fabric Manager fabric pane, right-click the Nexus switch in the LAN map that you want to open with DCNM.

You see the pop-up menu as shown in [Figure 5-21](#).

**Figure 5-21** Open with DCNM



- Step 2** In the pop up menu, click **DCNM** and select appropriate context.



## CHAPTER 6

# Device Manager

---

This chapter describes how to use the Cisco MDS 9000 Device Manager. This chapter contains the following sections:

- [About Device Manager, page 6-1](#)
- [Launching Device Manager, page 6-3](#)
- [Using Device Manager, page 6-4](#)
- [Setting Device Manager Preferences, page 6-10](#)

## About Device Manager

Device Manager provides a graphic representation of a Cisco MDS 9000 Family switch chassis or Cisco Nexus 5000 Series switch chassis, including the installed switching modules, the supervisor modules, the status of each port within each module, the power supplies, and the fan assemblies.

Device Manager provides a graphical representation of a Cisco MDS 9000 Family switch chassis or Cisco Nexus 5000 Series switch chassis, including the installed switching modules, the supervisor modules, the status of each port within each module, the power supplies, and the fan assemblies.

The tables in the Fabric Manager Information pane basically correspond to the dialog boxes that appear in Device Manager. However, while Fabric Manager tables show values for one or more switches, a Device Manager dialog box shows values for a single switch. Also, Device Manager provides more detailed information for verifying or troubleshooting device-specific configuration than Fabric Manager.

Device Manager Release 4.2 and later provides enhanced security using multiple perspectives (simple and advanced) allowing role based-access to its features. The Device Manager perspective filters out menu items that are not relevant to the user. Users with server admin role, can only access a subset of the fabric related features. The server admin role will not be able to manage Device Manager users or connected clients.

Device Manager Release 5.0 and later supports all the software features that are offered by Cisco NX-OS for managing Cisco MDS 9148 and 9124 Multilayer Fabric switches. Cisco MDS 9148 Multilayer Fabric Switch is a 48-port (1/2/4/8G) FC 1RU switch based on the Sabre ASIC and Cisco MDS 9124 Multilayer Fabric switch is a 1/2/4/8G switch module for HP BladeServer based on the Sabre ASIC. Device Manager and Fabric Manager allow you to discover, display, configure, monitor, and service both these new switches.

### Support for Cisco Nexus 5000 Series Switches

Device Manager allows you to discover, display, configure, monitor, and service the following Cisco Nexus 5000 Series switches:

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Cisco NX-OS Release 4.2(1)N2(1) supports the 2 RU (rack unit) Cisco Nexus 5020 switch. It has 40 10-Gigabit Ethernet host interfaces for its downlink connection to servers or hosts and supports two optional expansion modules (GEMs). It does not support Fibre Channel over Ethernet (FCoE).
- Cisco NX-OS Release 5.0(2)N1(1) supports the 1 RU (rack unit) Cisco Nexus 5548 switch. It has 32 10-Gigabit Ethernet and FCoE ports with small form-factor pluggable (SFP+) interface adapters for its downlink connection to servers or hosts. You can put the optional following expansion modules into the Cisco Nexus 5548 switch:
  - N55-M16P module—It has 16 10-Gigabit Ethernet and FCoE ports with SFP+ interface adapters for its uplink connections.
  - N55-M8P8FP module—It has eight 8-Gbps Fibre Channel interfaces and eight 10-Gigabit Ethernet and FCoE ports with SFP+ interface adapters for its uplink connections.

**Note**

You can configure Fibre Channel or FCoE on the switch by enabling the HTTP server application. Use the **feature http-server** command to enable the HTTP server on the switch.

### Support for Cisco Nexus 2000 Series Fabric Extenders

Device Manager supports the following Cisco Nexus 2000 Series Fabric Extenders on a Cisco Nexus 5000 Series switch that runs Cisco NX-OS Release 4.2(1)N2(1) or later releases:

- Cisco Nexus 2148T Fabric Extender—It has four 10-Gigabit Ethernet fabric interfaces for its uplink connection to the parent Cisco Nexus 5000 Series switch and 48 1000BASE-T (1-Gigabit) Ethernet host interfaces for its downlink connection to servers or hosts.
- Cisco Nexus 2232PP Fabric Extender—It has eight 10-Gigabit Ethernet fabric interfaces with small form-factor pluggable (SFP+) interface adapters for its uplink connection to the parent Cisco Nexus 5000 Series switch and 32 10-Gigabit Ethernet fabric interfaces with SFP+ interface adapters for its downlink connection to servers or hosts.
- Cisco Nexus 2248TP Fabric Extender—It has four 10-Gigabit Ethernet fabric interfaces with small form-factor pluggable (SFP+) interface adapters for its uplink connection to the parent Cisco Nexus 5000 Series switch and 48 1000BASE-T (1-Gigabit) Ethernet host interfaces for its downlink connection to servers or hosts.
- Cisco Nexus N2224TP Fabric Extender—It has two 10-Gigabit Ethernet fabric interfaces with small form-factor pluggable (SFP+) interface adapters for its uplink connection to the parent Cisco Nexus 5000 Series switch, and 24 1000BASE-T (1-Gigabit) Ethernet host interfaces for its downlink connection to servers or hosts. It does not support Fibre Channel over Ethernet (FCoE).

Device Manager allows you to discover, display, configure, monitor, and view these Fabric Extenders.

## Device Manager Features

Device Manager provides two views: Device View and Summary View. Use Summary View to monitor interfaces on the switch. Use Device View to perform switch-level configurations including the following:

- Configure virtual Fibre Channel interfaces.
- Configure Fibre Channel over Ethernet (FCoE).
- Configure zones for multiple VSANs.
- Manage ports, PortChannels, and trunking.
- Manage SNMPv3 security access to switches.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Manage CLI security access to the switch.
- Manage alarms, events, and notifications.
- Save and copy configuration files and software image.
- View hardware configuration.
- View chassis, module, port status, and statistics.

## Launching Device Manager

To launch Device Manager from your desktop, double-click the **Device Manager** icon and follow the instructions described in the “[Integrating Cisco Fabric Manager with Other Management Tools](#)” section on page 2-41.

To launch Device Manager, follow these steps:

- Step 1** You can choose one of the following:
- a. Right-click the switch you want to manage on the Fabric pane map and choose **Device Manager** from the menu that appears.
  - b. Double-click a switch in the Fabric pane map.
  - c. Select a switch in the Fabric pane map and choose **Tools > Device Manager**.

You see the Device Manager open dialog box as shown in [Figure 6-1](#)

**Figure 6-1** Device Manager: Open Dialog Box



- Step 2** Enter the IP address of the device.
- Step 3** Enter the user name and password.
- Step 4** Check the Proxy SNMP through FMS check box if you want Device Manager Client to use a TCP-based proxy server.

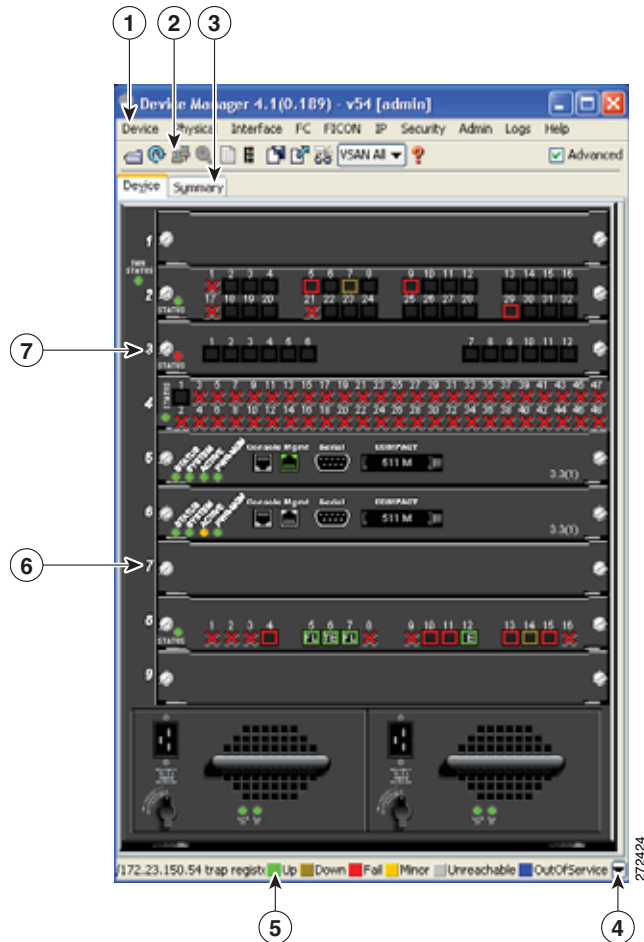
*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 5** Choose the Auth-Privacy option according to the privacy protocol you have configured on your switch:
- If you have not configured the switch with a privacy protocol, then choose Auth-Privacy option MD5 (no privacy).
  - If you have configured the switch with your privacy protocol, choose your Auth-Privacy choice.
- Step 6** Click **Open** to open the Device Manager.

## Using Device Manager

This section describes the Device Manager interface as shown in [Figure 6-2](#).

**Figure 6-2** Device Manager, Device Tab



1 Menu bar

5 Status

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

2	Toolbar	6	Supervisor modules
3	Tabs	7	Switching or services modules
4	Legend		

## Menu Bar

The menu bar at the top of the Device Manager main window provides options for managing and troubleshooting a single switch. The menu bar provides the following options:

- **Device**—Opens an instance of Device Manager, sets management preferences, sets the page layout, opens a Telnet/SSH session with the current switch, exports a device image, and closes the Device Manager application.
- **Physical**—Allows you to view and manage inventory, modules, temperature sensors, power supplies, fans, and the entire system.
- **Interface**—Allows you to configure and manage PortChannels, as well as Fibre Channel, Ethernet, iSCSI, and FICON ports. Also provides diagnostic, management and monitoring capabilities, as well as SPAN and port tracking.



**Note** The Interface > Port Channels menu option does not appear if the Cisco Nexus 5000 Series switch is in NPV mode and runs a Cisco NX-OS release prior to 4.2(1).

- **FC**—Allows you to configure and manage VSAN, domain, and name server characteristics. Also provides advanced configuration capabilities.
- **FCoE**—Allows you to configure the FCoE parameters and map VSANs to VLANs on a Cisco Nexus 5000 Series switch.



**Note** The FCoE menu option appears only if the Cisco Nexus 5000 Series switch runs Cisco NX-OS Release 4.0(1a) or later releases.












- **FICON**—Allows you to configure and manage FICON VSANs, configure RLIR ERL information, swap selected FICON ports, and view FICON port numbers.
- **IP**—Allows you to configure and manage the following types of information: FCIP, iSCSI, iSNS, routes, VRRP, and CDP.
- **Security**—Allows you to configure and manage FCSP, port security, iSCSI security, SNMP security, common roles, SSH, AAA, and IP ACLs.
- **Admin**—Allows you to save, copy, edit, and erase the switch configuration, monitor events, manipulate Flash files, manage licenses, configure NTP, use CFS, and reset the switch. Also enables you to use the **show tech support**, **show cores**, and **show image** commands.
- **Logs**—Shows the various logs: message, hardware, events, and accounting. Also displays FICON link incidents, and allows you to configure the syslog setup.
- **Help**—Displays online help topics for specific dialog boxes in the Information pane.

[Send documentation comments to fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)

## Toolbar Icons

The Device Manager toolbar provides quick access to many Device Manager features. Once the icon is selected, a dialog box may open that allows configuration of the feature. The toolbar provides the main Device and Summary View icons as shown in [Table 6-1](#).

**Table 6-1**      *Device Manager Main Toolbar*

Icon	Description
 Open Device	Opens the Device Manager view for another switch, with the option to open this view in a separate window.
 Refresh Display	Communicates with the switch and displays the information in the Device Manager view.
 Command-Line Interface	Opens a separate CLI command window to the switch.
 Configure Selected	Opens a configuration dialog box for the selected component (line card or port).
 SysLog	Opens a window that lists the latest system messages that occurred on the switch.
 VSANs	Opens the VSAN dialog box that provides VSAN configuration for the switch.
 Save Configuration	Saves the current running configuration to the startup configuration.
 Copy	Copies configuration file between server and switch.
 Toggle FICON/Interface Port Labels	Toggles the FICON and interface port labels.
 Select VSAN	Filters the port display to show only those ports belonging to the selected VSAN.
 Help	Accesses online help for Device Manager.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Dialog Boxes

If a toolbar icon is selected, a dialog box may open that allows configuration of the selected feature. The dialog box may include table manipulation icons. See the “[Information Pane](#)” section on page 5-13 for descriptions of these icons.

## Tabs

Click the **Device** tab on the Device Manager main window to see a graphical representation of the switch chassis and components.



**Note**

The Device view also shows the switch chassis information of the Cisco Nexus 2000 Series Fabric Extenders (FEXs) that are connected to a Cisco Nexus 5000 Series switch that runs Cisco NX-OS Release 4.2(1)N2(1) or later releases.

Click the **Summary** tab on the Device Manager main window to see a summary of active interfaces on a single switch, as well as Fibre Channel and IP neighbor devices. The Summary View also displays port speed, link utilization, and other traffic statistics. There are two buttons in the upper left corner of the Summary View tab used to monitor traffic. To monitor traffic for selected objects, click the **Monitor Selected Interface Traffic Util%** button. To display detailed statistics for selected objects, click the **Monitor Selected Interface Traffic Details** button. You can set the poll interval, the type or Rx/Tx display, and the thresholds.



**Note**

The Summary tab does not display the utilization statistics (Util%) of virtual Fibre Channel interfaces for Cisco Nexus 5000 Series switches that run Cisco NX-OS Release 4.2 or later releases.

## Legend

The legend at the bottom right of the Device Manager indicates port status, as follows:

### Colors

- Green—The port is up.
- Brown—The port is administratively down.
- Red—The port is down or has failed.
- Amber—The port has a minor fault condition.
- Gray—The port is unreachable.
- Blue—The port is out of service.

### Labels

- X—Link failure
- E—ISL
- TE—Multi-VSAN ISL
- F—Host/storage
- FL—F loop

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- I—iSCSI
- SD—SPAN destination
- CH—Channel
- CU—Control Unit
- NP—Proxy N-Port (NPV Mode)
- TNP—Trunking NP\_Port (NPV Mode)
- TF—Trunking F\_Port
- f—vFC Present (Cisco Nexus 5000 Series switches only)

## Supervisor and Switching Modules

In the Device View, you can right-click an object and get information on it, or configure it. If you right-click a module, the menu shows the module number and gives you the option to configure or reset the module. If you right-click a port, the menu shows the port number and gives you the option to configure, monitor, enable/disable, set beacon mode, or perform diagnostics on the port.



### Tip

You can select multiple ports in Device Manager and apply options to all the selected ports at one time. Either select the ports by clicking the mouse and dragging it around them, or hold down the **Control** key and click each port.

To enable or disable a port, right-click the port and click **Enable** or **Disable** from the pop-up menu. To enable or disable multiple ports, drag the mouse to select the ports and then right-click the selected ports. Then click **Enable** or **Disable** from the pop-up menu.

To manage trunking on one or more ports, right-click the ports and click **Configure**. In the dialog box that appears, right-click the current value in the Trunk column and click **nonTrunk**, **trunk**, or **auto** from the pull-down list.

To create PortChannels using Device Manager, click **PortChannels** from the Interface menu.



### Note

To create a PortChannel, all the ports on both ends of the link must have the same port speed, trunking type, and administrative state.

## Context Menus

Context menus are available in both Device Manager views by right-clicking a device or table.

From Device View:

- Device—Right-click a system, module, or power supply to bring up a menu that gives you the option to configure or reset the device.
- Port—Right-click a port to bring up a menu that shows you the number of the port you have clicked, and to give you the option to configure, monitor, enable, disable, set beacon mode, or perform diagnostics on the port.

From Summary View:

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- **Table**— Right-click the table header to show a list of which columns to display in that table: Interface, Description, VSANs, Mode, Connected To, Speed (Gb), Rx, Tx, Errors, Discards, and Log. Click the Description field to bring up the appropriate configuration dialog box for the port type.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Setting Device Manager Preferences

To set your preferences for the behavior of the Device Manager application, choose **Device > Preferences** from the Device menu. You can set the following preferences:

- **Retry Requests x Time(s) After x sec Timeout**—Allows you to set the retry request values. The default settings are 1 time after a 5-second timeout.
- **Enable Status Polling Every x secs**—Allows you to set the status polling value. The default setting is enabled (checked) with a time of 40 seconds.
- **Trace SNMP Packets in Message Log**—Allows you to set whether Device Manager traces SNMP packets and logs the trace. The default setting is disabled (unchecked).
- **Register for Events After Open, Listen on Port 1163**—Allows you to register this switch so that events are logged once you open Device Manager. The default setting is enabled (checked).
- **Show WorldWideName (WWN) Vendor**—Displays the world wide name vendor name in any table or listing displayed by Device Manager. If **Prepend** is checked, the name is displayed in front of the IP address of the switch. If **Replace** is checked, the name is displayed instead of the IP address. The default setting is enabled (checked) with the **Prepend** option.
- **Show Timestamps as Date/Time**—Displays timestamps in the date/time format. If this preference is not checked, timestamps are displayed as elapsed time. The default setting is enabled (checked).
- **Telnet Path**—Sets the path for the telnet.exe file on your system. The default is **telnet.exe**, but you need to browse for the correct location.



### Note

If you browse for a path or enter a path and you have a space in the pathname (for example, **c:\program files\telnet.exe**, then the path will not work. To get the path to work, manually place quotes around it (for example, **"c:\program files\telnet.exe"**).

- **CLI Session Timeout x secs (0= disable)**—Specifies the timeout interval for a CLI session. Enter 0 to disable (no timeout value). The default setting is 30 seconds.
- **Show Tooltips in Physical View**—Determines whether tooltips are displayed in Physical (Device) View. The default setting is enabled (checked).
- **Label Physical View Ports With:**—Specifies the type of label to assign to the ports when you are in Physical (Device) View. The options are FICON and Interface. The default setting is Interface.
- **Export Table**—Specifies the type of file that is created when you export a table using Device Manager. The options are Tab-Delimited or XML. The default setting is Tab-Delimited.



## CHAPTER 7

# Fabric Manager Web Client

---

## Fabric Manager Web Client

With Fabric Manager Web Client, you can monitor Cisco MDS switch events, performance, and inventory from a remote location using a web browser. You can also monitor the events, performance, and inventory information of Cisco Nexus 5000 Series switches.

This chapter contains the following sections:

- [About Fabric Manager Web Client, page 7-1](#)
- [Navigating Fabric Manager Web Client, page 7-2](#)
- [Installing Fabric Manager Web Client, page 7-3](#)
- [Launching Fabric Manager Web Client, page 7-7](#)
- [Health, page 7-9](#)
- [Performance, page 7-13](#)
- [Inventory, page 7-29](#)
- [Reports, page 7-39](#)
- [Admin, page 7-50](#)
- [Fabric Manager Web Search Engine, page 7-67](#)
- [Configuring Backups Using Fabric Manager WebClient, page 7-72](#)

## About Fabric Manager Web Client

Using Fabric Manager Web Client, you can monitor Cisco MDS 9000 Series or Cisco Nexus 5000 Series switch events, performance, and inventory, and perform minor administrative tasks.

Fabric Manager Web Client provides the following features:

- **Summary and drill down reports**—The Performance Manager summary report provides a high-level view of your network performance. These reports list the average and peak throughput and provides hot-links to additional performance graphs and tables with additional statistics. Both tabular and graphical reports are available for all interconnections monitored by Performance Manager. Performance Manager also analyzes daily, weekly, monthly and yearly trends. You can also view the results for specific time intervals using the interactive zooming functionality. These reports are only available if you create a collection using Performance Manager and start the collector. To view historical performance reports, you need to install Adobe Flash Player 10 or later.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

See the “[Historical Performance Monitoring](#)” section on page 11-4.

- **Zero maintenance database for statistics storage**—No maintenance is required to maintain Performance Manager’s round-robin database, because its size does not grow over time. At prescribed intervals the oldest samples are averaged (rolled-up) and saved. A full two days of raw samples are saved for maximum resolution. Gradually the resolution is reduced as groups of the oldest samples are rolled up together.

You see Fabric Manager Web Client window as shown in [Figure 7-1](#).

**Figure 7-1**      *Fabric Manager Web Client*



## Navigating Fabric Manager Web Client

With most screens, Fabric Manager Web Client has standardized certain navigation conventions.

### Navigation Tree

You can use the filter navigation tree in the left pane to access the areas you want as follows:

- Select **SAN** to view information for all fabrics and VSANs in the SAN. When you do this, a Fabric column is added as the first column of the tables.
- Click a fabric folder to view information for that specific fabric.
- Some screens have expandable fabric folders. You can expand the fabric folders (by clicking the + or - icons in front of the folders) to see a list of VSANs in that fabric. Select a VSAN to view information for that VSAN.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

The features accessible from the tabs are limited to the areas you select in the filter tree.

## Table Filtering and Navigation

You can filter the display of some tables to view subsets of the information. At the top right of these tables are one or more drop-down lists. Select an item from these lists, and then click **Filter** to filter the table information on that item.

You can change the number of rows displayed per page by selecting a number from the **Rows per page** drop-down list at the lower left corner of the table. Once you select a number, the table is updated with the new number of rows; you do not have to click a button.

For tables with multiple pages of information, you can:

- Jump to the first or last page of the table by clicking the first page or last page icons (arrows with a bar in front of it)
- Jump to the next page or previous page by clicking the next page or previous page icons (arrows)
- Jump to a specific page by entering the page number in the **Go to page** field and clicking the **Go** button.

You can search certain columns in the tables for information if a table column has a black icon next to the column head. Click the icon to display a Search dialog box.

## Printing

There is a **Print** icon in the lower right corner of some tables. Click this icon to view the table in a printer-friendly format. You can then print the page from the browser.

## Exporting to a File

There is an **Export** icon in the lower right corner of some tables. Click this icon to export the data to a .CSV file that can be read by programs such as Microsoft Excel.

## Sorting Columns

On some screens, you can click a column head to sort the information for that column.

# Installing Fabric Manager Web Client

If you are installing the Fabric Manager Web Client software for the first time, or if you want to update or reinstall the software, you access the supervisor module of the switch using a web browser. Install Fabric Manager Web Client on the same workstation where you installed Fabric Manager Server.

You must install Fabric Manager Web Client to view Performance Manager reports through a web browser.

For switches running Cisco MDS 9000 FabricWare, you need to install the Fabric Manager Web Client software from the CD-ROM included with your switch, or download Fabric Manager from Cisco.com.

To install Fabric Manager Web Client from the CD-ROM, navigate to the Fabric Manager installation notes and follow the directions.

To download the software from Cisco.com (requires a valid user name and password), go to the following website:

<http://cisco.com/cgi-bin/tablebuild.pl/mds-fm>

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

To download and install the software on your workstation, follow these steps:

- Step 1** Optionally, enter the IP address or host name of the supervisor module running Cisco MDS NX-OS in the Location or Address field of your browser. You see the installation page displayed by the HTTP server of the supervisor module.
- When you connect to the server for the first time, it checks to see if you have the correct Sun Java Virtual Machine version installed on your workstation. If you do not have the correct version installed, a link is provided to the appropriate web page on the Sun Microsystems website so you can install it.
- Click the **Sun Java Virtual Machine** software link (if required) to install the software.
  - Using the instructions provided by the Sun Microsystems website, reconnect to the supervisor module by reentering the IP address or host name in the Location or Address field of your browser.



**Note** We recommend Java version 1.5(x) or later. To use IPv6 addresses, you must have Java version 1.5. To change the Java Runtime Environment (JRE) version, start **Java Web Start** and set the Java preferences.

- Step 2** Click the **Fabric Manager Web Client** installation link. You see a prompt asking for permission to install the application on your workstation.
- Step 3** Click **Yes** to run the installer, which detects the installed version of the software, and prompts for upgrades or downgrades and other options if applicable.



**Note** If TCP port 80 is in use, Fabric Manager Web Client checks port 8080 next. If that port is also in use, Fabric Manager Web Client uses the next available port. You can set the TCP port that you want Fabric Manager Web Client to use during the installation process.

Unless you specify a different directory on a Windows PC, the software is installed in the default location of **C:\Program Files\Cisco Systems\MDS 9000**. A **Cisco MDS 9000** program group is created under Start > Programs. This program group contains shortcuts to Fabric Manager and Device manager.

On a UNIX (Solaris or Linux) machine, the installation path is `/usr/local/cisco_mds9000`. If this directory is not writable by the user, which is the case for non-root users, the default is set to `$HOME/cisco_mds9000`. Shell scripts are created in the bin directory.



**Note** On a Windows PC, you install Fabric Manager Web Client as a service. This service can then be administered using the Services Panel from the Windows Control Panel. By default, Fabric Manager Web Client automatically starts when the workstation is rebooted. You can change this behavior by modifying the properties in the Services Panel.



**Note** You need to configure the Fabric Manager Server on the DNS server for remote logins unless the Fabric Manager Server is binding to a specific interface.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Using Fabric Manager Web Client with SSL

Fabric Manager Web Client uses TCP port 80 by default. If you want to install SSL certificates and use Fabric Manager Web Client over HTTPS (using TCP port 443 or another custom port), you need a certificate for each external IP address that accepts secure connections. You can purchase these certificates from a well-known Certificate Authority (CA).

To enable SSL, users must set up the keystore to use either a self-signed certificate or a certificate from a trusted third-party company such as Verisign.

To create a local certificate, follow these steps:

- 
- Step 1** Set up a keystore to use self-signed certificate (local certificate). From the command line, enter the following command:
- ```
%JAVA_HOME%/bin/keytool -genkey -alias tomcat -keyalg RSA -keystore "C:\Program Files\Cisco Systems\MDS 9000\keystore"
```
- Step 2** Enter your name, organization, state, and country. Enter **changeit** when prompted for a keystore password. If you prefer to use your own password, do not forget to change the keystorepass attribute in the server.xml file. When prompted for a key password, press **Enter** or use the same password as the keystore password.




**Note** You can now follow the steps in the next section for modifying Fabric Manager Web Client to use SSL.

---

In order to obtain a certificate from the Certificate Authority of your choice, you must create a Certificate Signing Request (CSR). The CSR is used by the certificate authority to create a certificate that identifies your website as secure.

To create a CSR, follow these steps:

- 
- Step 1** Create a local certificate (as described in the previous section).
-  **Note** You must enter the domain of your website in the field first and last name in order to create a working certificate.
- 
- Step 2** The CSR is then created with this command:
- ```
keytool -certreq -keyalg RSA -alias tomcat -file certreq.csr -keystore "C:\Program Files\Cisco Systems\MDS 9000\keystore"
```
- Now you have a file called certreq.csr. The file is encoded in PEM format. You can submit it to the certificate authority. You can find instructions for submitting the file on the Certificate Authority website. You will receive a certificate.
- Step 3** Once you have your certificate, you can import it into your local keystore. You must first import a Chain Certificate or Root Certificate into your keystore. You can then import your certificate.
- Step 4** Download a Chain Certificate from the Certificate Authority where you obtained the certificate:
- For Verisign.com commercial certificates, go to:  
<http://www.verisign.com/support/install/intermediate.html>

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- For Verisign.com trial certificates, go to:  
[http://www.verisign.com/support/verisign-intermediate-ca/Trial\\_Secure\\_Server\\_Root/index.html](http://www.verisign.com/support/verisign-intermediate-ca/Trial_Secure_Server_Root/index.html)
- For Trustcenter.de, go to:  
<http://www.trustcenter.de/certservices/cacerts/en/en.htm#server>
- For Thawte.com, go to:  
<http://www.thawte.com/certs/trustmap.html>
- Import the Chain Certificate into your keystore by entering the following command:  
**keytool -import -alias root -keystore "C:\Program Files\Cisco Systems\MDS 9000\keystore" -trustcacerts -file filename\_of\_the\_chain\_certificate**
- Import the new certificate in X509 format:  
**keytool -import -alias tomcat -keystore "C:\Program Files\Cisco Systems\MDS 9000\keystore" -trustcacerts -file your\_certificate\_filename**

To modify Fabric Manager Web Client to use SSL, follow these steps:

- Step 1** Stop Fabric Manager Web Client if you have already launched it. If you installed this on Windows, you can stop the service using Windows Services under Administrative Tools.
- Step 2** Use a text editor to open `\jboss\server\default\deploy\jboss-web.deployer\server.xml` from the directory where Fabric Manager Web Client is installed. You see the following lines in the beginning after some copyright information:

```
<Connector className="org.apache.catalina.connector.http.HttpConnector"
    port="80" minProcessors="5" maxProcessors="75"
    enableLookups="false" redirectPort="8443"
    acceptCount="10" debug="0" connectionTimeout="60000" />
<!-- Define an SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector className="org.apache.catalina.connector.http.HttpConnector"
    port="8443" minProcessors="5" maxProcessors="75"
    enableLookups="true"
    acceptCount="10" debug="0" scheme="https" secure="true">
    <Factory className="org.apache.catalina.net.SSLServerSocketFactory"
        clientAuth="false" protocol="TLS" />
</Connector>
-->
```

- Step 3** Comment the first `<Connector>` element and uncomment the second one. Note that the port changes from 8443 to 443 and keystore and keypass are added. Your file should look like the following example:

```
<!--
<Connector className="org.apache.catalina.connector.http.HttpConnector"
    port="80" minProcessors="5" maxProcessors="75"
    enableLookups="false" redirectPort="8443"
    acceptCount="10" debug="0" connectionTimeout="60000" />
-->
<!-- Define an SSL HTTP/1.1 Connector on port 8443 -->
<Connector className="org.apache.catalina.connector.http.HttpConnector"
```

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

```
port="443" minProcessors="5" maxProcessors="75"
enableLookups="true"
acceptCount="10" debug="0" scheme="https" secure="true">
<Factory className="org.apache.catalina.net.SSLServerSocketFactory"
clientAuth="false" protocol="TLS"
keystoreFile="C:\Program Files\Cisco Systems\MDS 9000\keystore"
keystorePass="changeit"/>
</Connector>
```

- Step 4** Save this file.
- Step 5** Restart Fabric Manager Web Client.



**Note**

If you restart Fabric Manager Server with SSL enabled, you must restart Fabric Manager Web Client. If you want to stop and restart Fabric Manager Server with SSL disabled, then you must restart Fabric Manager Web Client.

## Launching Fabric Manager Web Client

Before you can use Fabric Manager Web Client to monitor a switch, the service must be started on the server you are connecting through. The browser does not have to be on the same workstation where Fabric Manager Web Client is installed.

To launch Fabric Manager Web Client, follow these steps:

- Step 1** If you are on the same workstation where you installed Fabric Manager Web Client, then open your browser and in the Location field enter **http://localhost:PORT**. Enter your port number if you specified a different port during installation. You can omit the port number if you used port 80 by default.

If you are on a different workstation from where you installed Fabric Manager Web Client, then open your browser and in the Location field enter **http://<yourServerAddress>:PORT**, where <yourServerAddress> is the address where you installed Fabric Manager Web Client, and **PORT** is 80 by default. Enter your port number if you specified a different port during installation.



**Tip**

Choose **Start > Control Panel > Administrative Tools > Services** to verify that Fabric Manager Web Client has started. To start Fabric Manager Web Client, use a browser to go to the location of the service.

You can also view this information using the **Admin > Status** menu of the Fabric Manager Web Client.

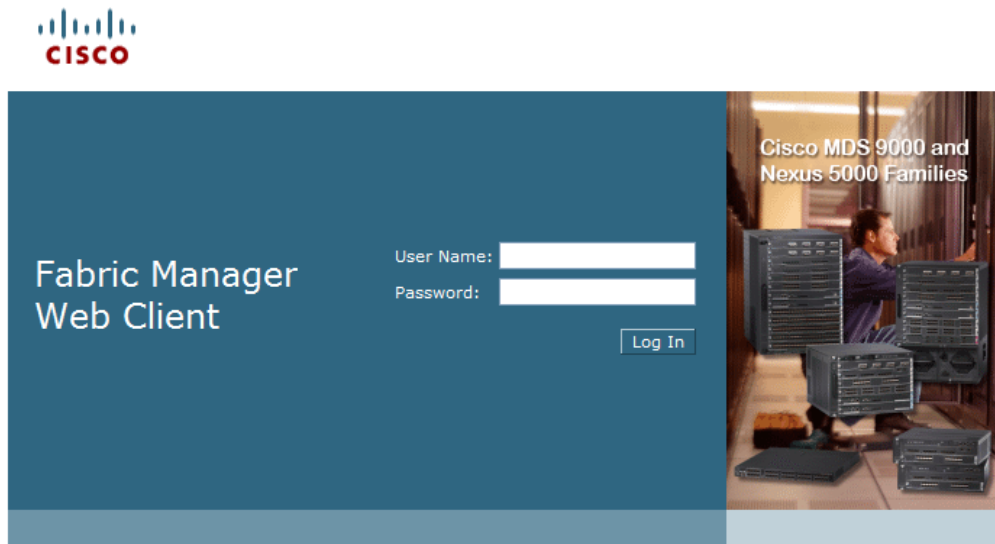
On a UNIX workstation, use the following command:

```
$ /usr/local/cisco_mds9000/bin/FMWebClient.sh status
```

You see the Fabric Manager Web Client Login dialog box as shown in [Figure 7-2](#). The text field at the bottom shows the Message of the Day from the server you logged into.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-2** Fabric Manager Web Client Login Dialog Box



**Step 2** Enter your user name and password.

**Step 3** Click **Login**.



**Note** If you have a new installation of Fabric Manager, the default user ID and password is admin/password. We recommend you change your password the first time you use Fabric Manager Server. If you do not have a new installation, you can use any existing passwords.



**Note** If you are using Firefox to access Fabric Manager Web Client, you may receive a warning message indicating a problem with the security certificate of the website. To resolve this issue, you may need to add the security exception.

To add the security exception, follow these steps:

**Step 1** On the warning page, click **Or you can add an exception**.

**Step 2** Click **Add Exception**.

The Add Security Exception dialog will appear.

**Step 3** Click **Get Certificate**.

Read the text describing the problems with this site.

**Step 4** Click **Confirm Security Exception**.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

After launching Fabric Manager Web Client, you see the screen as shown in [Figure 7-1](#), which you can also see by choosing **Health > Summary**. Fabric Manager Web Client polls the Fabric Manager Server database to display the managed devices in the left pane.

## Health

The Health tab shows events and issues for the selected items, persistent across user sessions.

The Health tab contains the following subtabs:

- **Summary**—Shows a summary of events and problems for all SANs, or a selected SAN, fabric, or switch. You can click any of the blue links for more information about that item.
- **Fabric**—Shows a detailed list of events and hardware, or accounting. You can filter these events by severity, date, and type of event.
- **Syslog**—Shows a detailed list of system messages. You can filter these events by severity, date, and type of event.
- **Analysis**—Enables you to schedule or run analysis reports and compile results to analyze the Fabric Manager Server database statistics.

## Viewing Summary Information

To view a summary of events and problems using Fabric Manager Web Client, follow these steps:

- 
- Step 1** Click the **Health** tab, and then click **Summary** tab.

You see the Summary tab window. In the left navigation pane you see a list of the fabrics managed by Fabric Manager Server. In the right pane is a summary table of problems and events for the last 24 hours as shown in [Figure 7-3](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-3 Summary Tab**



- Step 2** Do one of the following:
- Choose **SAN** to display summary information for all fabrics.
  - Choose one of the fabrics to display summary information for that fabric.
- Step 3** Click the warnings next to Switches, ISLs, Hosts, or Storage (other than 0) to see an inventory of switches, ISLs, or end devices for that fabric.
- Step 4** Choose the number of events next to the event severity levels (Emergency, Alert, Critical, Error, Warning, Notice, Info, or Debug) to see a table of events and descriptions for that fabric.

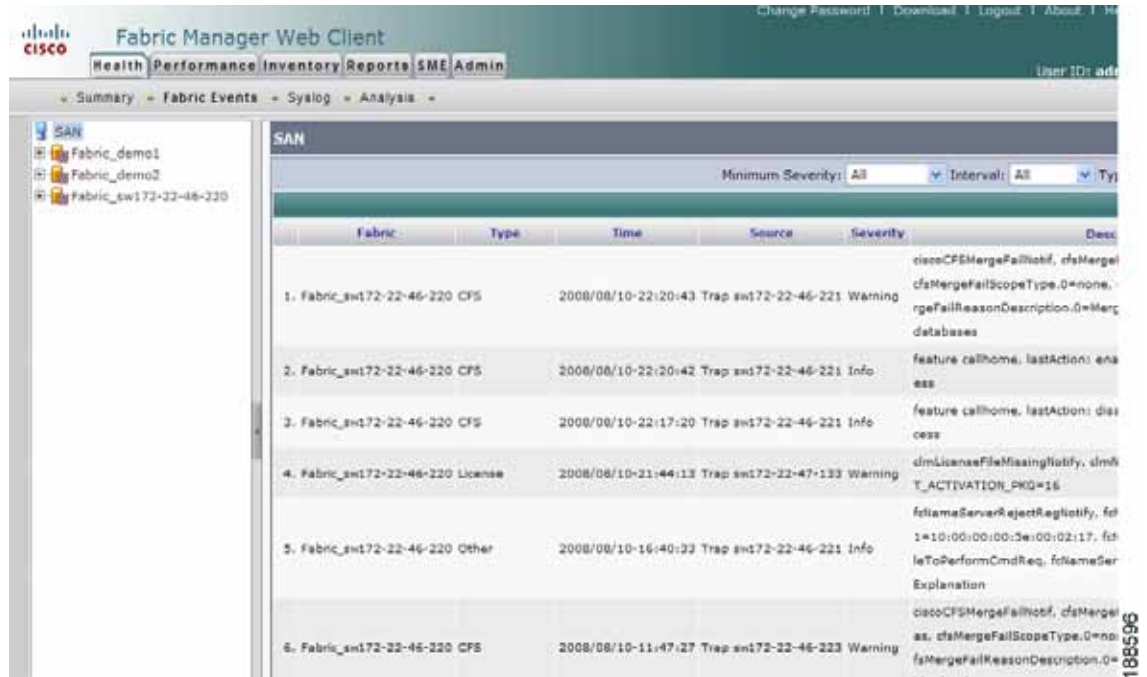
## Viewing Fabric Information

To view a detailed list of events and hardware or accounting using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Health** tab, and then click **Fabric Events** tab.
- You see the Fabric tab window as shown in [Figure 7-4](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-4**      **Fabric Events Tab**



**Step 2**      Expand a fabric and choose one of the switches to display event information for that switch.

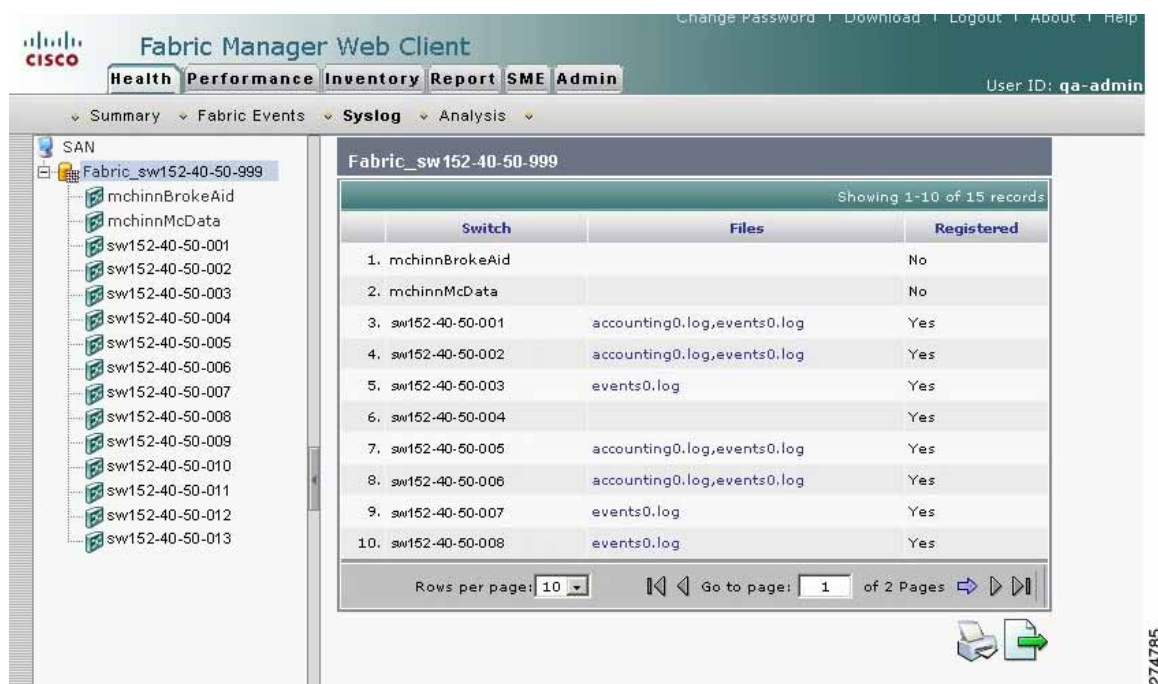
## Viewing Syslog Information

To view a detailed list of system messages using Fabric Manager Web Client, follow these steps:

**Step 1**      Click the **Health** tab, and then click **Syslog** tab.  
You see the Syslog tab as shown in [Figure 7-5](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-5 Syslog Tab**



- Step 2** Select one of the fabrics to display a table of syslog information for that fabric.
- Step 3** Expand a fabric and select one of the switches to display syslog information for that switch.
- Step 4** If you have selected a fabric and one or more switches in that fabric have system messages, you see **Events**, **Hardware**, **Accounting**, and **Link Incidents** in the Files column. Click one of these message types to see system messages for the switches in that fabric filtered by the message type you clicked.



**Note** If you select a switch, choose an interval and a message type from the drop-down lists, and then click **Filter** to see system messages filtered by the message type you chose.



**Note** To view MDS configuration changes, click accountingX.log under **Files**. To view the configuration changes of a switch using Device Manager, click **Logs > FMServer > Accounting > Current**.

## Viewing Analysis Reports

As of Cisco SAN-OS Release 3.2(1) and up to Cisco NX-OS 4.1(3), you can run or schedule analysis reports to summarize the Fabric Manager Server database statistics. You can run or schedule the following analysis reports:

- **Connectivity** (Host to Storage or Storage to Host)—The connectivity report summarizes zoning for multiple hosts or storage devices. If you choose host to storage, the report shows all storage devices zoned as accessible by each host. If you choose storage to host, the report shows all hosts that can access a specific storage device.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

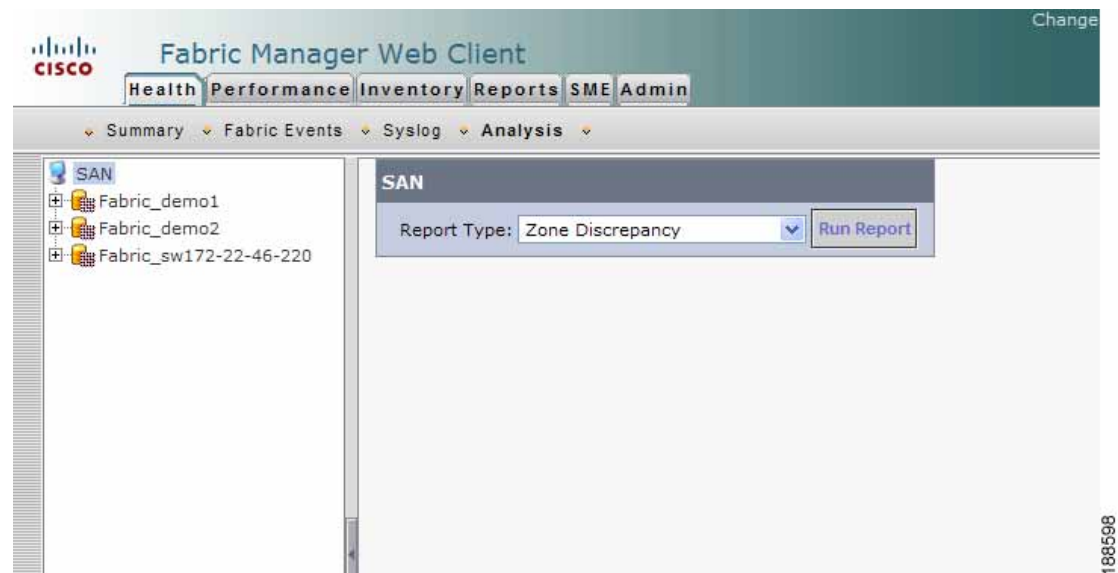
- **Zoning Discrepancies**—The zoning discrepancies report identifies zoning issues that might impact connectivity or security.
- **Multi Path**—The multi path report determines the number of active and inactive paths between hosts and storage enclosures.
- **Switch Health**—The switch health report provides status information on all critical Cisco MDS 9000 system, module, port, and Fibre Channel services.
- **Fabric Configuration**—The fabric configuration analysis compares multiple switches to a specific switch or a saved configuration.

To run analysis reports using Fabric Manager Web Client, follow these steps:

**Step 1** Click the **Health** tab, and then click **Analysis** tab.

You see the Analysis tab shown in [Figure 7-6](#).

**Figure 7-6 Analysis Tab**



**Step 2** Select a report from the Report Type drop-down list.

**Step 3** Click **Run Report** to run the report.

To schedule a report to run at a specified time, see [“Generating Custom Reports by Template” section on page 7-45](#).

## Performance

The Performance tab shows an overview of the average throughput and link utilization of SAN components. You see pie charts for the throughput and utilization. You can click a pie chart to view a table of the data. In these tables, clicking a blue link displays a graph of that data, if applicable. The Filter drop-down list at the top right of the screen allows you to filter the data based on various periods of time.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

The Performance tab contains the following subtabs:

- **Summary**—Shows the total utilization and throughput in summary form.
- **End Devices**—Shows a detailed list of end devices (host or storage), port traffic, and errors.
- **ISLs**—Shows a detailed list of ISL traffic and errors.
- **NPV Links**— Shows a detailed list of traffic between NPV devices and ports.
- **Flows**—Shows a detailed list of host-to-storage traffic.
- **Ethernet**—Shows a detailed list of Gigabit Ethernet ports and Cisco Nexus 5000 Series Ethernet ports and Ethernet port channels.
- **Others**—Shows a detailed list of other statistics.
- **Traffic Analyzer**—Shows a summary of SPAN ports configured in the SAN and any traffic analyzers configured.
- **Prediction**—Displays a graph that predicts future performance to help determine when storage network connections will become overutilized.
- **Switch Bandwidth**—Shows total bandwidth for a switch.

## Viewing Performance Summary Information

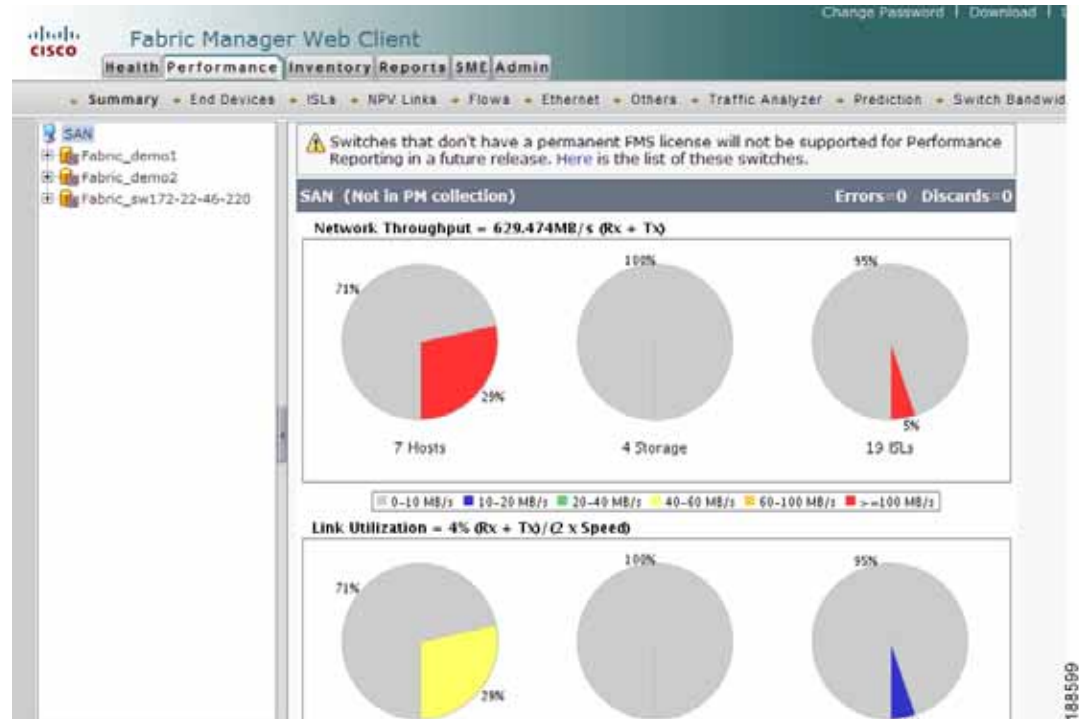
To view total utilization and throughput in summary form using Fabric Manager Web Client, follow these steps:

- 
- Step 1** Click the **Performance** tab, and then click **Summary** tab.

You see the Summary tab shown in [Figure 7-7](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-7 Summary Tab**



- Step 2** Expand a fabric and select one of the VSANs to display network throughput and link utilization information for that VSAN.



**Note** Click a pie chart (Hosts, Storage, or ISLs) to go to the appropriate performance table.



**Note** License compliance information is provided at the top of the pane indicating that unlicensed switches may not be supported in the future. You can click the link to view the list of unlicensed switches.



**Note** To view performance information, you must activate performance collector. To configure Performance Manager, follow the instructions described in the [“Creating Performance Collections”](#) section on page 7-61.

## Performance Detail Summary Report

To view a detailed summary report of the performance details using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Performance** tab, and then click **Summary** tab.
- Step 2** Click the **Performance Utilization Summary Details** link at the bottom of the page.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

You will see the summary report details as shown in [Figure 7-8](#).

**Figure 7-8** Performance Utilization Detail Summary Report

Performance Detail Summary Report

Device Bandwidth Utilization (per port)

	Fabric Name	Device Count	0 ~ 25%			25 ~ 75%			75 ~ 100%			Average (rx+tx)
			Avg1	Max Rx1	Max Tx1	Avg2	Max Rx2	Max Tx2	Avg3	Max Rx3	Max Tx3	
1.	Fabric_sw172-22-46-220	11	11	11	11	0	0	0	0	0	0	0 38.067MB
2.	TOTALS	11	11	11	11	0	0	0	0	0	0	0 38.067MB

Note: ISL Bandwidth ignore the ports with N/A traffic.

ISL Bandwidth Utilization (per port)

	Fabric Name	ISL Count	0 ~ 25%			25 ~ 75%			75 ~ 100%			Average (rx+tx)
			Avg1	Max Rx1	Max Tx1	Avg2	Max Rx2	Max Tx2	Avg3	Max Rx3	Max Tx3	
1.	Fabric_sw172-22-46-220	52	52	52	52	0	0	0	0	0	0	0 8.084MB
2.	TOTALS	52	52	52	52	0	0	0	0	0	0	0 8.084MB

Note: ISL Bandwidth ignore the ports with N/A traffic.

# Viewing Performance Information for End Devices

To view host and storage port traffic and errors using Fabric Manager Web Client, follow these steps:

- Step 1
- Click the **Performance** tab, and then click **End Devices** tab.

You see the End Devices tab window as shown in [Figure 7-9](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-9** End Devices Tab

The screenshot shows the 'Fabric Manager Web Client' interface. The 'Performance' tab is selected, and the 'End Devices' sub-tab is active. A sidebar on the left shows a tree view with 'SAN' expanded, listing 'Fabric\_sw-244-42' and 'Fabric\_sw-9509-207'. The main area displays a table titled 'SAN' with columns: Fabric, VSAN Id, Name, I/F Speed, Avg. Rx/sec, Avg. Tx/sec, (Rx+Tx)/sec, and Pa. The table lists 10 entries for Fabric\_sw-9509-207, showing VSAN 1 and various Qlogic device names. The first four entries show high traffic (Avg. Rx/Tx of 104.297MB), while the last six show zero traffic. A 'Rows per page: 10' dropdown is at the bottom.

Fabric	VSAN Id	Name	I/F Speed	Avg. Rx/sec	Avg. Tx/sec	(Rx+Tx)/sec	Pa
1. Fabric_sw-9509-207	1	10:00:00:00:00:04:00:00	n/a	104.297MB	104.297MB	208.594MB	
2. Fabric_sw-9509-207	1	10:00:00:00:00:02:00:00	n/a	104.297MB	104.297MB	208.594MB	
3. Fabric_sw-9509-207	1	10:00:00:00:00:03:00:00	n/a	104.297MB	104.297MB	208.594MB	
4. Fabric_sw-9509-207	1	10:00:00:00:00:01:00:00	n/a	104.297MB	104.297MB	208.594MB	
5. Fabric_sw-9509-207	1	Qlogic 21:01:00:00:8b:39:5d:37	n/a	0B	0B	0B	
6. Fabric_sw-9509-207	1	Qlogic 21:00:00:00:8b:19:3d:37	n/a	0B	0B	0B	
7. Fabric_sw-9509-207	1	Qlogic 21:00:00:00:8b:19:ff:36	n/a	0B	0B	0B	
8. Fabric_sw-9509-207	1	Qlogic 21:01:00:00:8b:39:ff:36	n/a	0B	0B	0B	
9. Fabric_sw-9509-207	1	Qlogic 21:01:00:00:8b:39:70:37	n/a	0B	0B	0B	
10. Fabric_sw-9509-207	1	Qlogic 21:00:00:00:8b:19:2b:39	n/a	0B	0B	0B	

**Step 2** Expand a fabric and select one of the VSANs to display performance information for the end devices in that VSAN.

**Step 3** Click the name of a device in the Name column to see a graph of the traffic on that device for the past 24 hours.



#### Note

There are variations to this procedure. In addition to these basic steps, you can also perform the following steps to view detailed information for the end devices:

- To change the time range for this graph, select it from the drop-down list in the upper right corner.
- To view the detailed information for specific period, drag the slider control to choose the time interval for which you need the information.
- To view information in grid format, click the grid icon in the bottom right corner.
- To export the data into a spreadsheet, click the excel icon in the upper right corner and then click **Save**.
- To view real time information, select **Real Time** from the drop-down list in the upper right corner. Real time data is updated in every 10 seconds.

## Viewing Performance Information for ISLs

To view ISL traffic and errors using Fabric Manager Web Client, follow these steps:

**Step 1** Click the **Performance** tab, and then click **ISLs** tab.

You see the ISLs tab window as shown in [Figure 7-10](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-10 ISLs Tab**

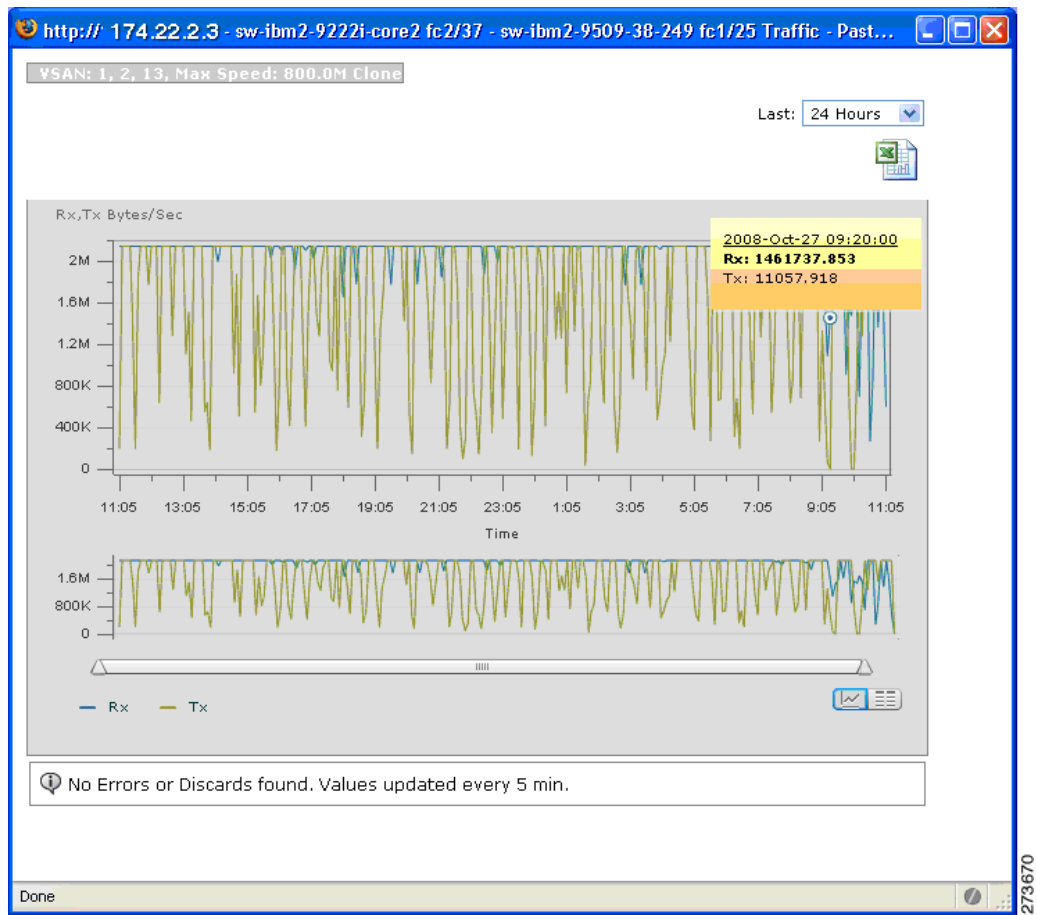
Fabric	VSAN Id	Name	I/F Speed	Avg. Rx/sec
1. Fabric_sw172-22-46-220	1,2,4...	sw172-22-46-220 fc3/2<->sw172-22-46-174 fc3/2	1,000MB	210.148MB
2. Fabric_sw172-22-46-220	1,2	sw172-22-47-133 fc3/1<->sw172-22-46-174 fc3/10	400,000MB	1,224KB
3. Fabric_sw172-22-46-220	1,2,4...	sw172-22-46-224 fc1/17<->sw172-22-46-221 fc2/17	200,000MB	634B
4. Fabric_sw172-22-46-220	1,2,4...	sw172-22-46-220 fc2/10<->sw172-22-46-221 fc2/13	200,000MB	352B
5. Fabric_sw172-22-46-220	1,2,4...	sw172-22-46-220 fc2/16<->sw172-22-46-221 fc2/25	200,000MB	313B
6. Fabric_sw172-22-46-220	1,444...	sw172-22-46-222 fc1/4<->sw172-22-46-225 fc1/4	200,000MB	167B
7. Fabric_sw172-22-46-220	1,2,4...	sw172-22-46-223 fc1/3<->sw172-22-46-224 fc1/3	200,000MB	214B
8. Fabric_sw172-22-46-220	1,444...	sw172-22-46-223 fc1/16<->sw172-22-46-225 fc1/16	200,000MB	211B
9. Fabric_sw172-22-46-220	1	172.22.47.167 fc1/1<->sw172-22-46-174 fc10/30	400,000MB	143B
10. Fabric_sw172-22-46-220	1,2,4...	sw172-22-46-225 fc1/13<->sw172-22-46-224 fc1/13	200,000MB	113B

- Step 2** Expand a fabric and select one of the VSANs to display performance information for the ISLs in that VSAN.
- Step 3** Click the name of an ISL from the Name column to see a graph of the traffic across that ISL for the past 24 hours.

You see the ISL traffic information window as shown in [Figure 7-11](#).

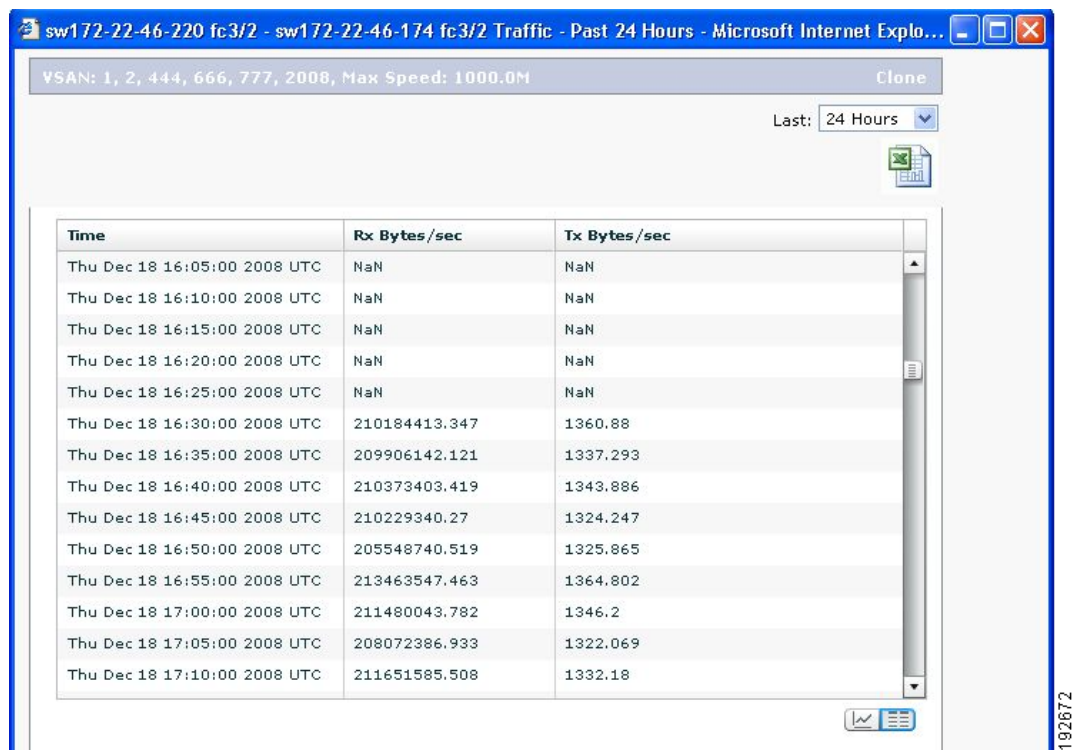
*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-11 ISL Traffic (24 Hours)**



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-12 ISL Traffic Grid View**



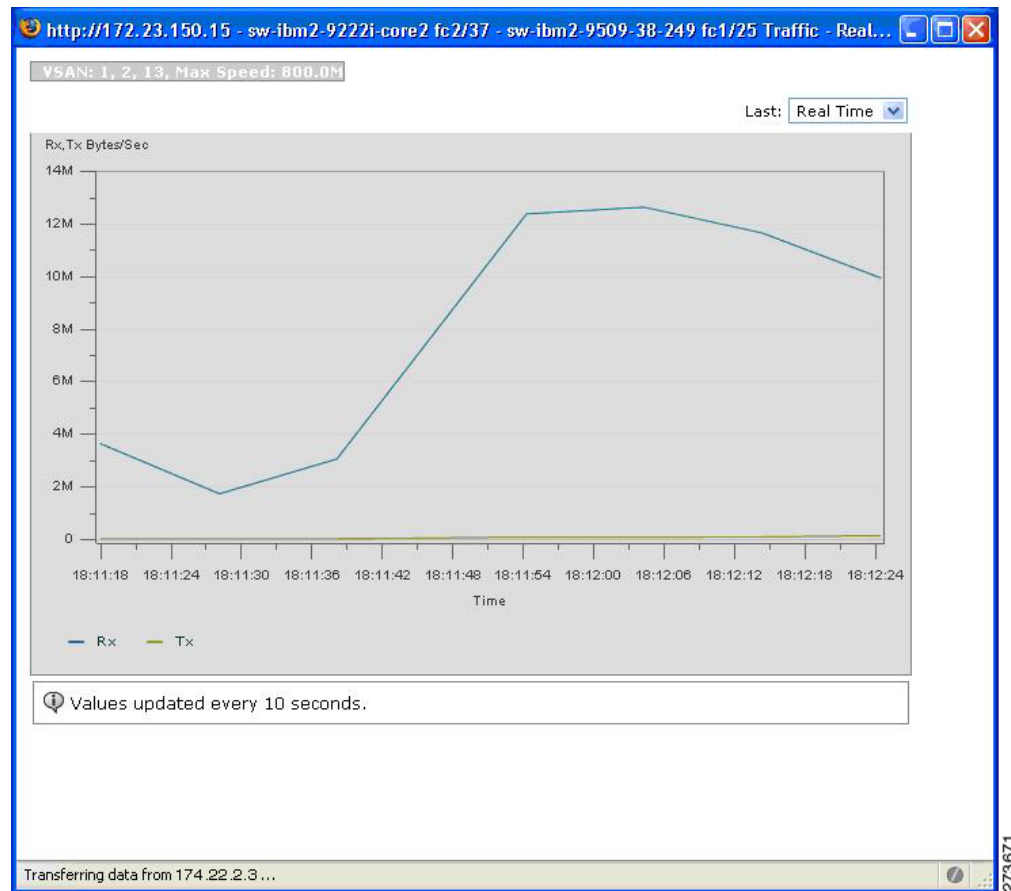
**Note**

Notation NaN (Not a Number) in the data grid means it is a negative value.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-13 ISL Traffic (Real Time)**



**Note**

There are variations to this procedure. In addition to the basic steps described above, you can also perform the following steps to view detailed information for ISLs:

- To change the time range for this graph, select it from the drop-down list in the upper right corner.
- To view the detailed information for specific period, drag the slider control to choose the time interval for which you need the information.
- To view information in grid format, click the grid icon in the bottom right corner.
- To export the data into a spreadsheet, click the excel icon in the upper right corner and then click **Save**.
- To view real time information, select **Real Time** from the drop-down list in the upper right corner. Real time data is updated in every 10 seconds.

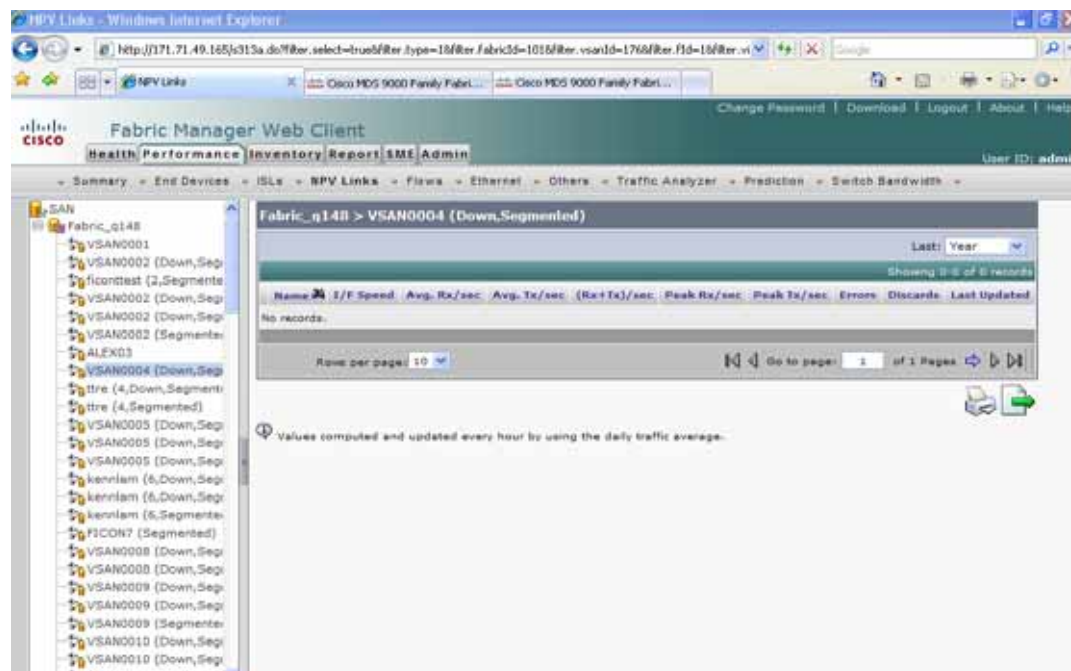
*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Viewing Performance Information for NPV Links

To view traffic between NPV devices and ports using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Performance** tab, and then click **NPV Links**.  
You see the NPV Links tab window shown in [Figure 7-14](#).

**Figure 7-14 NPV Links Tab**



- Step 2** Expand a fabric and select one of the VSANs to display performance information for the NPV Links in that VSAN.
- Step 3** Click the name of an NPV Link from the Name column to see a list of the traffic for the past 24 hours.



### Note

There are variations to this procedure. In addition to the basic steps described above, you can also perform the following steps to view detailed information for NPV Links:

- You can change the time range for this information by selecting it from the drop-down list in the upper right corner.
- To view the detailed information for specific period, drag the slider control to choose the time interval for which you need the information.
- To view information in grid format, click the grid icon in the bottom right corner.
- To export the data into a spreadsheet, click the excel icon in the upper right corner and then click **Save**.
- To view real time information, select Real Time from the drop-down list in the upper right corner. Real time data is updated in every 10 seconds.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Viewing Performance Information for Flows

To view host and storage traffic using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Performance** tab, and then click **Flows**.  
You see the Flows tab window as shown in [Figure 7-15](#).

**Figure 7-15** Flows Tab

Fabric	VSAN Id	Name	Avg. Rx/s
1. Fabric_sw172-22-46-220	1	Emulex 10:00:00:00:00:00:00:00->ClarionDA60	
2. Fabric_sw172-22-46-220	1	Emulex 10:00:00:00:00:00:00:00->ClarionDA60	
3. Fabric_sw172-22-46-220	1	ClarionDA60->SymBus 20:03:00:a0:b8:0e:0e:25	
4. Fabric_sw172-22-46-220	4001	Emulex 10:00:00:00:00:00:00:00->Seagate 21:00:00:20:37:39:ad:77	
5. Fabric_sw172-22-46-220	1	Emulex 10:00:00:00:00:00:00:00->SymBus 20:03:00:a0:b8:0e:0e:25	
6. Fabric_sw172-22-46-220	1	Emulex 10:00:00:00:00:00:00:00->SymBus 20:03:00:a0:b8:0e:0e:25	
7. Fabric_sw172-22-46-220	1	myINIDA7107<->ClarionDA60	
8. Fabric_sw172-22-46-220	1	myTapeDevD4x183<->SymBus 20:03:00:a0:b8:0e:0e:25	
9. Fabric_sw172-22-46-220	1	myINIDA7107<->SymBus 20:03:00:a0:b8:0e:0e:25	
10. Fabric_sw172-22-46-220	1	myINIDA7107<->SymBus 20:03:00:a0:b8:0e:0e:25	

- Step 2** Expand a fabric and select one of the VSANs to display performance information for the flows in that VSAN.
- Step 3** Click the name of a flow from the Name column to see a list of the traffic for the past 24 hours.



### Note

There are variations to this procedure. In addition to these basic steps, you can also perform the following steps to view detailed information for Flows:

- To change the time range for this graph, select it from the drop-down list in the upper right corner.
- To view the detailed information for specific period, drag the slider control to choose the time interval for which you need the information.
- To view information in grid format, click the grid icon in the bottom right corner.
- To export the data into a spreadsheet, click the excel icon in the upper right corner and then click Save.
- To view real time information, select Real Time from the drop-down list in the upper right corner. Real time data is updated in every 10 seconds.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Viewing Performance Information for Gigabit Ethernet and Ethernet Ports

To view Gigabit Ethernet ports and Cisco Nexus 5000 Series Ethernet ports and Ethernet PortChannel using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Performance** tab, and then click **Ethernet**.  
You see the Ethernet tab window as shown in [Figure 7-16](#).

**Figure 7-16 Ethernet Tab**



- Step 2** Expand a fabric and choose one of the VSANs to display the Gigabit Ethernet ports and Cisco Nexus 5000 Series Ethernet ports and PortChannel in that VSAN.



### Note

There are variations to this procedure. In addition to these basic steps, you can also:

- Select the time range, and click **Filter** to filter the display.
- Select the name of a GigE port from the Name column to see a graph of the traffic across that GigE port for the past 24 hours. You can change the time range for this graph by selecting it from the drop-down list in the upper right corner.

## Viewing Other Statistics

To view other statistics using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Performance** tab, and then click **Others**.  
You see the Others tab window as shown in [Figure 7-17](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-17 Others Tab**



**Step 2** Expand a fabric and select one of the VSANs to display the other statistics in that VSAN.



**Note**

There are variations to this procedure. In addition to these basic steps, you can also:

- Select the time range, and click **Filter** to filter the display.
- Select the IP address of a switch from the Name column to see a graph of the traffic across that switch for the past 24 hours. You can change the time range for this graph by selecting it from the drop-down list in the upper right corner.



**Note**

To configure Other Statistics, follow the instructions described in the [“Configuring Other Statistics” section on page 7-62](#).

## Viewing Detailed Traffic Information

To view SPAN port detailed traffic using Fabric Manager Web Client, follow these steps:

**Step 1** Click the **Performance** tab, and then click **Traffic Analyzer**.

You see the Traffic Analyzer tab window as shown in [Figure 7-18](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-18 Traffic Analyzer Tab**



- Step 2** Do one of the following:
- Select a SAN to display a list of SPAN ports for switches in all fabrics in the SAN.
  - Select one of the fabrics to display a list of SPAN ports for switches in that fabric.

## Viewing Switch Bandwidth

To view the total bandwidth for a switch using Fabric Manager Web Server, follow these steps:

- Step 1** Choose **Performance > Switch Bandwidth**.
- Step 2** Select the period of time (**24 Hours**, **Week**, **Month** or **Year**) for which you want to view bandwidth usage from the **Last** drop-down list.

## Viewing Predicted Future Performance

To plan storage network changes, it is necessary to determine when configuration changes (such as rezoning) may be needed to meet growing performance demands. Fabric Manager Server provides a performance prediction report to enable you to more easily predict when storage network connections will become overutilized.

In general, to create a performance prediction report, do the following:

- Specify the period of time in the past that you want to use as a sample to predict the future performance.
- Specify the threshold values that you do not want to exceed.
- Specify the period of time in the future for which you want to view performance.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

Fabric Manager Server extrapolates the performance and lists in chronological order which interfaces are expected to reach the threshold within the specified time period.

## Using the Default Values

When you first view predicted future performance by clicking the **Performance** tab and then the **Prediction** tab, you see a table showing the predicted performance for your entire SAN using the default values. The default values are as follows:

- Scope—Entire SAN
- Past performance period—Month
- Future performance period—Month
- Threshold—80%
- SAN elements or links—ISLs
- Performance prediction type—Average

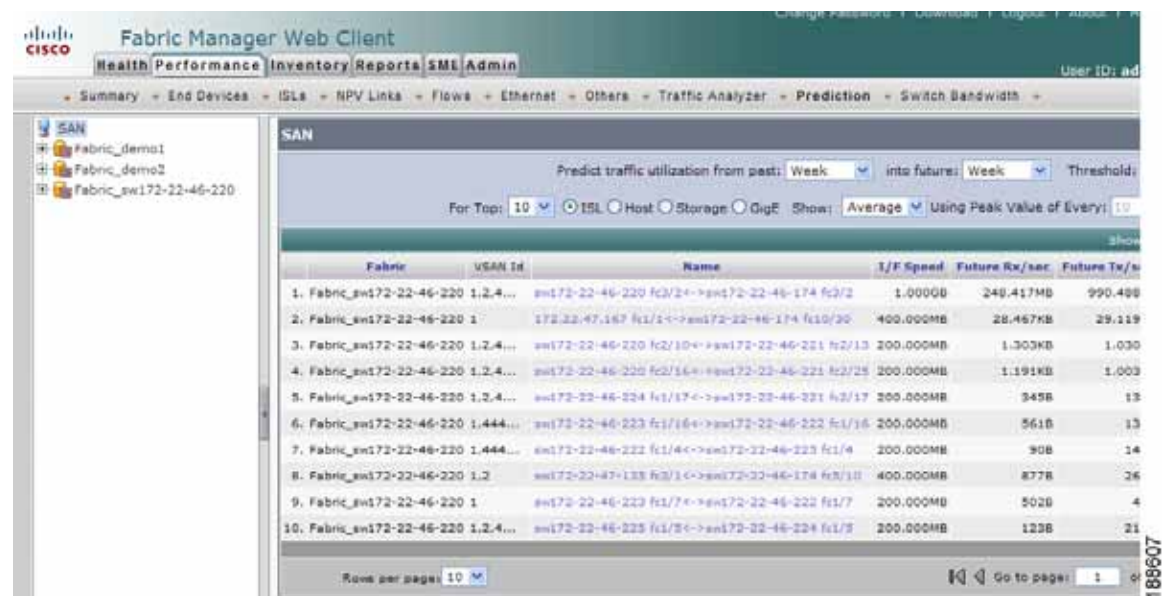
Click a link in the Name column to view a graph of that ISL's performance for the past 24 hours. To view the performance for the past week, month, year, or custom time, select an option from the drop-down list.

## Using Your Own Values

To view a table of predicted future performance with your own values using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Performance** tab, and then click **Prediction**.  
You see the Prediction tab window as shown in [Figure 7-19](#).

**Figure 7-19 Prediction Tab**



- Step 2** Expand a fabric and select one of the VSANs to specify that the prediction report will be generated for that VSAN.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 3** Select the period of time (Week, Month, 3 Months, 6 Months or Year) to use to predict performance from the past drop-down list.
- Step 4** Select the period of time (Week, Month, 3 Months, 6 Months or Year) for which to make the prediction from the future drop-down list.
- Step 5** Enter the threshold percentage (1—100) of utilization that you do not want the traffic to exceed.
- Step 6** Enter the number of ISLs, hosts, storage devices, port group or flows for which you want to make the prediction. The prediction will show the top 10, top 20, or top 50 with the most traffic.
- Step 7** Select the type of traffic prediction to show:
- **Average**—The average value of all the sample data is used.
  - **Peak**—The average value of all the peak values is used. The number of peak values is obtained by dividing the total number of records into groups based on the number you enter in the Use Peak Value of Every *xx* Records field. For example, if you have 1000 records and you enter 100 into the field, your records are divided into 10 groups and 10 peak values are used.
- Step 8** Click **Predict**.
- You see the prediction table with the new data. Click the links in the Name column to show performance charts based on the history data.
- 

## Viewing Switch Bandwidth

To view the total bandwidth for a switch using Fabric Manager Web Client, follow these steps:

- 
- Step 1** Click the **Performance** tab, and then click **Switch Bandwidth**.
- You see the Switch Bandwidth tab window as shown in [Figure 7-20](#).



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-20 Switch Bandwidth Tab**

Fabric Manager Web Client

Health

Performance

Inventory

Reports

SME

Admin

Summary

End Devices

ISLs

NPV Links

Flows

Ethernet

Others

Traffic Analyzer

Prediction

Switch Bandwidth

SAN

Fabric

VSAN Id

Name

I/F Speed

Avg. R/s/sec

1. Fabric\_sw172-22-46-220 1.2.4...

sw172-22-46-220 fc3/2<->sw172-22-46-174 fc3/2

1.000GB

210.148MB

2. Fabric\_sw172-22-46-220 1.2

sw172-22-47-138 fc3/1<->sw172-22-46-174 fc3/10

400.000MB

1.224KB

3. Fabric\_sw172-22-46-220 1.2.4...

sw172-22-46-224 fc1/17<->sw172-22-46-221 fc2/17

200.000MB

634B

4. Fabric\_sw172-22-46-220 1.2.4...

sw172-22-46-220 fc2/10<->sw172-22-46-221 fc2/13

200.000MB

352B

5. Fabric\_sw172-22-46-220 1.2.4...

sw172-22-46-220 fc2/16<->sw172-22-46-221 fc2/28

200.000MB

313B

6. Fabric\_sw172-22-46-220 1.444...

sw172-22-46-222 fc1/4<->sw172-22-46-225 fc1/4

200.000MB

167B

7. Fabric\_sw172-22-46-220 1.2.4...

sw172-22-46-223 fc1/5<->sw172-22-46-224 fc1/5

200.000MB

214B

8. Fabric\_sw172-22-46-220 1.444...

sw172-22-46-223 fc1/16<->sw172-22-46-222 fc1/16

200.000MB

211B

9. Fabric\_sw172-22-46-220 1

172-22-47-187 fc1/1<->sw172-22-46-174 fc10/30

400.000MB

143B

10. Fabric\_sw172-22-46-220 1.2.4...

sw172-22-46-225 fc1/13<->sw172-22-46-224 fc1/13

200.000MB

113B

Rows per page: 10

- Step 2** Select the period of time (24 Hours, Week, Month or Year) for which you want to view bandwidth usage from the Last drop-down list.

## Inventory

The Inventory tab shows an inventory of the selected SAN, fabric, or switch. You can export this information to an ASCII file in comma-separated value format that can be read by applications such as Microsoft Excel. You can set the number of rows and columns per page.

The Inventory tab contains the following subtabs:

- **VSANs**—Shows details about VSANs.
- **Switches**—Shows details about switches.
- **Licenses**—Shows details about the licenses in use in the fabric.
- **Modules**—Shows details for MDS switching and services modules, fans, and power supplies.
- **End Devices**—Shows the host and storage ports.
- **ISLs**—Shows the Inter-Switch Links.
- **NPV Links**—Shows the links between NPV devices and ports.
- **Zones**—Shows the active zone members (including those in inter-VSAN zones).
- **Summary**—Shows VSANs, switches, ISLs, ports, and end devices.

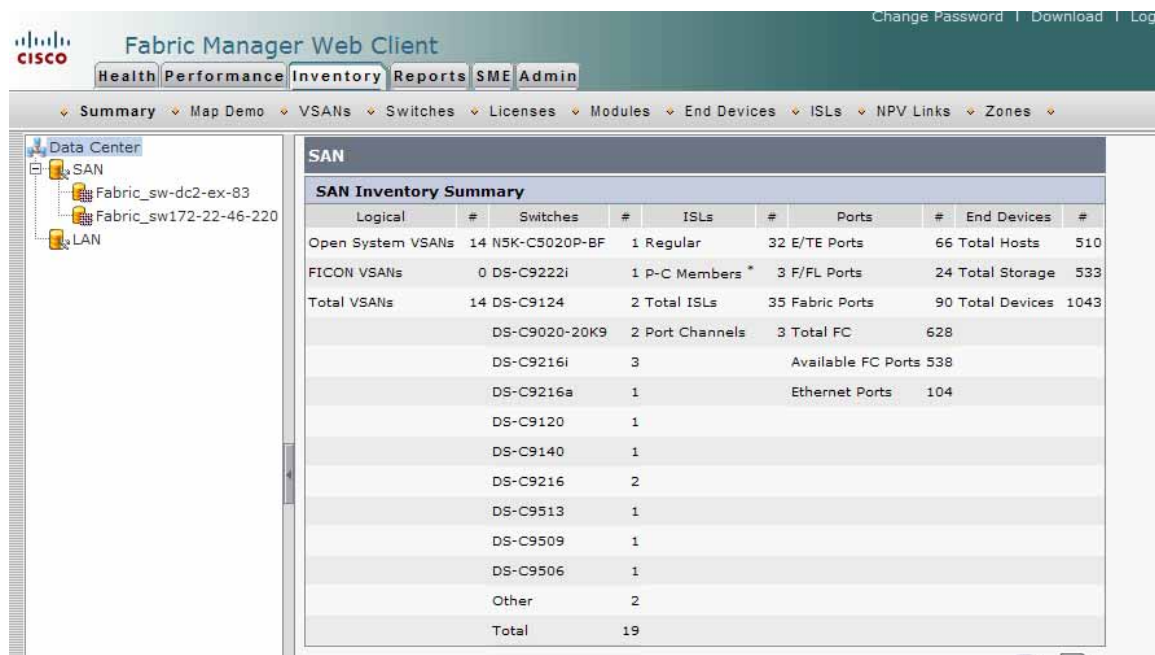
*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Viewing Summary Inventory Information

To view a summary of VSANs, switches, ISLs, ports, and end devices using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Inventory** tab, and then click **Summary**.  
You see the Summary tab window as shown in [Figure 7-21](#).

**Figure 7-21** Summary Tab



- Step 2** Do one of the following:
- Select a SAN to display a summary of inventory information for all fabrics in the SAN.
  - Select one of the fabrics to display a summary of inventory information for that fabric.

## Viewing Detailed Summary Inventory Information

Detailed summary includes a number of key summary statistics such as port usage and any statistics information, license use summary, environmental status and switch states, monitoring and alerting status that is useful for creating comprehensive SAN health reports.

To view a detailed summary using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Inventory** tab, and then click **Summary**.  
**Step 2** Click **Inventory Summary Details** at the bottom of the page.  
You see the Inventory Summary Details as shown in [Figure 7-22](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-22 Detailed Summary Information**

Summary Details - Windows Internet Explorer

http://171.71.49.165/g211.do?filter.fabricId=1

Summary Details

Inventory Detail Summary Report

Device Count

Device Description	Count	Device Description	Count
1. QLogic	1	Cisco	15

Port Usage

Fabric Name	Port Use								Fan Out Ratios			Port Module Types					
	Disk	Tape	Unknown	Device	Host	ISL	HPV	Free	Total	Host:Disk	Port:ISL	Device:ISL	DWDM	10G SFP	SFP	GBIC	OTHER
1. Fabric_q148	4	0		0	4	62	0	-70	0	1.0 : 1	-1.0 : 1	0.12 : 1	0	0	78	0	9
2. TOTALS	4	0		0	4	62	0	-70	0	1.0 : 1	-1.0 : 1	0.12 : 1	0	0	78	0	9

Health Status And Monitoring

Fabric Name	Switch State		Power Supplies			Fans			
	WARN	OK	FAILED	OFF	ON	FAN WARN	DOWN	UP	
1. Fabric_q148	12	4		0	8	13	0	5	22
2. TOTALS	12	4		0	8	13	0	5	22

Permanent License Summary

Fabric Name	10G_PORT	DMM	ENTERPRISE	FM_SERVER	MAINFRAME	PORT	SAN_EXTN	SME	SSE
1. Fabric_q148	0	0	1	0	0	3	0	0	0
2. TOTALS	0	0	1	0	0	3	0	0	0

Trial License Summary

Fabric Name	10G_PORT	DMM	ENTERPRISE	FM_SERVER	MAINFRAME	PORT	SAN_EXTN	SME	SSE
1. Fabric_q148	0	1	11	12	7	0	5	0	1
2. TOTALS	0	1	11	12	7	0	5	0	1

67692

## Viewing Detailed Information for VSANs

To view detailed inventory information about VSANs using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Inventory** tab, and then click **VSANs**.  
You see the VSANs tab window as shown in [Figure 7-23](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-23 VSANs Tab**

Fabric	Id	Name	Status	Activated Zoneset, When
1. Fabric_demo1	1	VSAN0001	Up	DMM_IPFC_ZS, 2008/07/24-03:24:10
2. Fabric_demo1	9	VSAN0009	Down	zs_9, 2008/07/24-03:31:21
3. Fabric_demo1	100	VSAN0100	Down	dmm_zs100, 2008/07/24-03:31:21
4. Fabric_demo2	1	VSAN0001	Up	DMM_IPFC_ZS, 2008/07/29-13:46:05
5. Fabric_demo2	9	VSAN0009	Up	zs_9, 2008/07/29-13:45:58
6. Fabric_demo2	100	VSAN0100	Down	dmm_zs100, 2008/07/29-13:45:58
7. Fabric_sw172-22-46-220	1	VSAN0001	Down, Segmented at sw172-22-46-220	none
8. Fabric_sw172-22-46-220	1	VSAN0001	Up, Segmented at sw172-22-46-220	Zonesetiv1, 2008/08/10-11:09:38
9. Fabric_sw172-22-46-220	2	MyVsan2	Up	Zonesetiv2, 2008/08/10-16:22:37
10. Fabric_sw172-22-46-220	444	VSAN0444	Up	none

**Step 2** Select one of the fabrics to display VSAN inventory information for that fabric.



**Note**

There are variations to this procedure. In addition to these basic steps, you can also:

- Select the status level, then click **Filter** to filter the display to show all VSANs or just those with errors.

## Viewing Detailed Information for Switches

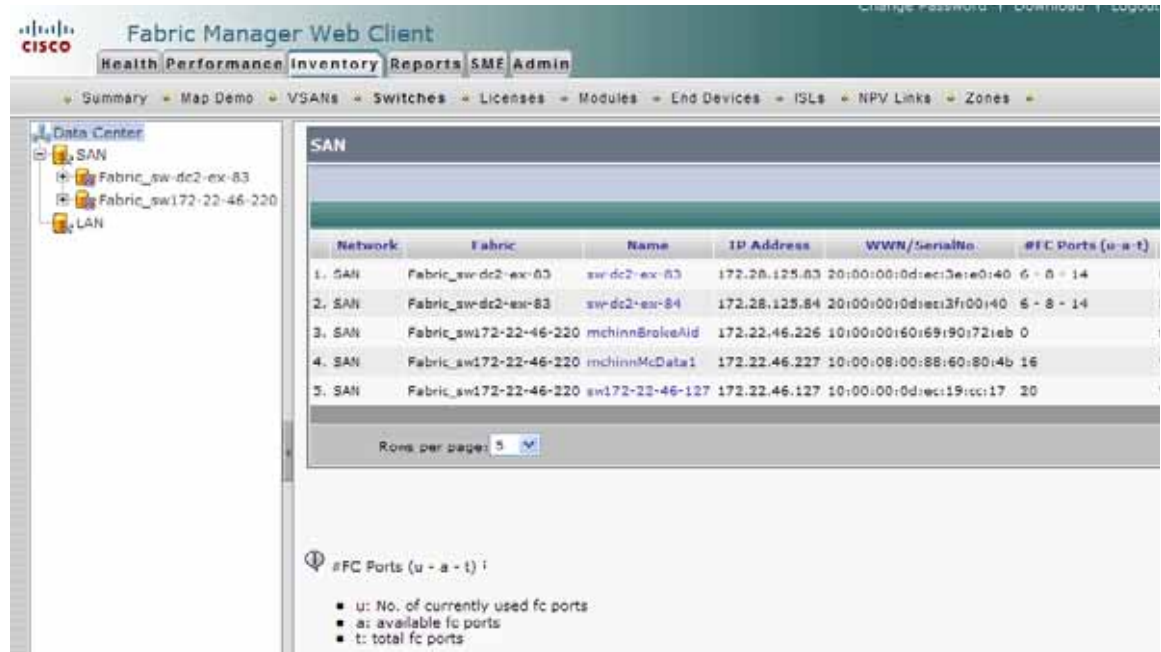
To view detailed inventory information about switches using Fabric Manager Web Client, follow these steps:

**Step 1** Click the **Inventory** tab, and then click **Switches**.

You see the Switches tab window as shown in [Figure 7-24](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-24 Switches Tab**



**Step 2** Do one of the following:

- Select a SAN to display switch inventory information for all fabrics in the SAN.
- Select one of the fabrics to display switch inventory information for that fabric.
- Expand a fabric and select one of the VSANs to display switch inventory information for that VSAN.



**Note** (u-a-t) indicates the number of used (u), available (a) and total (t) Fibre Channel ports.

## Viewing License Information

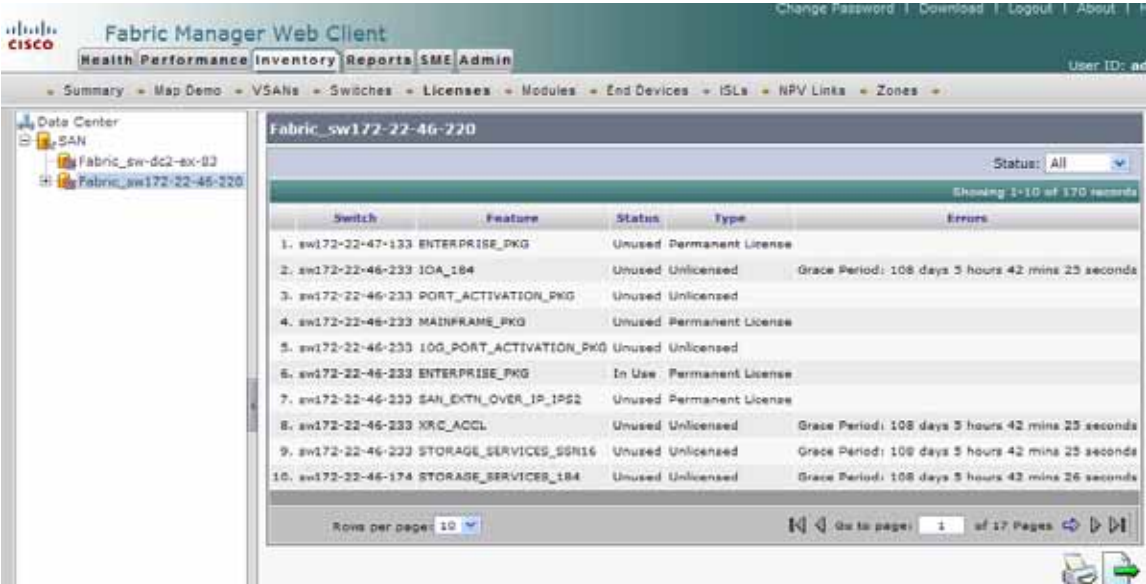
To view license information for switches using Fabric Manager Web Client, follow these steps:

**Step 1** Click the **Inventory** tab, and then click **Licenses**.

You see the Switch Licenses tab window as shown in [Figure 7-25](#).

Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)

Figure 7-25 Switch Licenses Tab



Step 2 Select one of the fabrics to display license information for switches in that fabric.

  
Note

There are variations to this procedure. In addition to these basic steps, you can also:

- Select the status level, and click **Filter** to filter the display to show all licenses or just those with errors.

## Viewing Detailed Information for Modules

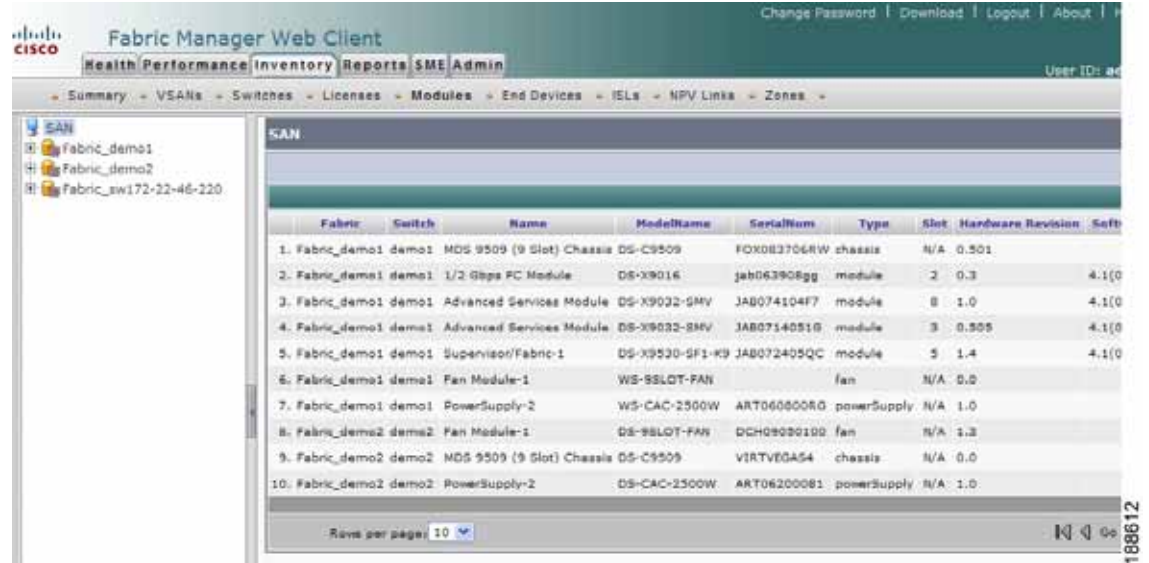
To view detailed inventory information about modules using Fabric Manager Web Client, follow these steps:

Step 1 Click the **Inventory** tab, and then click **Modules**.  
You see the Modules tab window as shown in [Figure 7-26](#).



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-26 Modules Tab**



**Step 2** Do one of the following:

- Select a SAN to display module inventory information for all fabrics in the SAN.
- Select one of the fabrics to display module inventory information for that fabric.
- Expand a fabric and select one of the VSANs to display module inventory information for that VSAN.

## Viewing Detailed Information for End Devices

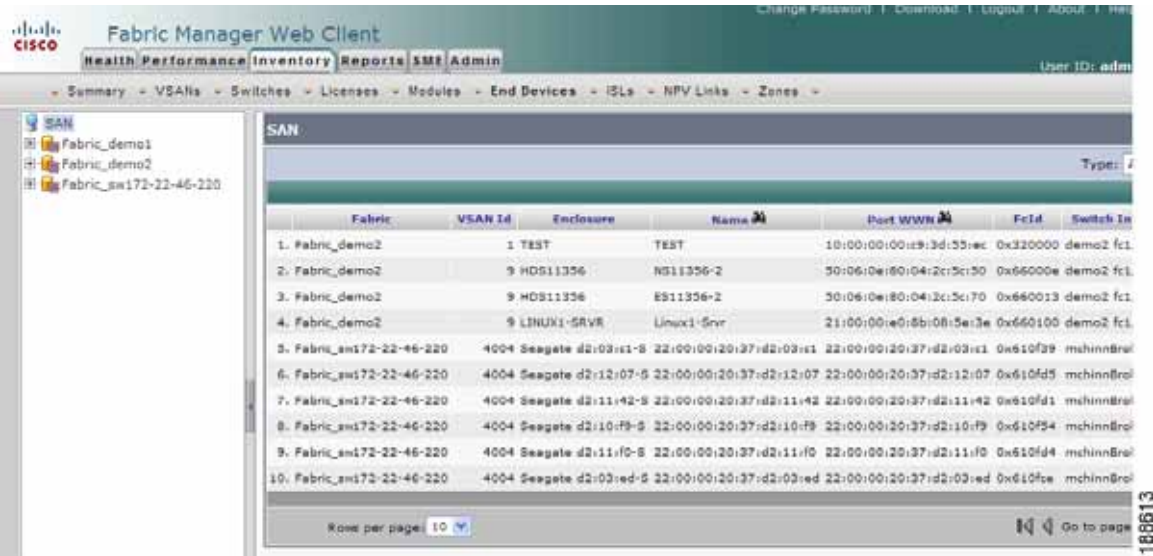
To view detailed inventory information about end devices using Fabric Manager Web Client, follow these steps:

**Step 1** Click the **Inventory** tab, and then click **End Devices**.

You see the End Devices tab window as shown in [Figure 7-27](#).

Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)

Figure 7-27 End Devices Tab



Step 2 Expand a fabric and select one of the VSANs to display end device inventory information for that VSAN.



Note

If you filter by hosts or enclosures, you can click a host in the resulting table to see host enclosure performance, a list of hosts, a list of hosts to which your device is connected, and the connection paths. This allows you to see performance statistics for hosts and enclosures.

You can also filter by end devices or by port groups to view aggregate information for those port groups, such as peak and average usage.

# Viewing Detailed Information for ISLs

To view detailed inventory information about ISLs using Fabric Manager Web Client, follow these steps:

- Step 1 Click the **Inventory** tab, and then click **ISLs**.  
You see the ISLs tab window as shown in [Figure 7-28](#).



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-28** ISLs Tab

	Fabric	VSANs	From Switch	From Interface	To Switch	To Interface
1.	Fabric_sw172-22-46-220	1	172.22.47.167	fc1/1	sw172-22-46-174	fc10/30
2.	Fabric_sw172-22-46-220		172.22.47.167	fc1p2	sw172-22-46-174	fc1p2
3.	Fabric_sw172-22-46-220	4003	mchinMcData	5	sw172-22-46-225	fc1/17
4.	Fabric_sw172-22-46-220	444	sw172-22-46-220	fc1/14	sw172-22-46-174	fc10/14
5.	Fabric_sw172-22-46-220	1,2,444,666,777,4002,4003	sw172-22-46-220	fc9/1	sw172-22-46-174	fc1/1
6.	Fabric_sw172-22-46-220	444	sw172-22-46-220	channel4	sw172-22-46-174	channel1
7.	Fabric_sw172-22-46-220	1,2,444,666,777,4002,4003	sw172-22-46-220	fc3/2	sw172-22-46-174	fc3/2
8.	Fabric_sw172-22-46-220	1,2,444,666,777,4001,4002,4003	sw172-22-46-220	fc2/5	sw172-22-46-221	fc2/5
9.	Fabric_sw172-22-46-220	1,2,444,666,777,4001,4002,4003	sw172-22-46-220	fc2/10	sw172-22-46-221	fc2/13
10.	Fabric_sw172-22-46-220		sw172-22-46-220	fc2/9	sw172-22-46-221	fc2/9

**Step 2** Expand a fabric and select one of the VSANs to display ISL inventory information for that VSAN.



**Note**

There are variations to this procedure. In addition to these basic steps, you can also:

- Select the status level, and click **Filter** to filter the display to show all ISLs or only those with errors.

## Viewing Detailed Information for NPV Links

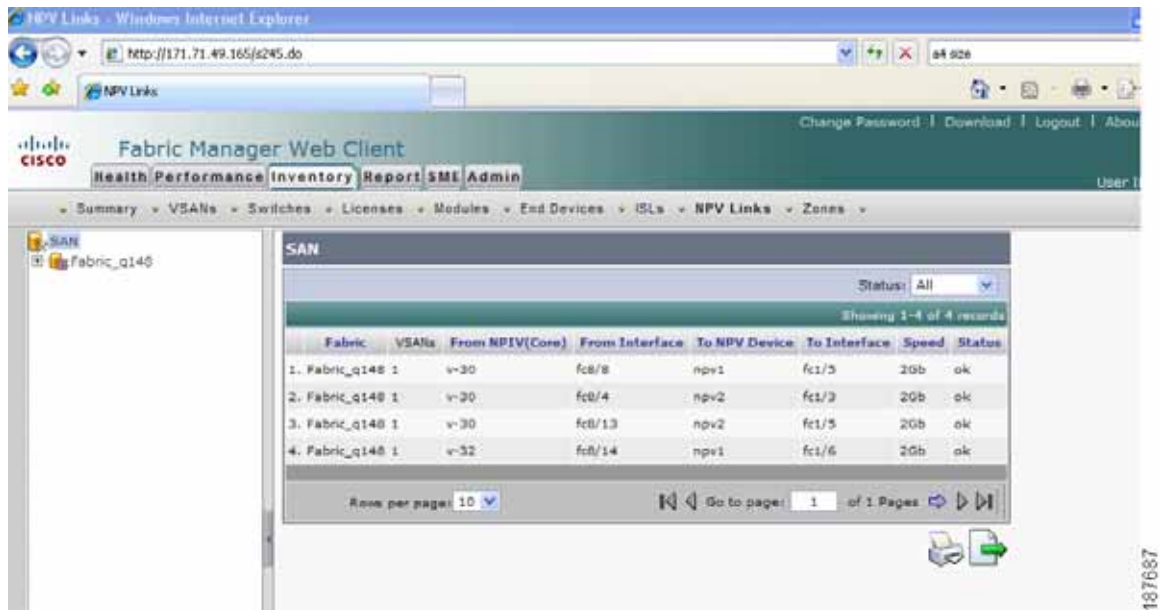
To view detailed inventory information about NPV Links using Fabric Manager Web Client, follow these steps:

**Step 1** Click the **Inventory** tab, and then click **NPV Links**.

You see the NPV Links tab window as shown in [Figure 7-29](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-29 NPV Links**



**Step 2** Expand a fabric and select one of the VSANs to display NPV Links information for that VSAN.

## Viewing Detailed Information for Zones

To view detailed inventory information about zones using Fabric Manager Web Client, follow these steps:

**Step 1** Click the **Inventory** tab, and then click **Zones**.

You see the Zones tab window as shown in [Figure 7-30](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-30** Zones Tab

Fabric	VSAN Id	Zoneset	Zone	Type	Switch Interface	Member
1. Fabric_demo1 1		DMM_IPFC_ZS \$default_zones\$		FCID		
2. Fabric_demo1 1		DMM_IPFC_ZS \$default_zones\$		FCID		
3. Fabric_demo1 1		DMM_IPFC_ZS DMM_IPFC_ZN		IP Subnet(v4)		10.1.2.3
4. Fabric_demo1 1		DMM_IPFC_ZS DMM_IPFC_ZN		IP Subnet(v4)		10.1.2.8
5. Fabric_demo1 1		DMM_IPFC_ZS DMM_IPFC_ZN		IP Subnet(v4)		10.1.2.5
6. Fabric_demo1 9	zs_9	DMM_Zone_admin_2008_07_01_18_09	WWN			21:2b:00:00:30:00
7. Fabric_demo1 9	zs_9	DMM_Zone_admin_2008_07_01_18_09	WWN		demo2 fci/10	ES11356-2
8. Fabric_demo1 9	zs_9	DMM_Zone_admin_2008_07_01_18_09	WWN		demo2 fci/9	NS11356-2
9. Fabric_demo1 9	zs_9	DMM_Zone_admin_2008_07_10_18_21	WWN		demo2 fci/10	ES11356-2
10. Fabric_demo1 9	zs_9	DMM_Zone_admin_2008_07_10_18_21	WWN		demo2 fci/9	NS11356-2

**Step 2** Expand a fabric and select one of the VSANs to display zone inventory information for that VSAN.



**Note**

There are variations to this procedure. In addition to these basic steps, you can also:

- Select the status level, and click **Filter** to filter the display to show all zones or just those with errors.

## Reports

The Reports tab allows you to create customized reports based on historical performance, events, and inventory information gathered by the Fabric Manager Server. You can create aggregate reports with summary and detailed views. You can also view previously saved reports.

The Report tab contains the following subtabs:

- **View**—Displays previously saved reports.
- **Generate**—Generates a custom report based on the selected report template.
- **Configuration**—Creates and configures a report template, allowing you to select any combination of events, performance categories, and inventory.
- **Scheduled Jobs**—Displays scheduled jobs based on the selected report template.

## Creating a Custom Report Template

You can create custom reports from all or any subset of information gathered by Fabric Manager Server. You create a report template by selecting events, performance, and inventory statistics that you want in your report and set the desired SAN, fabric or VSAN to limit the scope of the template. You can generate

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

and schedule a report of your fabric based on this template immediately or at a later time. Fabric Manager Web Client saves each report based on the report template used and the time you generate the report.

As of Cisco MDS NX-OS Release 5.0, the report template design has changed to resolve the limitations of the earlier versions. With the new design model, you can perform add, delete and modify functionalities in a single page. You can choose multiple fabrics and VSANs using the new navigation system and it has good scalability to add new items and categories in future.

The new design model has three panels:

- Template panel.
- Configuration panel.
- User selection panel.

The Template panel allows you to navigate through the available templates, add new templates and delete existing templates.

The Configuration panel allows you to configure a new template when it is added and modify an existing template. The options in the configuration panel will be disabled until the user either adds a new template or select an existing template. The upper portion of the configuration panel is stacked with categories that you can choose and configure.

The User Selection panel displays the user's configuration options in real time. While the configuration panel can display information pertaining to one category at a time, user selection panel displays all the user's selection or configuration.

To create a custom report template using Fabric Manager Web Client, follow these steps:

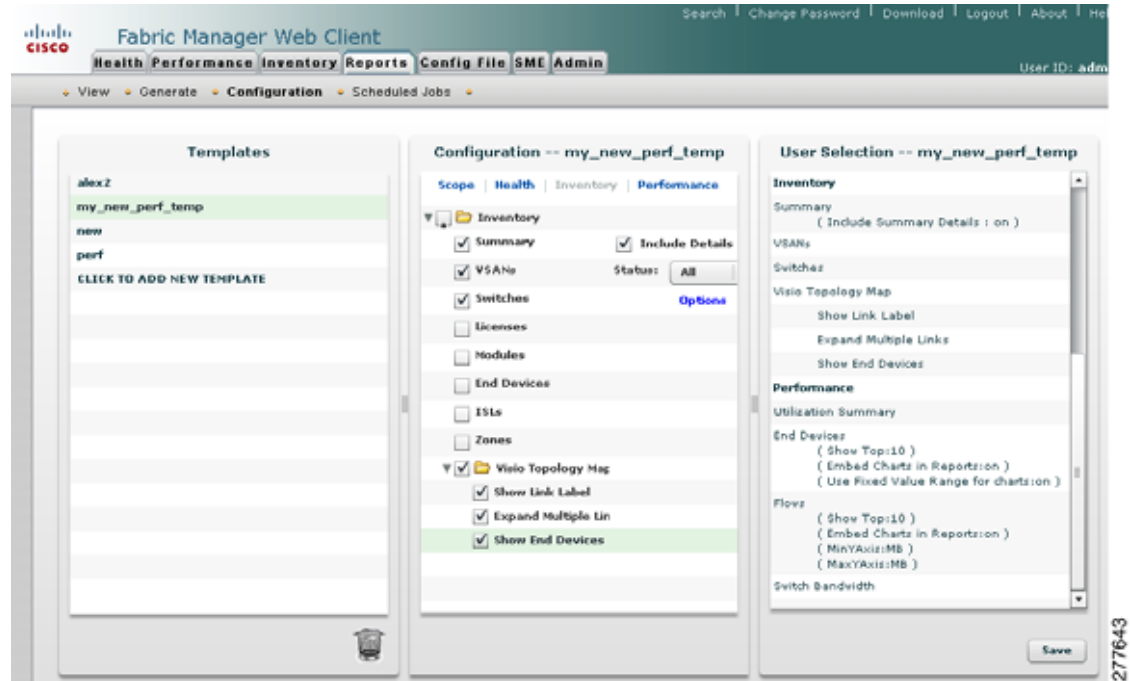
---

**Step 1** Click the **Report** tab, and then click **Configuration**.

You see the Report Configuration tab as shown in [Figure 7-31](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

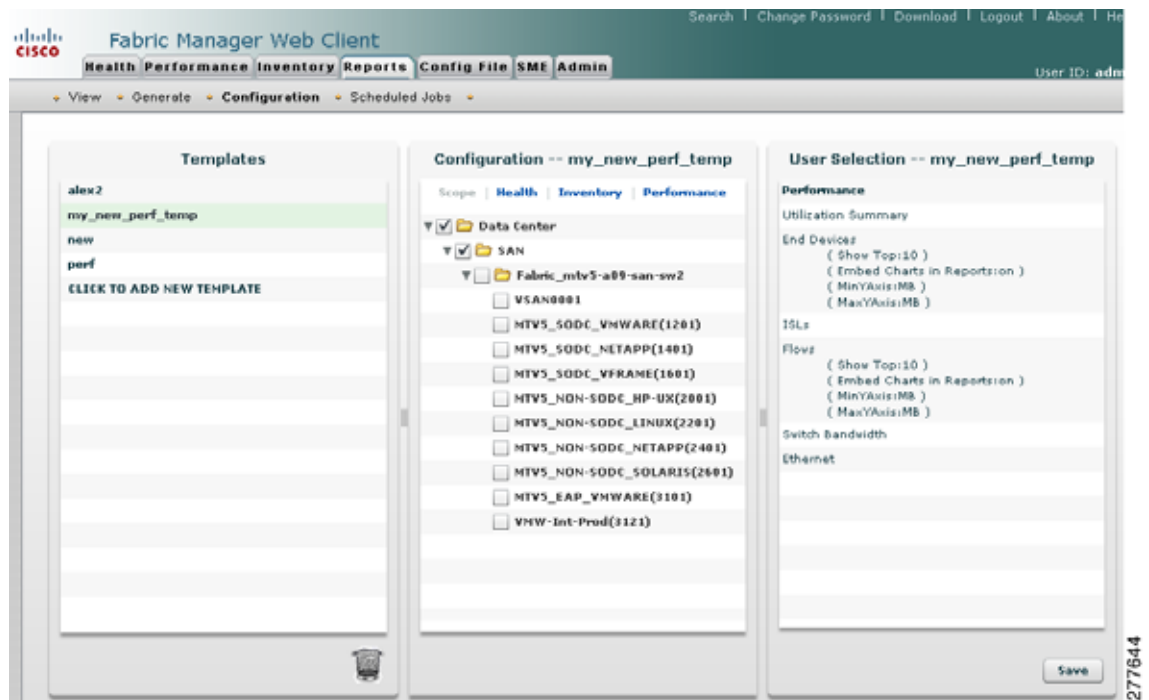
**Figure 7-31 Report Configuration Tab**



- Step 2** Click **CLICK TO ADD NEW TEMPLATE** in the Templates panel to create a new name for your report.
- Step 3** Click **Scope** in the configuration panel to define the scope.
- Step 4** Indicate the information you want in the report by navigating to each category such as **Health**, **Performance**, and **Inventory** in the Configuration panel.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-32 Configuration Panel**



- Step 5** (Optional) Select Severity for events, Status for inventory information, or Type of end devices for performance information and inventory information.
- Step 6** Click **Save** to save this report template.

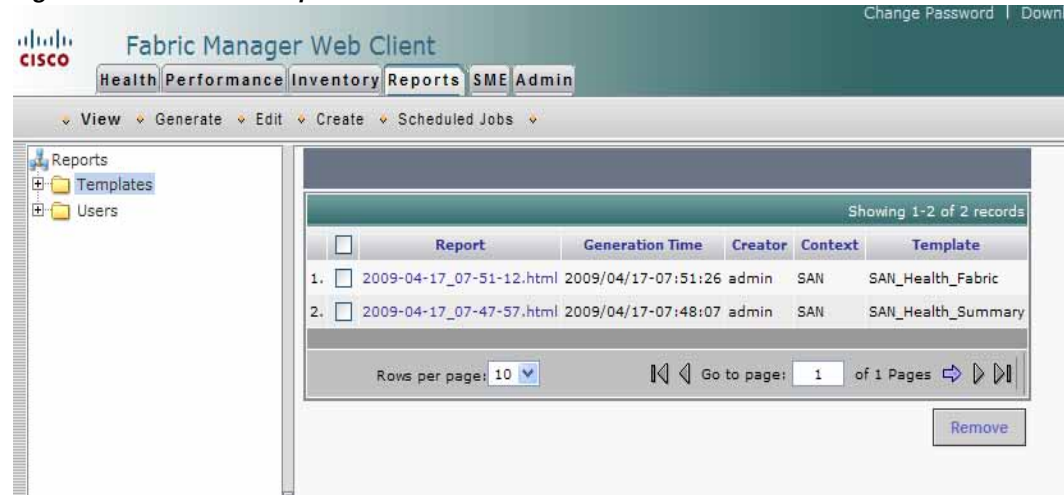
*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Viewing Custom Reports by Template

To view a custom report based on a specific template using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Reports** tab, and then click **View**.  
You see the Report table window as shown in [Figure 7-33](#).

**Figure 7-33 View Report Table**



- Step 2** In the left pane expand **Templates**.  
**Step 3** Select the report that you want to view. You can view the report in the main screen or you can view the report in a new browser window if you click the report in the report table.  
**Step 4** To delete a specific report, click the check box and then click **Remove**.  
**Step 5** To delete all the reports click the check box in the header and then click **Remove**.

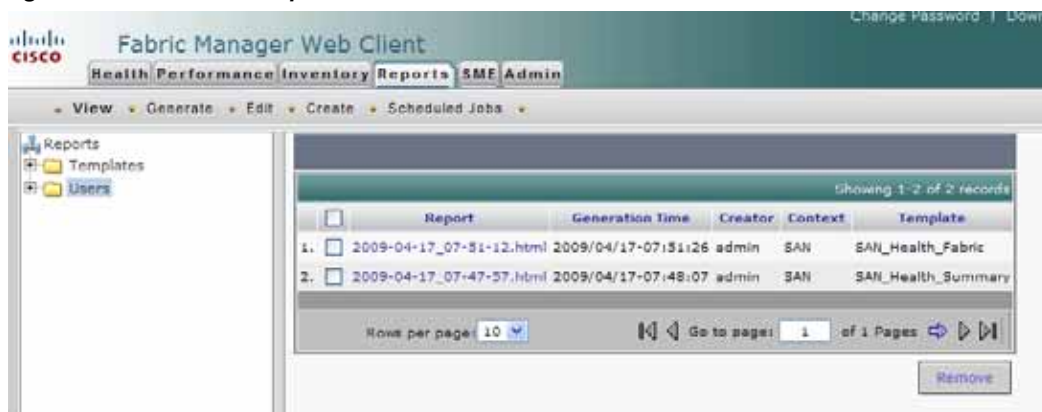
## Viewing Custom Reports by Users

To view a custom report based on a specific user using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Reports** tab, and then click **View**.  
You see the report table window as shown in [Figure 7-34](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-34 View Report Table**



- Step 2** In the left pane, click to expand **Users**.
- Step 3** Double-click the user name.
- Step 4** Select the report that you want to view. You can view the report in the main screen or you can view the report in a new browser window if you click the report in the report table.
- Step 5** To delete a specific report, click the check box and then click **Remove**.
- Step 6** To delete all reports click the check box in the header and then click **Remove**.

## Delete a Report Template

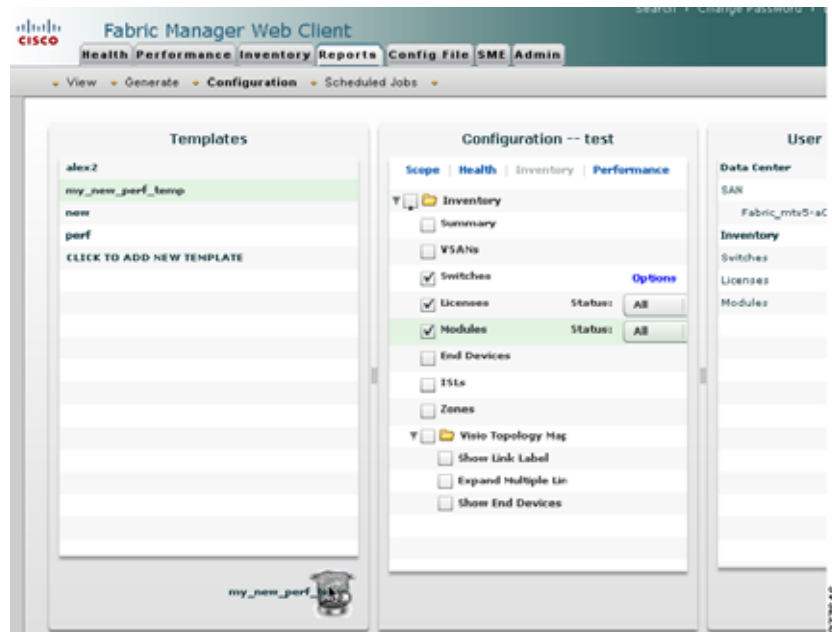
To delete a custom report using Fabric Manager Web Client, follow these steps:

- Step 1** In the Template panel, click to select the report template you want to delete.



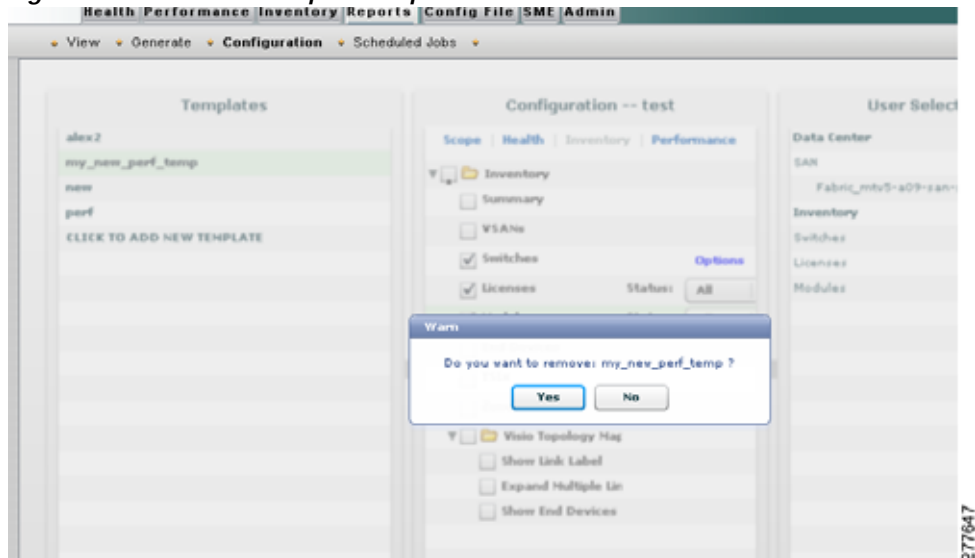
*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-35 Delete Report Template**



**Step 2** Drag the selected report template to the trash at the right-bottom corner of the Template panel.

**Figure 7-36 Delete Report Template Confirm**



**Step 3** Click **Yes** to delete the template.

## Generating Custom Reports by Template

You can generate reports based on a selected template or you can schedule the report to run at a specified time.

To generate a report or to schedule a report using Fabric Manager Web Client, follow these steps:

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 1** Select a SAN, fabric, or VSAN on which to base the report.
- Step 2** Click the **Reports** tab, and then click **Generate**.
- You see the Generate Custom Report tab window as shown in [Figure 7-37](#).

**Figure 7-37** Generate Custom Report Tab



- Step 3** Choose a report template from the Available drop-down list.
- Step 4** (Optional) Change the name of the report. By default, report names are based on the date and time generated.
- Step 5** (Optional) Uncheck the **Use Scope from Template** check box to override the scope defined by the filter type.
- Step 6** (Optional) Check the **Private** check box to change the attribute of the report. If selected, the report can be viewed only by the specific user and network administrator.
- Step 7** (Optional) Check the **Email Report** check box to receive an e-mail notification.
- Step 8** Click **Generate** to generate a report based on this template.
- You see the report results in a new browser window. Alternatively, you can view the report by clicking **Report > View** and selecting the report name from the report template you used in the navigation pane.
- Step 9** Click **Schedule** to schedule a report based on this template. You see the schedule panel.
- You see the Generate Custom Report tab window as shown in [Figure 7-38](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-38**      **Schedule Reports**

**Step 10** In the schedule panel, specify the scheduled run time and how often you want the report to run.

**Step 11** Click the calendar next to **Start Date** or **End Date** to modify the date settings.

**Step 12** Select the **Start Time** or **End Time** drop-down list to modify time settings.

**Step 13** Select the frequency at which you need the report to be generated.

**Step 14** Enter a name for the report in the Job Name field and click **Create Job** to save the report.

You can view the scheduled jobs on the Scheduled Jobs page but once the scheduled jobs have started running, they are removed from the Scheduled Job table.



**Note** The **End Date** must be at least five minutes earlier than the **Start Date**.

## Modifying a Custom Report Template

To edit a custom report template using Fabric Manager Web Client, follow these steps:

**Step 1** Click the **Reports** tab, and then click **Configuration**.

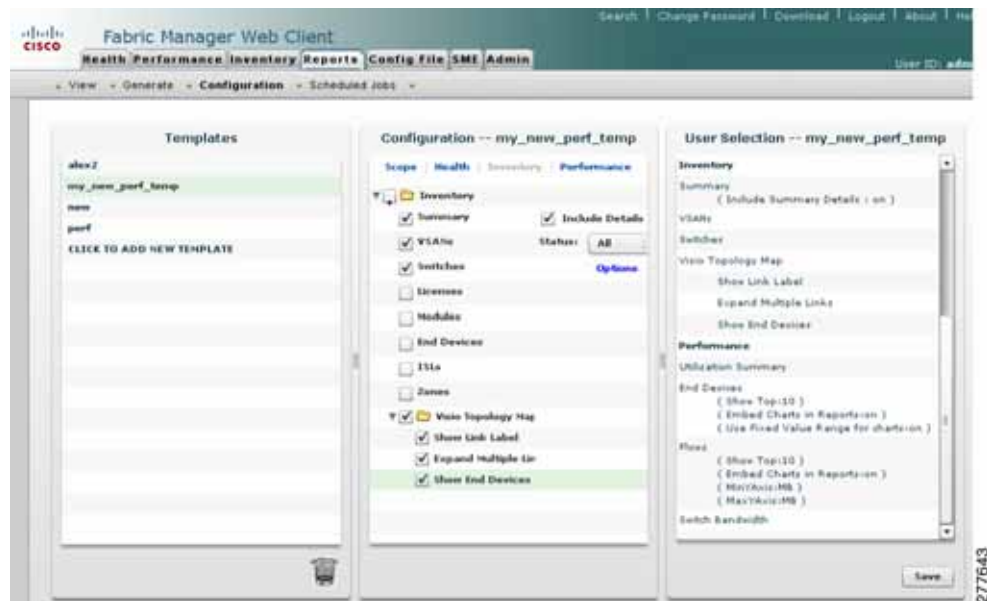
You see the Templates, Configuration and User Selection panels.

**Step 2** Double-click to select a report from the template panel.

You see the current information about this report in the Configuration panel as shown in [Figure 7-39](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-39 Report**



- Step 3** Indicate the information you want to gather in the report by clicking the **Health**, **Performance**, and **Inventory** tabs in the configuration panel.
- Step 4** (Optional) Select a severity level for events, status for inventory information, or type of end device for performance information and inventory information.
- Step 5** Click **Save** to save this report template.



**Note** You cannot change the SAN, fabrics or VSAN the report is based on. Generate a new report for a new SAN, fabrics or VSAN.

## Deleting Custom Reports

Reports you generate are saved by Fabric Manager Server. To delete a custom report, you need to first select the report you want to delete. To delete a custom report based on a specific user using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Reports** tab, and then click **View**.
- Step 2** In the left pane, expand **Users**.
- Step 3** Double-click the user name.
- Step 4** In the right pane, select the report that you want to delete and then click **Remove**.

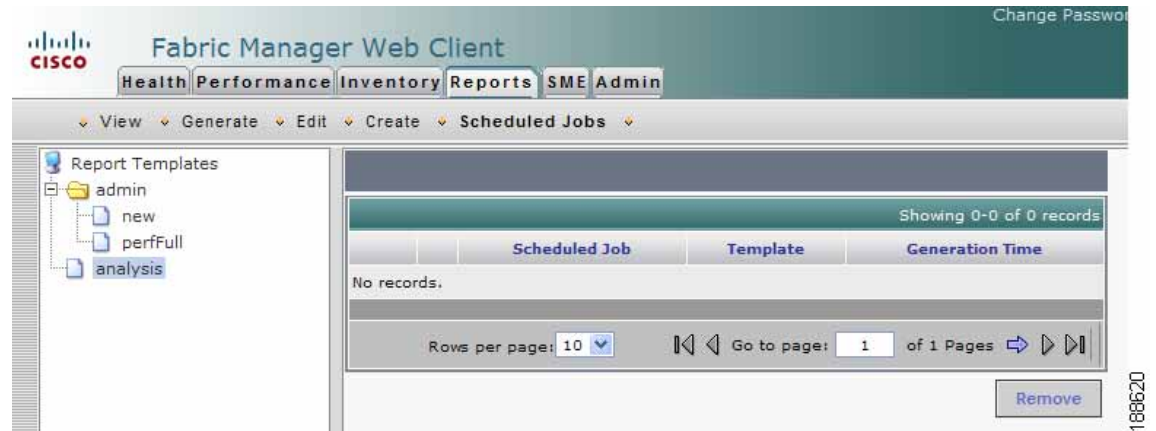
*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Viewing Scheduled Jobs by Report Template

To view scheduled jobs by report template using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Reports** tab, and then click **Scheduled Jobs**.  
You see the Scheduled Jobs table window as shown in [Figure 7-40](#).

**Figure 7-40** Scheduled Jobs Table



- Step 2** Click a report template in the left navigation pane to view the scheduled jobs based on the selected template.

## Modifying Scheduled Jobs

To modify scheduled jobs using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Reports** tab, and then click **Scheduled Jobs**.  
**Step 2** In the right pane, click **View**.  
You see the modify options in the Scheduled Jobs table as shown in [Figure 7-41](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-41**      *Modify Scheduled Jobs*

The screenshot displays the 'Fabric Manager Web Client' interface. At the top, there are tabs for Health, Performance, Inventory, Reports, SME, and Admin. The 'Admin' tab is selected. Below the tabs, there are buttons for View, Generate, Edit, Create, and Scheduled Jobs. The 'Scheduled Jobs' button is highlighted. On the left, a 'Report Templates' sidebar shows a tree structure with 'admin' selected, containing 'new', 'perfFull', and 'analysis'. The main content area is titled 'Modify Scheduled Jobs'. It includes fields for 'Start Date' (2008-Aug-04), 'Start Time' (11:59:55 PM), 'Run' frequency (radio buttons for Once, Daily, Weekly, Every 5 minutes; 'Once' is selected), 'Job Name' (admin.perfFull), and an 'Email Notification' checkbox. Below these fields are 'Edit Job' and 'Cancel' buttons. A table below shows a list of scheduled jobs with columns 'Scheduled Job', 'Template', and 'Generation Time'. It contains one record: '1. admin.perfFull view admin.perfFull 2008/08/04-07:15:33'. At the bottom of the table are 'Rows per page: 10' and 'Go to page: 1 of 1 Pages'. A 'Remove' button is located at the bottom right of the table.

- Step 3** Click the calendar next to Start Date to modify the date settings.
- Step 4** Select the Start Time drop-down list to modify time settings.
- Step 5** Click to select the appropriate radio button to change the frequency of generating report.
- Step 6** (Optional) Check the **Email Notification** check box to get the report by e-mail.
- Step 7** Click **Edit Job** to save changes.

## Admin



### Note

Only network administrators can access the Fabric Manager Web Client Admin tab. Network operators cannot view the Admin tab.

The Admin tab allows you to perform minor administrative and configuration tasks on the Fabric Manager Server sending data to your web client.

The Admin tab contains the following subtabs:

- **Status**—Displays the status of the Database Server, and allows you to start and stop Performance Collector services on your server. You should restart services only if something is not working properly, or if too large a percentage of system resources are being consumed.



### Note

You cannot start or stop the Database Server services using Fabric Manager WebClient. If you are using Microsoft Windows operating system, you need to use Microsoft Management Console to stop, start, or restart the Database Server.

- **Configure**—Allows you to configure various parameters for Fabric Manager Server.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- **Logs**—Allows you to view all the logs from the various services running on the Fabric Manager Server.



**Note**

If you see a database file lock error in the database log, you can fix it by shutting down and restarting the database server using the web client.

## Recovering a Web Server Password

Fabric Manager Web Client user passwords are encrypted and stored locally on the workstation where you installed Web Server. If you forget a password, you can create a new network-admin user locally on the workstation where you installed Web Server and then log in and delete the old user account under the Admin tab.

To create a user on the workstation where you installed Web Server and delete the old user, follow these steps:

- 
- Step 1** Go to the Web Server installation directory and enter the **cd** command to access the bin directory.
- Step 2** Enter the following line to create a user:
- ```
addUser. {sh,bat} <userName> <dbpassword>
```
- Step 3** Choose **Admin > Configure > Web Users > Local Database**.
- You see the list of users in the local database.
- Step 4** Select the user that you want to delete and click **Delete** to remove the old user.
- 

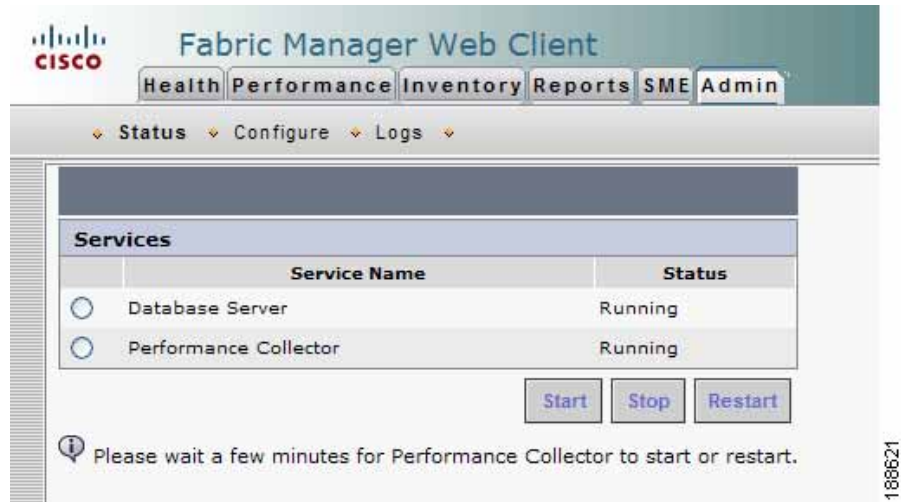
## Starting, Restarting, and Stopping Services

To start, restart, or stop services using Fabric Manager Web Client, follow these steps:

- 
- Step 1** Click the **Admin** tab, and then click **Status**.
- You see a table of services and the status of each as shown in [Figure 7-42](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-42 Fabric Manager Services Status**



**Step 2** Select the services you want to start, restart, or stop.

**Step 3** Click **Start** or **Stop**, or **Restart**.

The selected services are started, restarted, or stopped.



**Note** If the word “more” is in the Status column, you can click it to view a detailed status of the service.



**Note** You need to configure Performance collection in order to start, stop or restart Performance Collector.

## Adding, Editing, and Removing Managed Fabrics

Fabric Manager Web Client reports information gathered by the Fabric Manager Server on any fabric known to the Fabric Manager Server.

To start managing a fabric from the Fabric Manager Server using Fabric Manager Web Client, follow these steps:

**Step 1** Click the **Admin** tab, and then click **Configure**.

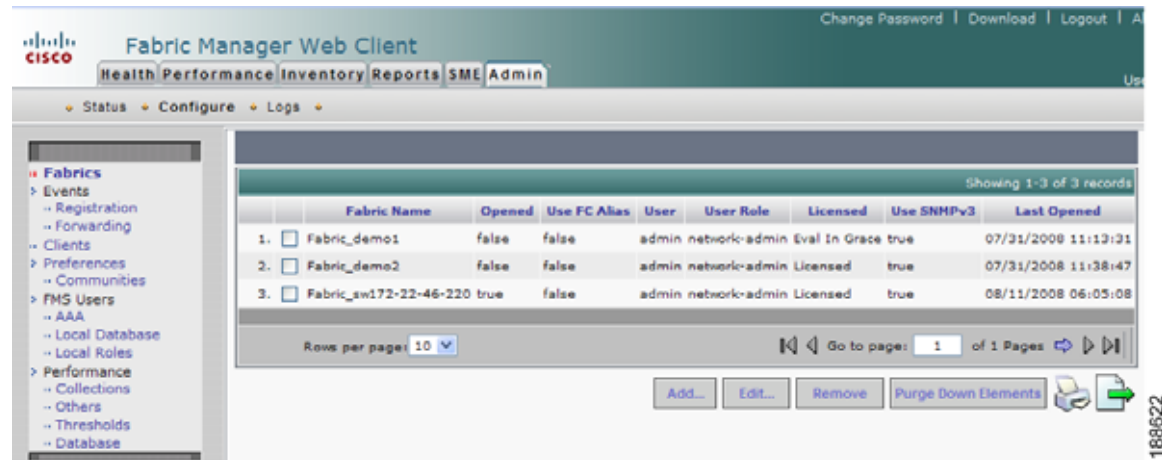
**Step 2** Click **Fabrics** in the left navigation pane.

You see the list of fabrics (if any) managed by Fabric Manager Server in the Opened column as shown in [Figure 7-43](#).



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-43** List of Fabrics Managed by the Fabric Manager Server



**Step 3** Click **Add**.

You see the Add Fabric dialog box as shown in Figure 7-44.

**Figure 7-44** Add Fabric Dialog Box



- Step 4** Enter the seed switch IP address, read community and write community for this fabric.
- Step 5** Enter the user name and password for this fabric.
- Step 6** (Optional) Check the SNMPV3 check box. If you check SNMPV3, the fields Read Community and Write Community change to User Name and Password. You must enter your user name and password.
- Step 7** Select the privacy settings from the **Auth-Privacy** listbox.
- Step 8** Click **Add** to begin managing this fabric.
- Step 9** Select the IP address of the server from the **Server** listbox.

To stop managing a fabric from Fabric Manager Server using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Admin** tab, and then click **Configure**.
- Step 2** Click **Fabrics** in the left navigation pane.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

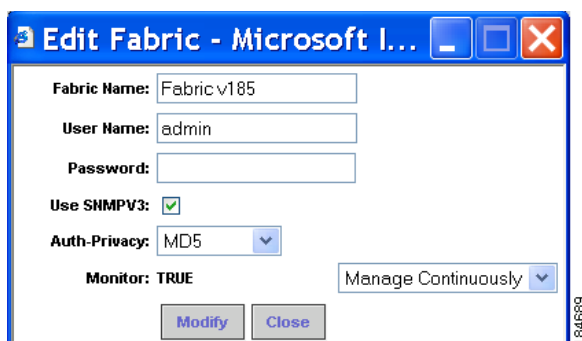
- Step 3** Check the check box next to the fabric that you want to remove and click **Remove** to discontinue data collection for that fabric.
- 

To edit a fabric from Fabric Manager Server using Fabric Manager Web Client, follow these steps:

---

- Step 1** Click the **Admin** tab, and then click **Configure**.
- Step 2** Click **Fabrics** in the left navigation pane.
- Step 3** Check the check box next to the fabric that you want to edit and click **Edit**.  
You see the Edit Fabric dialog box as shown in [Figure 7-45](#).

**Figure 7-45** Edit Fabric Dialog Box



- Step 4** Enter a new fabric name, user name and password and specify how you want Fabric Manager Server to manage the fabric by selecting an option from the drop-down list.
- Step 5** Click **Modify** to save the changes.
- 

## Viewing Trap and Syslog Registration Information

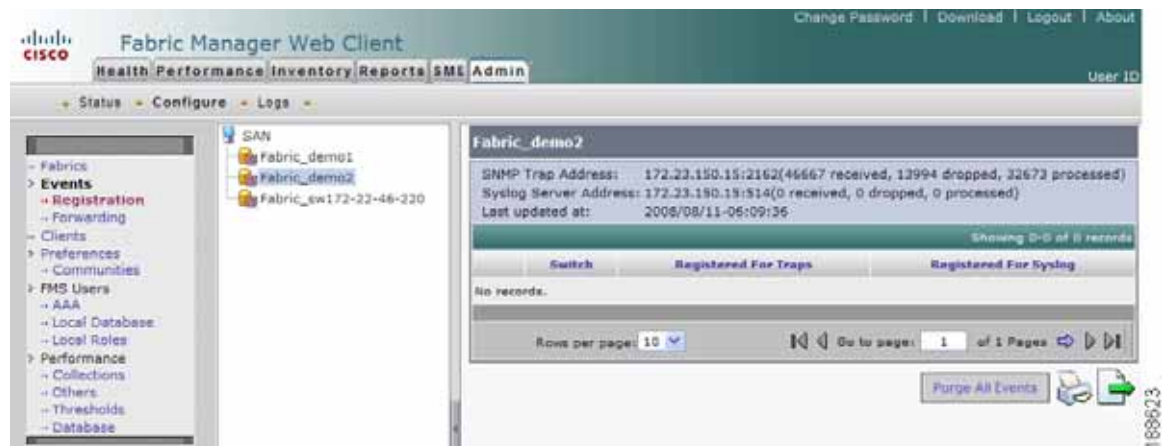
To view trap and syslog registration information from Fabric Manager Server using Fabric Manager Web Client, follow these steps:

---

- Step 1** Click the **Admin** tab, and then click **Configure**.
- Step 2** Click **Registration** in the left navigation pane.
- Step 3** Select a fabric to display registration information for that fabric.  
You see the Registration screen showing the registration information for the selected fabric as shown in [Figure 7-46](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-46 Registration Screen**



**Step 4** (Optional) Click the **Print** icon or the **Export Report** icon for a copy of the information.

## Configuring Forwarding of Notifications for Events

You can use Fabric Manager Web Client to add and remove notification forwards for system messages.



**Note**

Fabric Manager Web Client forwards fabric events via e-mail or SNMPv1 traps.

To add a notification forward using Fabric Manager Web Client, follow these steps:

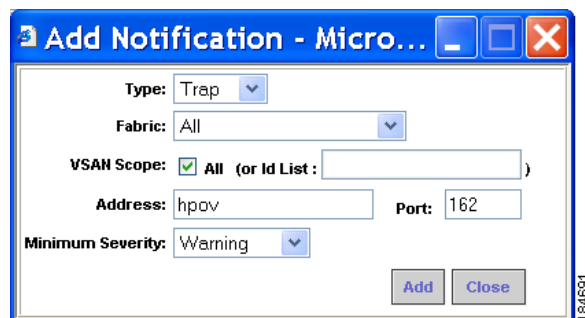
**Step 1** Click the **Admin** tab, and then click **Configure**.

**Step 2** Click **Forwarding** in the left navigation pane.

**Step 3** Click **Add**.

You see the Add Notification dialog box as shown in [Figure 7-47](#).

**Figure 7-47 Add Notification Dialog Box**



**Step 4** In the Type field, either choose E-Mail or SNMP Trap. If you choose Trap, a Port field is added to the dialog box.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 5** From the Fabric drop-down list, choose the fabric for notification.
- Step 6** Either check the **VSAN Scope** check box to receive notifications for all VSANs, or enter the VSAN IDs in the ID List field to limit the VSANs for which you want to receive notifications.
- Step 7** Enter the e-mail address for notifications in the Address field.
- Step 8** From the Minimum Severity drop-down list, select the severity level of the messages to receive.
- Step 9** Click **Add** to add the notification.



**Note**

The traps sent by Fabric Manager Server correspond to the severity type followed by a text description:

```
trap type(s) = 40990 (emergency) 40991 (alert) 40992 (critical) 40993 (error) 40994
(warning) 40995 (notice) 40996 (info) 40997 (debug)textDescriptionId = 1, 3, 6, 1, 4, 1,
9, 9, 40999, 1, 1, 3, 0
```

To remove a notification forward using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Admin** tab, and then click **Configure**.
- Step 2** Click **Forwarding** in the left navigation pane.
- Step 3** Check the check box in front of the notification that you want to remove.
- Step 4** Click **Remove**.

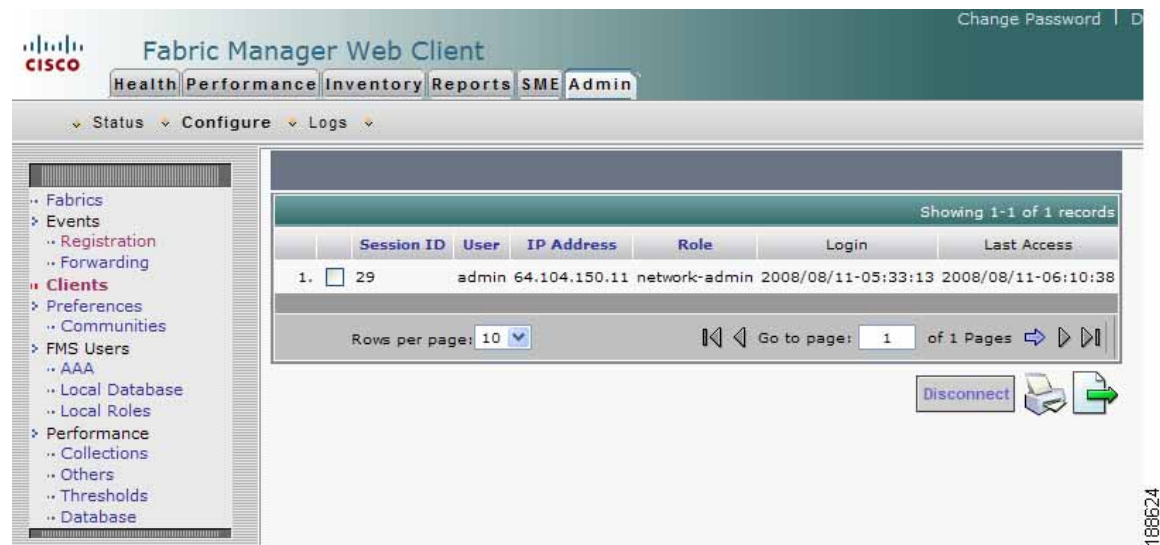
## Viewing and Disconnecting Clients

To view or disconnect clients from the Fabric Manager Server using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Admin** tab, and then click **Configure**.
  - Step 2** Click **Clients** in the left navigation pane.
- You see the Clients page as shown in [Figure 7-48](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-48** List of Clients



- Step 3** Check the check box next to the client you want to disconnect.
- Step 4** Click **Disconnect**.

## Configuring Fabric Manager Server Preferences

To configure Fabric Manager Server preferences, click the **Admin** tab, click **Configure** and then click **Preferences** in the left navigation pane. Follow the on-screen instructions.

## Adding and Removing Communities

You can use Fabric Manager Web Client to add and remove communities.

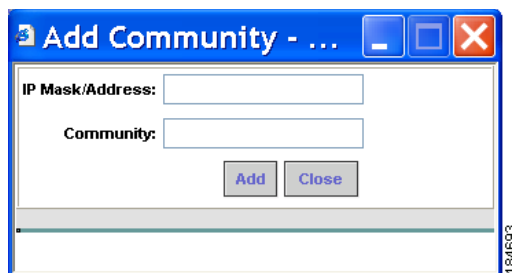
To add a community fabric using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Admin** tab, and then click **Configure**.
- Step 2** Click **Communities** in the left navigation pane.
- Step 3** Click **Add**.

You see the Add Community dialog box shown in [Figure 7-49](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-49 Add Community Dialog Box**



The dialog box is titled "Add Community - ...". It contains two input fields: "IP Mask/Address:" and "Community:". Below these fields are two buttons: "Add" and "Close".

- Step 4** Enter the IP mask or address of the community in the **IP Mask/Address** field.



**Note** The IP mask can contain wildcards (0s) you can use to assign communities to subnets.

- Step 5** Enter the name of the community in the Community field.

- Step 6** Click **Add** to add the community.

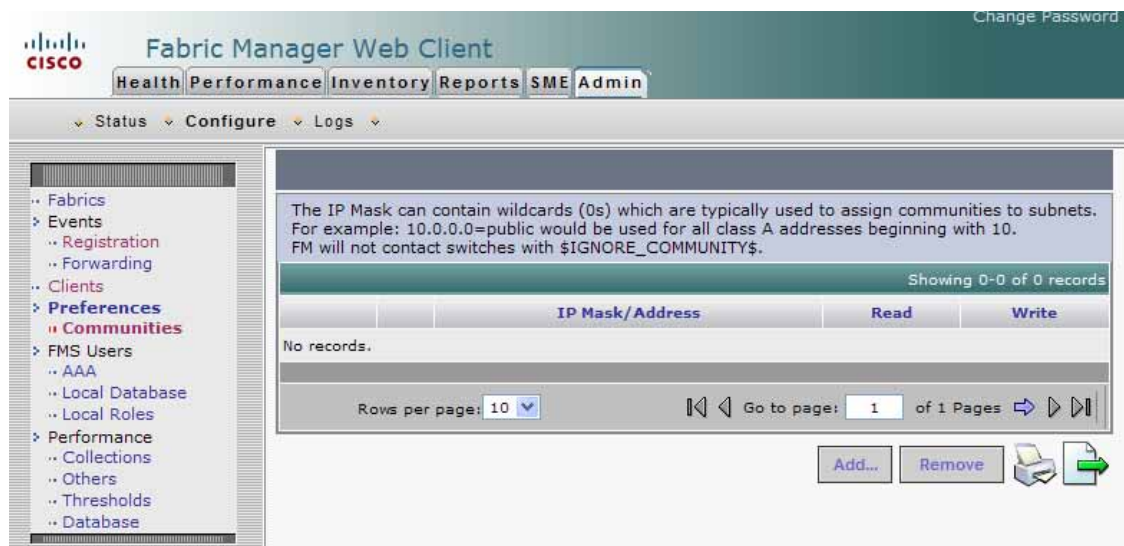
To remove a community using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Admin** tab, and then click **Configure**.

- Step 2** Click **Communities** in the left navigation pane.

You see the Communities page shown in [Figure 7-50](#).

**Figure 7-50 Communities Page**



The screenshot shows the Fabric Manager Web Client interface. The top navigation bar includes tabs for Health, Performance, Inventory, Reports, SME, and Admin. The left navigation pane shows a tree structure with categories like Fabrics, Events, Registration, Forwarding, Clients, Preferences, and Communities. The Communities page displays a message: "The IP Mask can contain wildcards (0s) which are typically used to assign communities to subnets. For example: 10.0.0.0=public would be used for all class A addresses beginning with 10. FM will not contact switches with \$IGNORE\_COMMUNITY\$." Below this message is a table with columns: IP Mask/Address, Read, and Write. The table shows "Showing 0-0 of 0 records" and "No records." At the bottom, there are buttons for "Add...", "Remove", and a "Go to page" dropdown set to "1" of 1 Pages.

- Step 3** Check the check box next to the community that you want to remove and click **Remove**.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*



**Note**

Cisco Fabric Manager 3.0(1) does not require you to make changes to the communities.properties file even if you are using a Cisco MDS 9020 switch or any third-party devices.

## Configuring AAA Information

To configure Fabric Manager Server preferences, click the **Admin** tab, click **Configure**, and then in the left pane, select **FMS Users** and **AAA** and follow the instructions on the screen.

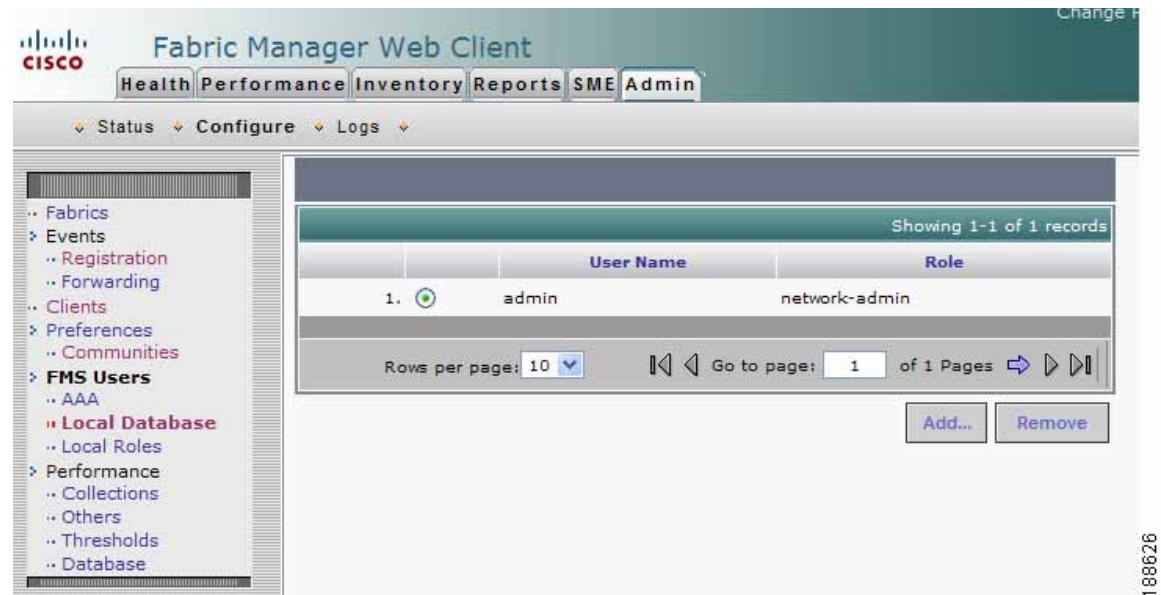
## Adding and Removing Users

You can use Fabric Manager Web Client to add and remove Web Server users.

To add a user using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Admin** tab, and then click **Configure**.
- Step 2** Select **Local Database** in the left navigation pane.  
You see the Local Database page as shown in [Figure 7-51](#).

**Figure 7-51** Local Database Page



- Step 3** Click **Add**.  
You see the **Add User** dialog box as shown in [Figure 7-52](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-52 Add User Dialog Box**

**Step 4** Enter the user name in the User Name field.



**Note** The user name **guest** is a reserved name (case insensitive). The guest user can only view reports. The guest user cannot change the guest password, nor can the guest user access the Admin tab in Fabric Manager Web Client.

**Step 5** Select a role for the user from the Role drop-down list.

**Step 6** Enter the password in the Password field.

**Step 7** Enter the password again in the Confirm Password field.

**Step 8** Click **Add** to add the user to the database.

**Step 9** Repeat Steps 3 through 7 to continue adding users.

To remove a user using Fabric Manager Web Client, follow these steps:

**Step 1** Click the **Admin** tab, and then click **Configure**.

**Step 2** Select **Local Database** in the left navigation pane.

**Step 3** Click the radio button next to the user that you want to remove and click **Remove**.

## Adding and Removing Roles

You can use Fabric Manager Web Client to add and remove Web Server roles.

To add a role using Fabric Manager Web Client, follow these steps:

**Step 1** Click the **Admin** tab, and then click **Configure**.

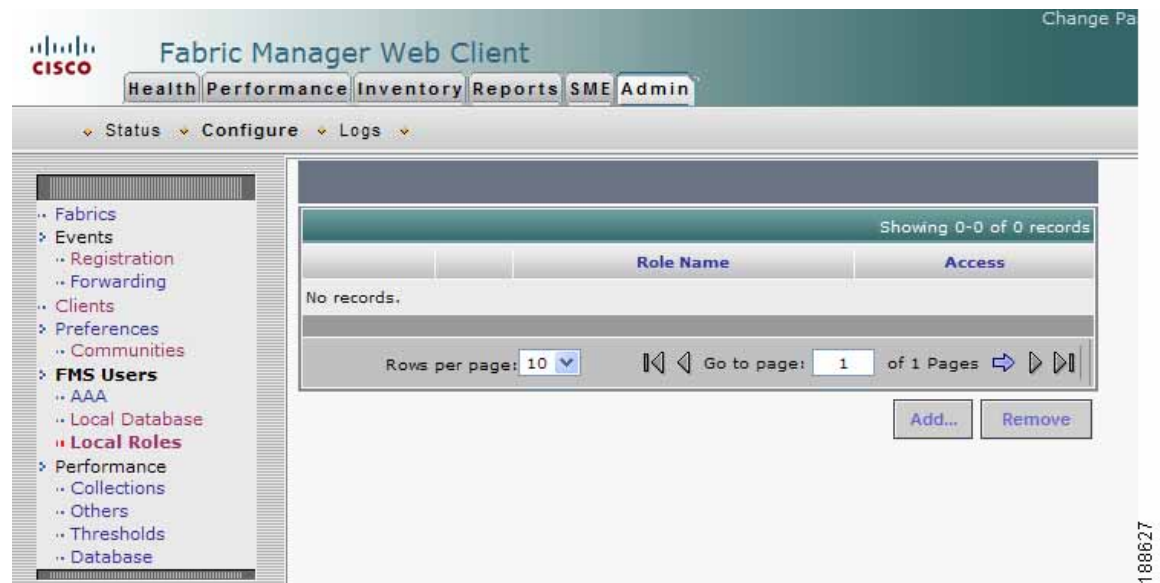
**Step 2** Click **Local Roles** in the left navigation pane.

You see the Local Roles page as shown in [Figure 7-53](#).



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

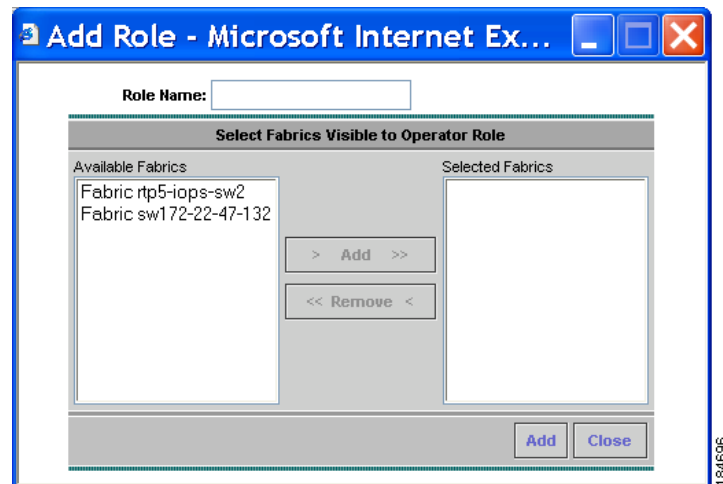
**Figure 7-53** Local Roles Page



**Step 3** Click **Add**.

You see the Add Role dialog box as shown in [Figure 7-54](#).

**Figure 7-54** Add Role Dialog Box



**Step 4** Enter the role name in the Role Name field.

**Step 5** Select fabrics that the role can access from the Available Fabrics column and add them to the Selected Fabrics column.

**Step 6** Click **Add** to add the role to the database.

**Step 7** Repeat Steps 3 through 5 to add additional roles.

To remove a role using Fabric Manager Web Client, follow these steps:

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- 
- Step 1** Click the **Admin** tab and then click **Configure**.
- Step 2** Select **Local Roles** in the left navigation pane.
- Step 3** Click the radio button next to the role you want to remove and click **Remove**.
- 

## Creating Performance Collections

If you are managing your fabrics with Performance Manager, you need to set up an initial set of flows and collections on the fabric. You can use Fabric Manager Web Client to add and remove performance collections. The fabric has to be licensed and in the Managed Continuously state before a collection for the fabric can be created.



### Note

You cannot manage performance collections for multiple devices through a single port interface. Since only one set of statistics exists per interface, Fabric Manager Web Client can manage performance collections for only one visible FL or iSCSI device through an interface.

To add a collection using Fabric Manager Web Client, follow these steps:

- 
- Step 1** Click the **Admin** tab, and then click **Configure**.
- Step 2** Click **Collections** in the left navigation pane.
- You see the Collections page as shown in [Figure 7-55](#).

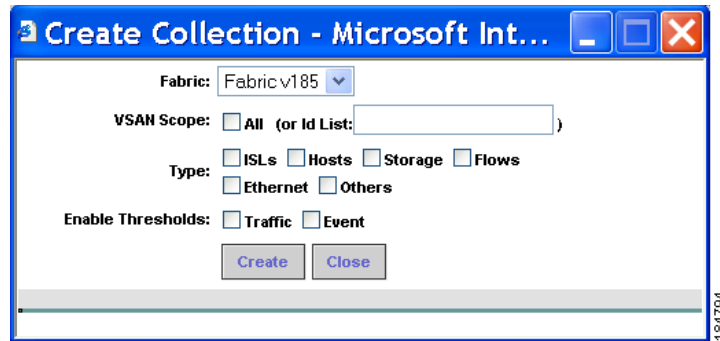
**Figure 7-55** Collections Page



- Step 3** Click **Add**.
- You see the Create Collection dialog box as shown in [Figure 7-56](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-56** Create Collection Dialog Box



- Step 4** Select a fabric for which to collect performance data from the Fabric drop-down list.
- Step 5** Either check the **VSAN Scope** check box to receive notifications for all VSANs, or enter the VSAN IDs in the **ID List** field to limit the VSANs for which you want to collect performance data.
- Step 6** Check the check boxes for the type(s) of entities for which you want to collect performance data.
- Step 7** Check the check boxes for the type(s) of thresholds you want to enable.
- Step 8** Click **Create** to add the collection and add it to the table.
- Step 9** Repeat Steps 3 through 8 to continue adding roles.



**Note**

Performance Manager shows statistics for fabrics that you have configured collections for using the Collection Wizard.

To remove a collection using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Admin** tab, and then click **Configure**.
- Step 2** Click **Collections** in the left navigation pane.
- Step 3** Check the check box next to the collection you want to remove and click **Remove**.

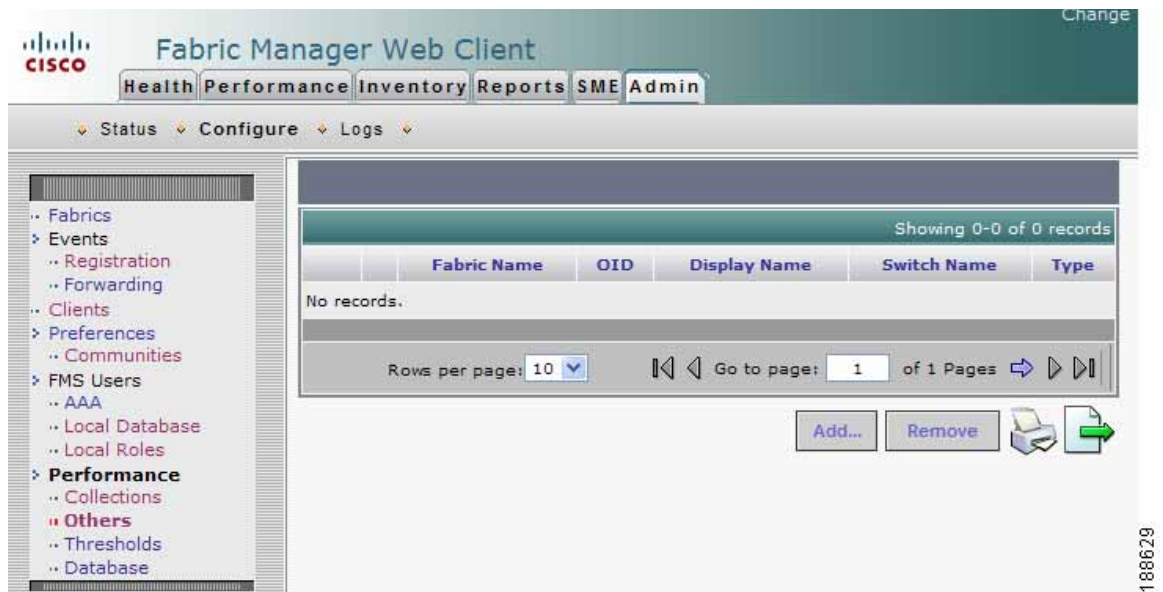
## Configuring Other Statistics

To configure other statistics using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Admin** tab, and then click **Configure**.
  - Step 2** Click **Others** in the left navigation pane.
- You see the Others page as shown in [Figure 7-57](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

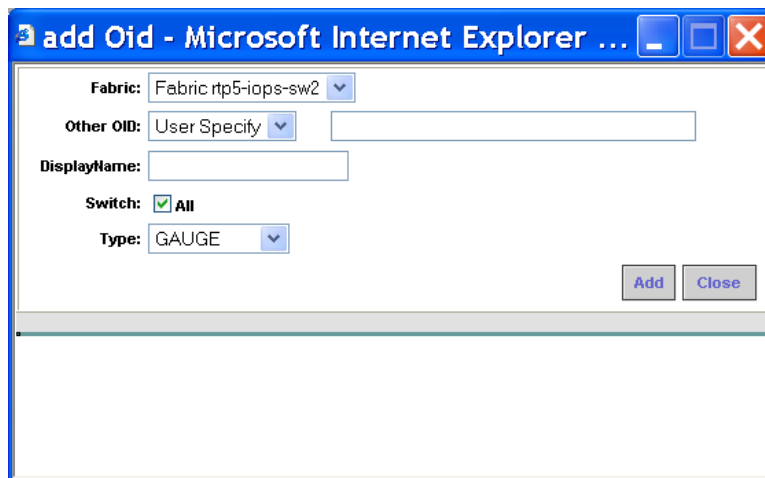
**Figure 7-57 Others Page**



**Step 3** Click **Add**.

You see the Add Oid dialog box as shown in [Figure 7-58](#).

**Figure 7-58 Add Oid Dialog Box**



**Step 4** Select a fabric for which you want to add other statistics.

**Step 5** Select the statistic that you want to add from the Other OID drop-down list and specify a name for the statistic in the Display Name field.

**Step 6** Click **Add** to add this statistic.

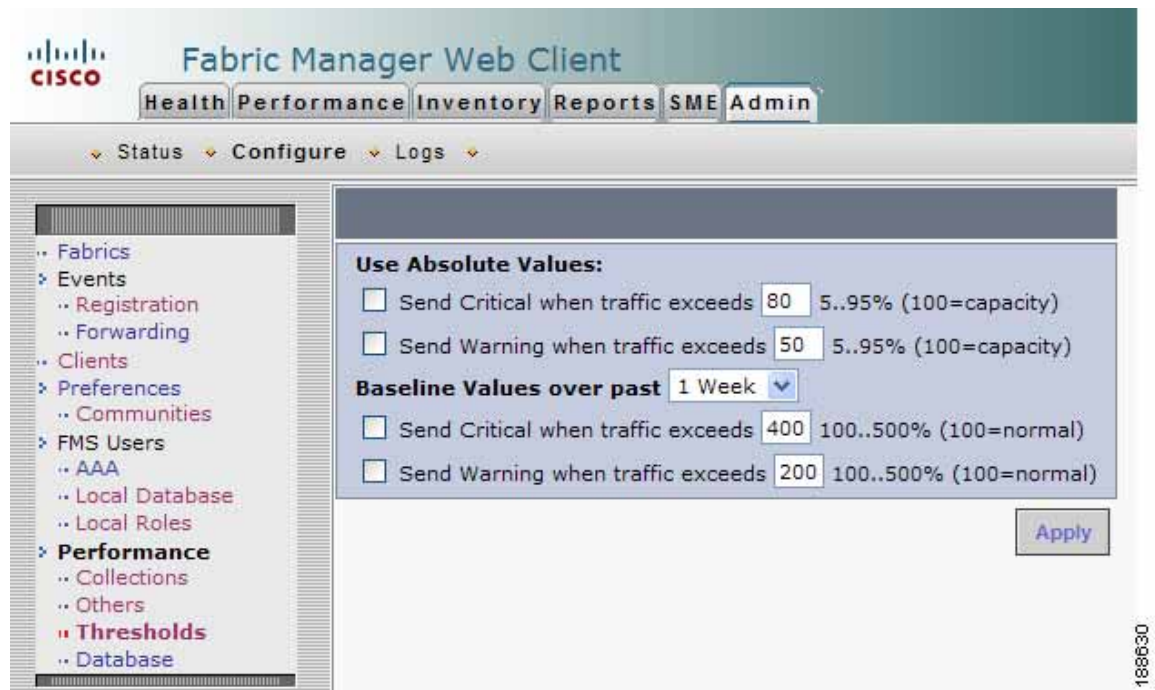
*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Configuring Collection Thresholds

To configure collection thresholds using Fabric Manager Web Client, follow these steps:

- Step 1** Click the **Admin** tab, and then click **Configure**.
- Step 2** Select **Thresholds** in the left navigation pane.
- You see the Thresholds page as shown in [Figure 7-59](#).

**Figure 7-59** Thresholds Page



- Step 3** If you are using absolute values, follow these steps, otherwise skip to Step 3.
- To configure conditions for sending Critical notifications, check the **Send Critical** check box. In the "...when traffic exceeds" field, enter a number (from 5 to 95) to indicate the percentage at which the Critical notification is sent. For example, entering **10** causes a notification to be sent when traffic at any given time exceeds 10% of capacity.
  - To configure conditions for sending Warning notifications, check the **Send Warning** check box. In the "...when traffic exceeds" field, enter a number (from 5 to 95) to indicate the percentage at which the Warning notification is sent. For example, entering **9** causes a notification to be sent when traffic at any given time exceeds 9% of capacity.
- Step 4** Select the time period for the collection (1 Week, 1 Month, or 1 Year) from the Baseline Values over past drop-down list. The baseline value represents the sum of the absolute values.
- To configure conditions for sending Critical notifications, check the **Send Critical** check box. In the "...when traffic exceeds" field, enter a number to indicate the percentage at which the Critical notification is sent. For example, entering **300** causes a notification to be sent when traffic for the selected period exceeds 300% of capacity.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- b. To configure conditions for sending Warning notifications, check the **Send Warning** check box. In the "...when traffic exceeds" field, enter a number to indicate the percentage at which the Warning notification is sent. For example, entering **150** causes a notification to be sent when traffic for the selected period exceeds 150% of capacity.

**Step 5** Click **Apply**.

---

## Importing the RRD Statistics Index

To manually import the RRD statistics index, follow these steps:

- 
- Step 1** Stop Fabric Manager Server.
  - Step 2** Copy the original RRD file into \$INSTALLDIR/pm/db.
  - Step 3** Run \$INSTALLDIR/bin/pm.bat s.
  - Step 4** Restart the Fabric Manager Server and add the fabric.
- 

## Configuring the RRD Database

Configuring the RRD database allows you to set the intervals at which data samples are collected. After applying the configuration, the database storage format is converted to a new format at those intervals. Since database formats are incompatible with each other, you must copy the old data (before the conversion) to the \$INSTALLDIR/pm directory. See "[Importing the RRD Statistics Index](#)" section on [page 7-65](#).

To configure the RRD database using Fabric Manager Web Client, follow these steps:

- 
- Step 1** Click the **Admin** tab, and then click **Configure**.
  - Step 2** Select **Database** in the left navigation pane.  
You see the Performance Database (collection interval) page as shown in [Figure 7-60](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-60** Performance Database Page

| Days   | Intervals |       | Samples |      |
|--------|-----------|-------|---------|------|
|        | Default   | ISLS  | Default | ISLS |
| 2.083  | 5 min     | 5 min | 600     | 600  |
| 14.583 | 30 min    |       | 700     |      |
| 64.583 | 2 hr      |       | 775     |      |
| 300.0  | 1 day     |       | 300     |      |

Disk Space per ISL/End Device: 115KB  
Total Disk Space in Use: 28.6MB

Apply Defaults

- Step 3** Enter the number of days to collect samples at 5-minute intervals in the top row of the Days column.
- Step 4** Enter the number of days to collect samples at 30-minute intervals in the second row of the Days column.
- Step 5** Enter the number of days to collect samples at 2-hour intervals in the third row of the Days column.
- Step 6** Enter the number of days to collect samples at 1-day intervals in the bottom row of the Days column.



**Note** As of Cisco SAN-OS Release 3.1(1) and later, you can configure the sampling interval for ISLS. Select a sampling interval from the ISLS drop-down list.

- Step 7** Click **Apply** to apply your changes, or click **Defaults** to reset the file sizes to the default values.
- If you are applying new values, or if the current values are not the default values, you see a message indicating that conversion of the RRD files will take a certain amount of time and that the database will be unavailable until then. The time it takes depends on the difference between the old and new values.



**Note** The system allows you to convert data, one process at a time. When you start converting the data, the Apply and Default buttons change to Refresh and Cancel so that another process cannot be inadvertently started. The display is the same for all browsers accessing the server during this time. Click **Refresh** to view the latest progress. Click **Cancel** to cancel the process of converting the data. If the job is successfully canceled, you see the Apply and Default buttons again. If the cancel job is not successful, you see a message indicating that the cancellation has failed.

If you want to perform this procedure, it is best to perform it before collecting a lot of data. Otherwise, converting the data can take a long time.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Viewing Log Information

You may occasionally want to view logs such as the Fabric Manager Server log. These processes have no corresponding GUI to allow you to view information about these log files. If you see errors, preserve these two files for viewing.

To view log information using Fabric Manager Web Client, follow these steps:

- 
- Step 1** Click the **Admin** tab, and then click **Logs**.  
You see a list of viewable logs in the left column.
- Step 2** Click a log file to view it.
- 

## Downloading Fabric Manager Client

You must use Fabric Manager Web Client to launch Fabric Manager Client. See the “[Launching Fabric Manager Client in Cisco SAN-OS Release 3.2\(1\) and Later](#)” section on page 5-2 for information on launching Fabric Manager Client.

To launch Fabric Manager Client, follow these steps:

- 
- Step 1** Choose **Admin > Download**.
- Step 2** Click the link for either **Fabric Manager** or **Device Manager**.  
If you are launching Fabric Manager Client for the first time, you see a message asking whether you want to create shortcuts for Fabric Manager.
- Step 3** Click **Yes** to create shortcuts for Fabric Manager.




---

**Note** This message only appears the first time you launch Fabric Manager Client.

---

## Fabric Manager Web Search Engine

The search engine helps you locate records that match a specific criteria. The search entity is divided into two categories: inventory and performance. In the inventory type, you can search by the switch (name of the switch, IP address of the switch and WWN), Endport (alias, IP address of the switch and WWN) and VSANs (name of the VSAN, IP address of the principle switch and WWN). In the performance type, you can search by end device (Endport alias, Endport WWN), Flow (name of the flow) and ISLs (name of the ISL and WWN of the ISL). You can also use wild card characters in the search.

## Using Fabric Manager Search Engine

To conduct a search, follow these steps:

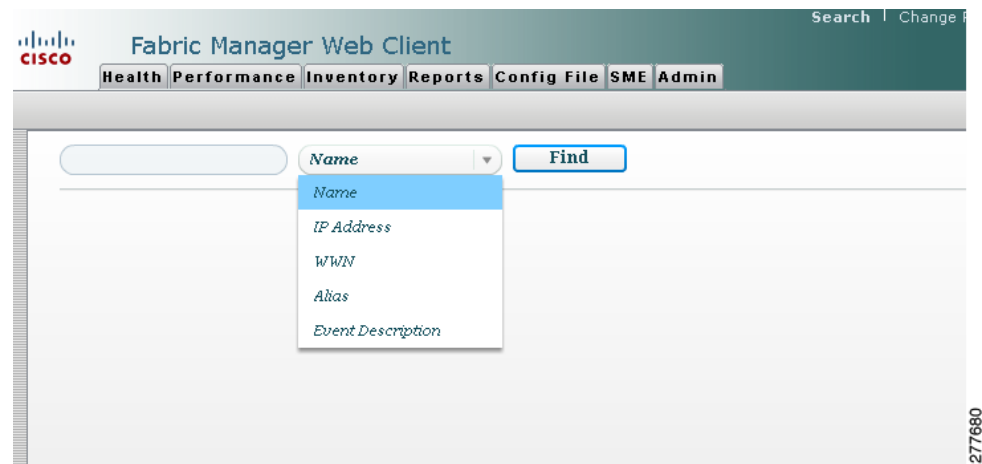
- 
- Step 1** Click **Search** on the top.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

You see the search page as shown in [Figure 7-61](#).

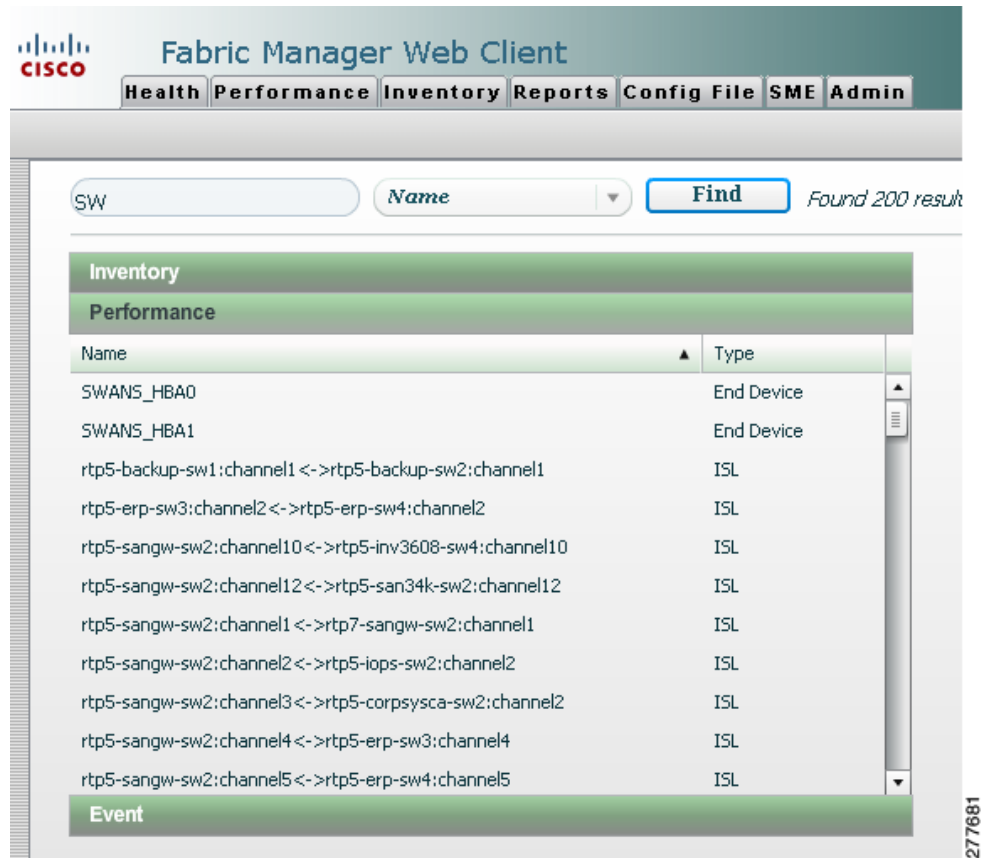
**Figure 7-61** Search Page



- Step 2** Enter the name to search in the text box.
- Step 3** Select the appropriate type from the combo box and then click **Find**.
- A window appears with your results as shown in [Figure 7-62](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-62 Search Results**

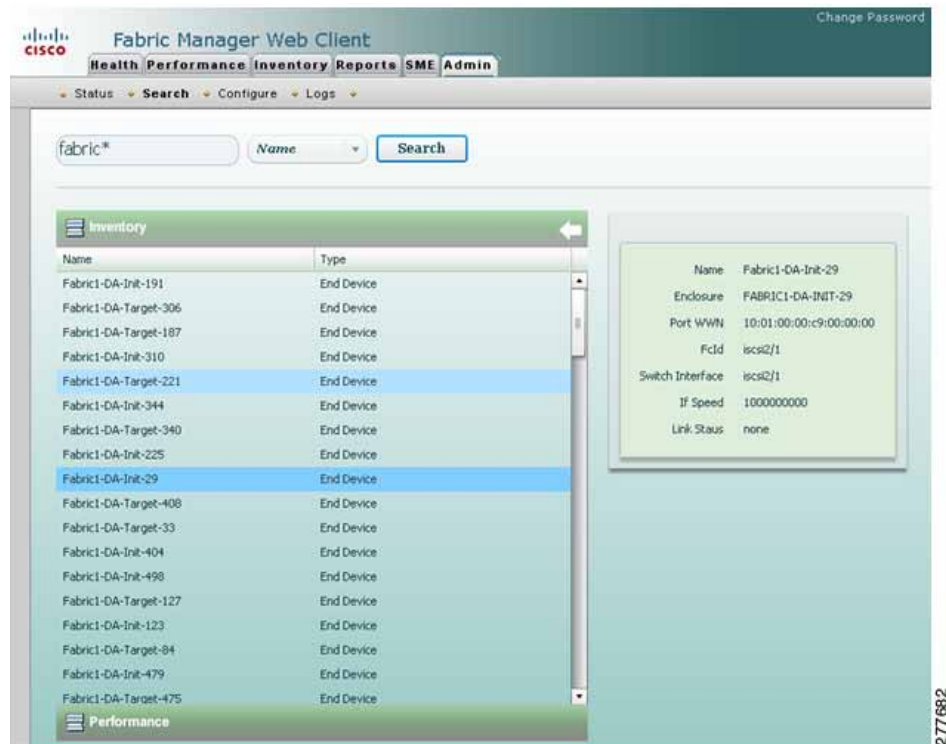


**Step 4** Click the entity type to see the details.

You see the details of the selected entity in the right pane as shown in [Figure 7-63](#).

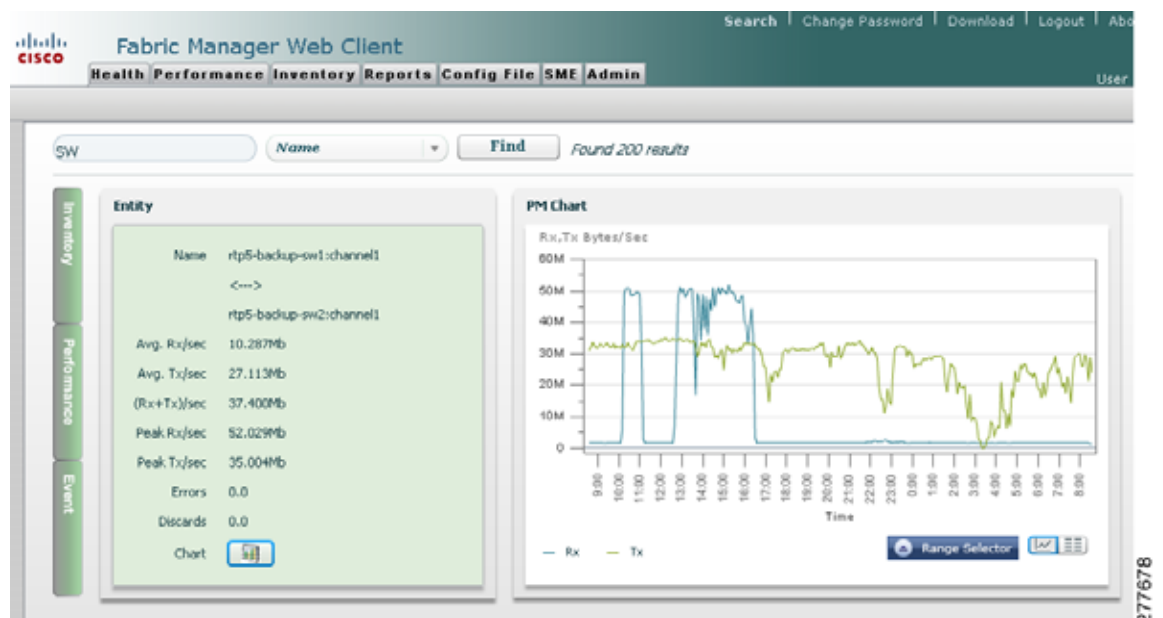
*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-63 Detailed Results**



- Step 5** Click the chart icon at the bottom of the right pane to view the graphical representation of the data. You see the graph as shown in Figure 7-64.

**Figure 7-64 Data in Chart**

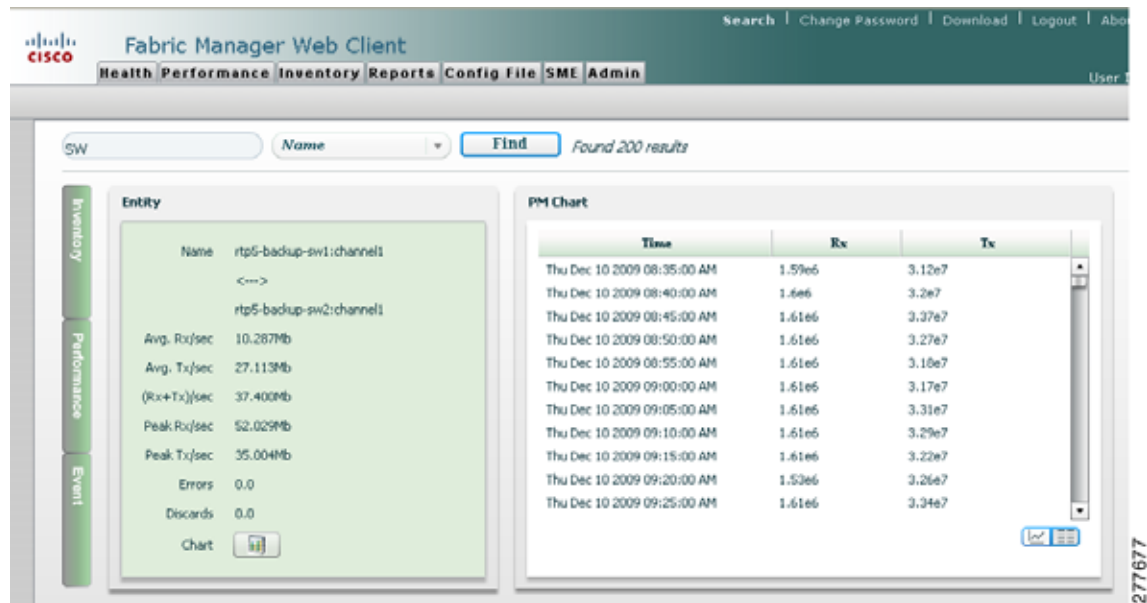


- Step 6** Click the grid icon in the right pane to View the data in grid format.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

You see the data in grid format as shown in [Figure 7-65](#).

**Figure 7-65 Data in Grid**



**Step 7** Click **Range Selector** to analyze performance data in a specific range.

**Step 8** You see the range selector as shown in [Figure 7-66](#).

**Figure 7-66 Range Selector**



**Step 9** Use the sliders to select a specific range.

**Step 10** Click the **Range Selector** again to turn off the range selector.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Configuring Backups Using Fabric Manager WebClient

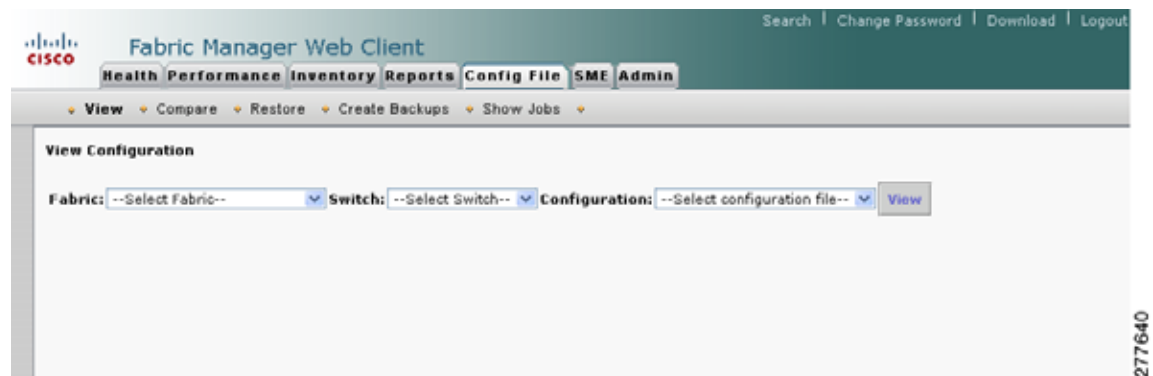
Using Fabric Manager WebClient, you can periodically backup startup and running configurations of the switch. You can also view backed-up configurations, schedule configuration backups, compare two backed-up configurations, and restore a configuration onto a switch.

### Viewing a Configuration

To view a configuration, follow these steps:

- 
- Step 1** Click the **Config File** tab and then click **View**.  
You see the configuration information as shown in [Figure 7-67](#).

**Figure 7-67** Viewing Configuration



- Step 2** Select a fabric name from the Fabric drop-down list.
- Step 3** Select a switch from the Switch drop-down list.
- Step 4** Select a configuration file name from the Configuration file drop-down list.
- Step 5** Click **View**.
- 

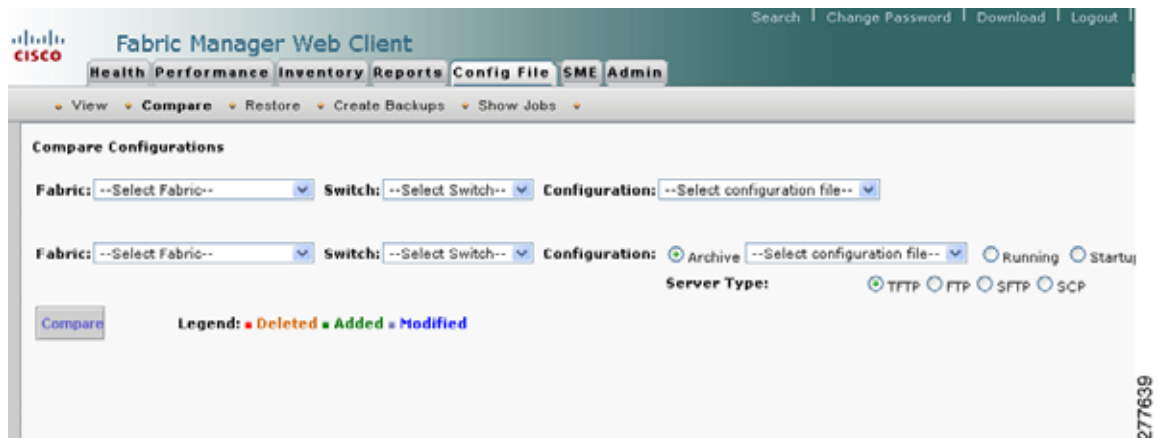
### Comparing Configurations

To compare configurations, follow these steps:

- 
- Step 1** Click the **Config File** tab, and then click **Compare**.  
You see the compare configuration information as shown in [Figure 7-68](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 7-68** Compare Configurations



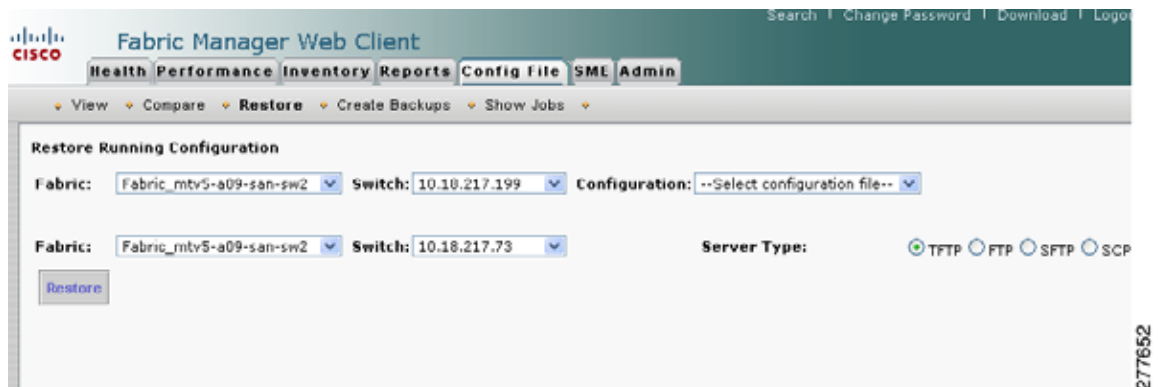
- Step 2 Select a fabric name from the Fabric drop-down list.
- Step 3 Select a switch from the Switch drop-down list.
- Step 4 Select a configuration file name from the Configuration file drop-down list.
- Step 5 Select a fabric name from the Fabric drop-down list in the second row.
- Step 6 Select a switch from the Switch drop-down list in the second row.
- Step 7 Click to select a configuration type (Archive, Running, Startup).
- Step 8 Click to select a Server Type (TFTP, FTP, SFTP, SFP).
- Step 9 Click **Compare**.

## Restoring Configurations

To restore a configuration on a switch, follow these steps:

- Step 1 Click the **Config File** tab, and then click **Restore**.  
You see the compare configuration information as shown in [Figure 7-69](#).

**Figure 7-69** Restore Configurations



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 2** Select a fabric name from the Fabric drop-down list.
- Step 3** Select a switch from the Switch drop-down list.
- Step 4** Select a configuration file name from the Configuration file drop-down list.
- Step 5** Select a fabric name from the Fabric drop-down list in the second row.
- Step 6** Select a switch from the Switch drop-down list in the second row.
- Step 7** Click to select a Server Type (TFTP, FTP, SFTP, SFP).
- Step 8** Click **Restore**.

## Creating Backups

To create a backup of the configuration, follow these steps:

- Step 1** Click **Config File** tab and then click **Create Backups**.  
You see the backup configuration page as shown in [Figure 7-70](#).

**Figure 7-70** Creating Backups

- Step 2** Select a fabric name from the Fabric drop-down list.
- Step 3** Click to select a configuration type (Archive, Running, Startup).
- Step 4** Click to select a Server Type (TFTP, FTP, SFTP, SFP).
- Step 5** Click the calendar icon to select a start date.
- Step 6** Enter the start time.
- Step 7** Click to select the frequency (Once, Daily, Weekly, Monthly) at which you want to perform backup.
- Step 8** Enter a name to identify this backup task.
- Step 9** Click **Create Job** to save this job schedule.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Viewing Scheduled Jobs

To view the scheduled backup jobs, follow these steps:

- Step 1** Click the **Config File** tab, and then click **Show Jobs**.  
You see the scheduled jobs information as shown in [Figure 7-71](#).

**Figure 7-71** Viewing Scheduled Jobs



- Step 2** Double-click one of the listed scheduled jobs to view them.





## CHAPTER 8

# Performance Manager

---

The primary purpose of Fabric Manager is to manage the network. A key management capability is network performance monitoring. This chapter includes the following topics:

- [Performance Manager Architecture, page 8-1](#)
- [Flow Statistics, page 8-6](#)

## Performance Manager Architecture

Performance Manager gathers network device statistics historically and provides this information graphically using a web browser. It presents recent statistics in detail and older statistics in summary. Performance Manager also integrates with external tools such as Cisco Traffic Analyzer.

The Performance Manager has three operational stages:

- Definition—The Flow Wizard sets up flows in the switches.
- Collection—The Web Server Performance Collection screen collects information on desired fabrics.
- Presentation—Generates web pages to present the collected data through Fabric Manager Web Server.

Performance Manager can collect statistics for ISLs, hosts, storage elements, and configured flows. Flows are defined based on a host-to-storage (or storage-to-host) link. Performance Manager gathers statistics from across the fabric based on collection configuration files. These files determine which SAN elements and SAN links Performance Manager gathers statistics for. Based on this configuration, Performance Manager communicates with the appropriate devices (switches, hosts, or storage elements) and collects the appropriate information at fixed five-minute intervals.

Performance Manager uses a round-robin database to hold the statistical data collected from the fabric. This data is stored based on the configured parameters in the collection configuration file. At each polling interval, Performance Manager gathers the relevant statistics and stores them in the round-robin database. This database is a fixed size and will not grow beyond its preset limits.

Performance Manager creates a series of archived data to hold summarized information present in the real-time round-robin database. This archived data is used to generate daily, weekly, monthly, and yearly consolidated reports. In this way, Performance Manager maintains significant historical data without the cost of an ever-increasing database size.



### Note

You must restart Performance Manager if you change the user credentials on Fabric Manager Server.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Data Interpolation

One of the unique features of Performance Manager is its ability to interpolate data when statistical polling results are missing or delayed. Other performance tools may store the missing data point as zero, but this can distort historical trending. Performance Manager interpolates the missing data point by comparing the data point that preceded the missing data and the data point stored in the polling interval after the missing data. This maintains the continuity of the performance information.

## Data Collection

One year's worth of data for two variables (Rx and Tx bytes) requires a round-robin database (rrd) file size of 76 K. If errors and discards are also collected, the rrd file size becomes 110 K. The default internal values are as follows:

- 600 samples of 5 minutes (2 days and 2 hours)
- 700 samples of 30 minutes (12.5 days)
- 775 samples of 2 hours (50 days)
- 300 samples of 1 day

A 1000-port SAN requires 110 MB for a year's worth of historical data that includes errors and discards. If there were 20 switches in this SAN with equal distribution of fabric ports, about two to three SNMP packets per switch would be sent every 5 minutes for a total of about 100 request or response SNMP packets required to monitor the data.

Because of their variable counter requests, flows are more difficult to predict storage space requirements for. But in general you can expect that, each extra flow adds another 76 KB.



### Note

---

Performance Manager does not collect statistics on nonmanageable and non-MDS switches. Loop devices (FL/NL) are not collected.

---

## Using Performance Thresholds

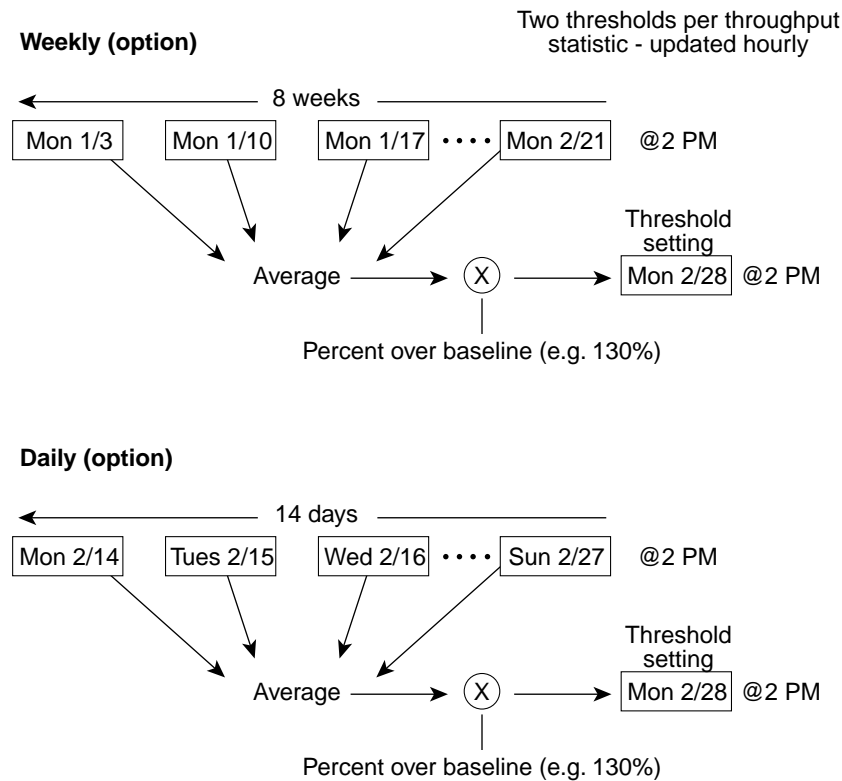
The Performance Manager Configuration Wizard allows you to set up two thresholds that will trigger events when the monitored traffic exceeds the percent utilization configured. These event triggers can be set as either Critical or Warning events that are reported on the Fabric Manager web client Events browser page.

Absolute value thresholds apply directly to the statistics gathered. These statistics, as a percent of the total link capacity, are compared to the percent utilization configured for the threshold type. If the statistics exceed either configured threshold, an event is shown on the Fabric Manager web client Events tab.

Baseline thresholds create a threshold that adapts to the typical traffic pattern for each link for the same time window each day, week, or every two weeks. Baseline thresholds are set as a percent of the average (110% to 500%), where 100% equals the calculated weighted average. [Figure 8-1](#) shows an example of setting a baseline threshold for a weekly or daily option.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 8-1 Baseline Threshold Example**



The threshold is set for Monday at 2 p.m. The baseline threshold is set at 130% of the average for that statistic. The average is calculated from the statistics value that occurred at 2 p.m. on Monday, for every prior Monday (for the weekly option) or the statistics value that occurred at 2 p.m. on each day, for every prior day (for the daily option).

## Flow Setup Wizards

The Performance Manager Flow and Performance Manager Setup wizards greatly simplify configuration. All you need to do is select the categories of statistics to capture and the wizards provide a list of flows and links to monitor. You can remove entries if desired, or just accept the provided list and start data collection. Statistics for host and storage links are not associated with a specific port on a switch, so you do not lose long term statistics if a connection is moved to a different port.

## Creating a Flow Using Flow Configuration Wizard

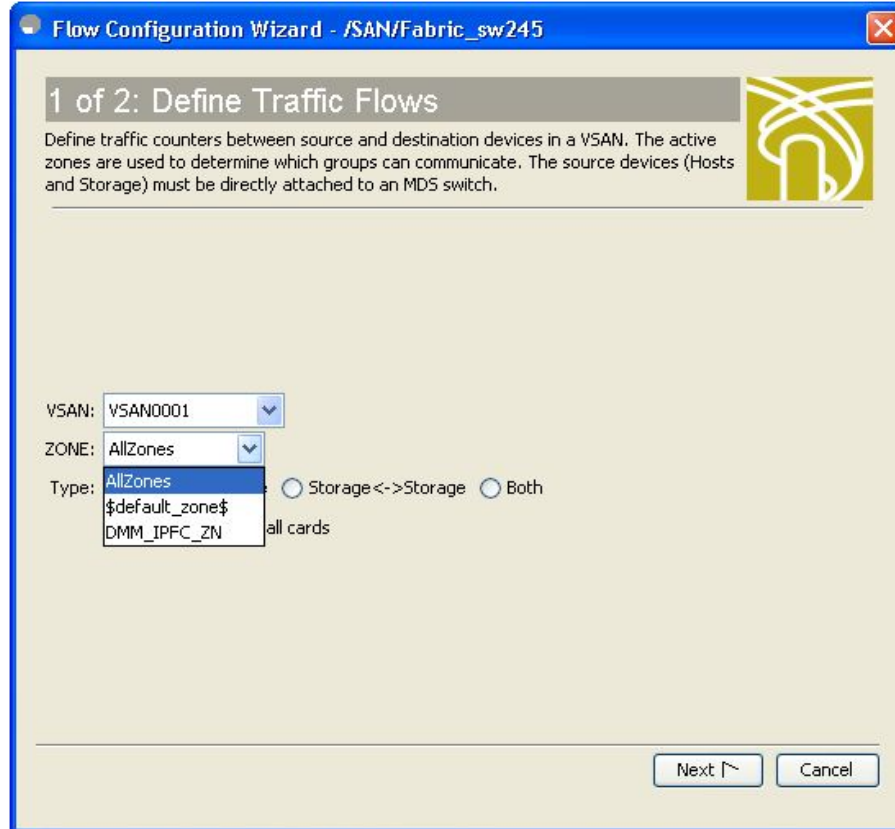
To create a flow using Fabric Manager, follow these steps:

**Step 1** Choose **Performance > Create Flows**.

You see the Define Traffic Flows dialog box as shown in [Figure 8-2](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

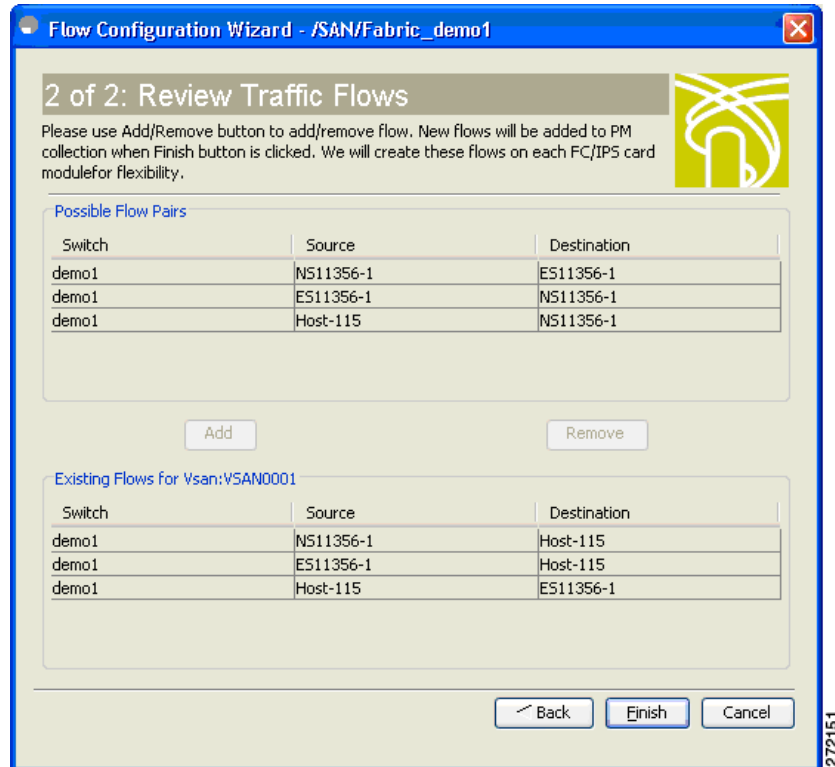
**Figure 8-2** Create Flows Dialog Box



- Step 2** Click the drop-down menu in the VSAN field.
- Step 3** Choose the list of VSANs provided by the flow configuration wizard.
- Step 4** Click the drop-down menu in the Zone field.
- Step 5** Choose the list of zones provided by the flow configuration wizard.
- Step 6** Click **Next** to continue to the next window as shown in [Figure 8-3](#).

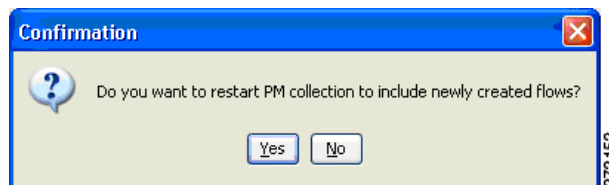
*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 8-3 Review Traffic Flows Dialog Box**



- Step 7** Choose items in the Possible Flow Pairs area.
- The Review Traffic Flows window displays all VSAN flow pairs in the Existing Flows for Vsan area.
- Step 8** Click **Add** to create the selected flow.
- Step 9** Choose items in the Existing Flows for Vsan area.
- Step 10** Click **Remove** to remove the selected flow.
- Step 11** Click **Finish** to restart the Performance Manager collection.
- You see the Confirmation dialog box as shown in [Figure 8-4](#).

**Figure 8-4 Confirmation Dialog Box**



To verify the newly created flow, choose **Physical Attributes > End Devices > Flow Statistics**. The newly created flows are displayed.

[Send documentation comments to fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)

## Flow Statistics

Flow statistics count the ingress traffic in the aggregated statistics table. You can collect two kinds of statistics:

- Aggregated flow statistics to count the traffic for a VSAN.
- Flow statistics to count the traffic for a source and destination ID pair in a VSAN.

If you enable flow counters, you can enable a maximum of 1 K entries for aggregate flow and flow statistics. Be sure to assign an unused flow index to a module for each new flow. Flow indexes can be repeated across modules. The number space for flow index is shared between the aggregate flow statistics and the flow statistics.

Generation 1 modules allow a maximum of 1024 flow statements per module. Generation 2 modules allow a maximum of 2048-128 flow statements per module.

[Table 8-1](#) explains the Flow Type radio button that defines the type of traffic monitored.

**Table 8-1** Performance Manager Flow Types

| Flow type     | Description                                                                   |
|---------------|-------------------------------------------------------------------------------|
| Host->Storage | Unidirectional flow, monitoring data from the host to the storage element     |
| Storage->Host | Unidirectional flow, monitoring data from the storage element to the host     |
| Both          | Bidirectional flow, monitoring data to and from the host and storage elements |



## CHAPTER 9

# Cisco Traffic Analyzer

Cisco Traffic Analyzer is a version of network top (ntop) software that is modified to support Fibre Channel and SCSI.

This chapter contains the following sections:

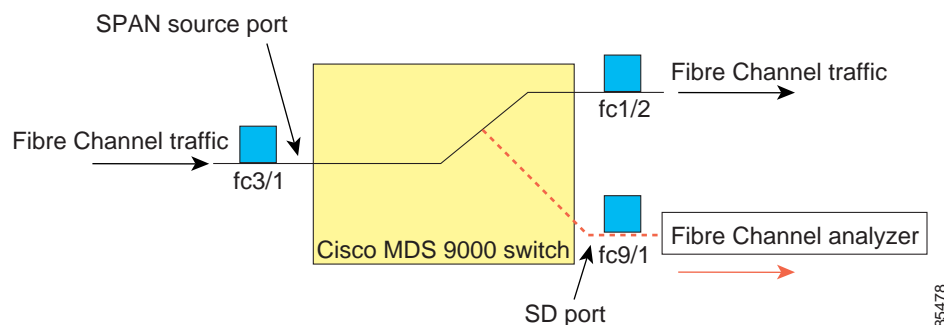
- [Understanding SPAN, page 9-1](#)
- [Using Cisco Traffic Analyzer with Performance Manager, page 9-2](#)
- [Installing Cisco Traffic Analyzer, page 9-3](#)
- [Accessing Traffic Analyzer from Fabric Manager Web Server, page 9-5](#)

## Understanding SPAN

The SPAN feature is specific to switches in the Cisco MDS 9000 Family. It monitors network traffic through a Fibre Channel interface. Traffic through any Fibre Channel interface can be replicated to a special port called the SPAN destination port (SD port). Any Fibre Channel port in a switch can be configured as an SD port. Once an interface is in SD port mode, it cannot be used for normal data traffic. You can attach a Fibre Channel analyzer to the SD port to monitor SPAN traffic.

SD ports do not receive frames, they transmit a copy of the SPAN source traffic. The SPAN feature is nonintrusive and does not affect switching of network traffic for any SPAN source ports (see [Figure 9-1](#)).

**Figure 9-1** SPAN Transmission



For information on configuring SPAN, refer to the *Cisco MDS 9000 Family Fabric Manager System Management Configuration Guide*.

[Send documentation comments to fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)

## Using Cisco Traffic Analyzer with Performance Manager

Performance Manager works in conjunction with Cisco Traffic Analyzer to monitor and manage the traffic on your fabric. Using Cisco Traffic Analyzer with Performance Manager requires the following components:

- A configured Fibre Channel Switched Port Analyzer (SPAN) destination (SD) port to forward Fibre Channel traffic.
- A Port Analyzer Adapter 2 (PAA-2) to convert the Fibre Channel traffic to Ethernet traffic.
- Cisco Traffic Analyzer software to analyze the traffic from the PAA-2.

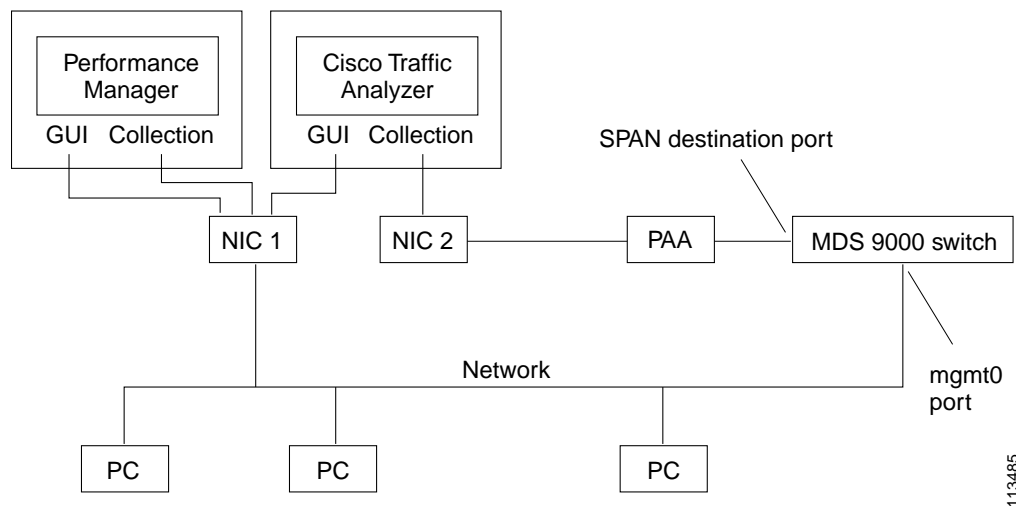


### Note

We recommend that you install Traffic Analyzer and Performance Manager on separate servers. Linux server is recommended for installing Traffic Analyzer.

Figure 9-2 shows how Performance Manager works with Cisco Traffic Analyzer to monitor traffic on your fabric.

**Figure 9-2** Overview of Performance Manager Working with Cisco Traffic Analyzer



113485

## Understanding the PAA-2

The PAA-2 enables effective, low-cost analysis of Fibre Channel traffic. The device is a standalone Fibre Channel-to-Ethernet adapter, designed primarily to analyze SPAN traffic from a Fibre Channel port on a Cisco MDS 9000 Family switch. The main function of the Port Analyzer Adapter 2 is to encapsulate Fibre Channel frames into Ethernet frames. This allows low-cost analysis of Fibre Channel traffic while leveraging the existing Ethernet infrastructure.

The PAA-2 allows you to examine Fibre Channel frames of various sizes. Fibre Channel frames from Layers 2, 3, and 4 may be examined without network disruption.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Understanding Cisco Traffic Analyzer

Performance Manager collects Fibre Channel level performance statistics using SNMP to access counters on Cisco MDS 9000 Family switches. To view detailed SCSI I/O statistics, you need to look at the data on an SD port with the help of Cisco Traffic Analyzer, which uses the Cisco Port Analyzer Adapter 2 (PAA-2).

Cisco Traffic Analyzer provides real-time analysis of SPAN traffic or analysis of captured traffic through a Web browser user interface. Traffic encapsulated by one or more Port Analyzer Adapter 2 products can be analyzed concurrently with a single workstation running Cisco Traffic Analyzer, which is based on ntop, a public domain software enhanced by Cisco for Fibre Channel traffic analysis.

Round-trip response times, SCSI I/Os per second, SCSI read or traffic throughput and frame counts, SCSI session status, and management task information are monitored. Additional statistics are also available on Fibre Channel frame sizes and network management protocols.

For seamless performance analysis and troubleshooting, Cisco Traffic Analyzer can be launched in-context from Fabric Manager. Port world wide name (pWWN), Fibre Channel ID (FC ID), FC alias, and VSAN names are passed to Cisco Traffic Analyzer.

Cisco Traffic Analyzer must be downloaded and installed separately from the following website:

<http://www.cisco.com/kobayashi/sw-center/sw-stornet.shtml>.

Cisco Traffic Analyzer software is available under the Port Analyzer Adapter link. See the “[Installing Cisco Traffic Analyzer](#)” section on page 9-3.



### Caution

Cisco Traffic Analyzer for Fibre Channel throughput values are not accurate when used with the original Cisco Port Analyzer Adapter (PAA) if data truncation is enabled. PAA Version 2 (product ID DS-PAA\_2) is required to achieve accurate results with truncation, because it adds a count that enables Cisco Traffic Analyzer to determine how many data bytes were actually transferred.



### Note

Refer to the *Cisco MDS 9000 Family Fabric Manager System Management Configuration Guide* for information on configuring the settings for your SPAN destination port. It is important that the data you collect through this port matches the data collected by Performance Manager through the mgmt0 port. If the data does not match, you cannot view Cisco Traffic Analyzer information through a Traffic Analyzer link on the detail page of a Performance Manager report.

## Installing Cisco Traffic Analyzer

To install Cisco Traffic Analyzer on a UNIX workstation, follow these steps:

- Step 1** Open a browser and go to the following website to access the web page where Cisco Traffic Analyzer is available:  
  
<http://cisco.com/cgi-bin/tablebuild.pl/mds-fm>.
- Step 2** Download fc-ntop.tar.gz and install it using the instructions at the following website:  
  
<http://www.ntop.org>.
- Step 3** Verify that the Fibre Channel port on the PAA-2 is connected to the SD port on the switch ([Figure 9-2](#)).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 4** Verify that the Ethernet port on the PAA-2 is connected to the workstation running Cisco Traffic Analyzer.
- Step 5** Click **Interfaces > SPAN** in Device Manager to configure SPAN on the required switch ports.
- Step 6** Click **Interfaces > SPAN** in Device Manager to verify that the Fibre Channel port connected to the PAA-2 is configured as an SD port. The port mode of the destination interface must be SD.
- Step 7** Click the **Sessions** tab in Device Manager to verify the correct destination and source of traffic (ingress).



#### Caution

Cisco Traffic Analyzer must not be used with the PAA-2 in Management mode (MNM). Refer to the *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*.

To install Cisco Traffic Analyzer on a Windows workstation, follow these steps:

- Step 1** Open a browser and go to the following website to access the web page where Cisco Traffic Analyzer is available:  
  
<http://cisco.com/cgi-bin/tablebuild.pl/mds-fm>.
- Step 2** Download ntop-win32.zip and save it on your workstation.
- Step 3** Unzip the downloaded file.



#### Note

You need the WinPcap library file to use Cisco Traffic Analyzer on a Microsoft Windows system. You can download this file from the following website:

<http://winpcap.polito.it/>.

- Step 4** Open a command prompt and change directories to your ntop installation directory.
- Step 5** Type **ntop -i** or install ntop as a service on Windows by following these steps:
  - a. Type **ntop /i** to install ntop as a service.
  - b. Choose **Start > Programs > Administrative Tools > Services** to access the Windows Services Panel.
  - c. Right-click **ntop** and choose **properties**. You see the Properties dialog box.
  - d. Set the Start Parameters to **-i interface number**, where *interface number* is the number of the interface on your workstation that connects to the PAA-2.
  - e. Click **Start** to start ntop on that interface.



#### Note

Subsequent restarts of the ntop service do not require setting the -i option, unless you are changing the interface that connects to the PAA-2.

- Step 6** Verify that the Fibre Channel port on the PAA-2 is connected to the SD port on the switch (Figure 9-2).
- Step 7** Verify that the Ethernet port on the PAA-2 is connected to the workstation running Cisco Traffic Analyzer.
- Step 8** Click **Interfaces > SPAN** in Device Manager to configure SPAN on the required switch ports.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 9** Click the **Sources** tab in Device Manager to verify that the Fibre Channel port connected to the PAA-2 is configured as an SD port. The port mode of the destination interface must be SD.
- Step 10** Click the **Sessions** tab in Device Manager to verify the correct destination and source of traffic (ingress).
- 

**Tip**

To modify the script that launches ntop (ntop.sh or ntop.bat), follow the instructions provided within the script file. Create a backup of the original script before modifying the file.

—Linux platforms use the shell script path. The ntop output is sent to the syslog file (/var/log/messages by default).

—Windows platforms use the batch file. The ntop output is sent to a file located in the same directory as the one from which ntop is launched.

---

## Accessing Traffic Analyzer from Fabric Manager Web Server

Fabric Manager supports discovering instances of Traffic Analyzer and SPAN ports configured within your fabric.

Fabric Manager Web Server supports the following Traffic Analyzer integration features:

- SCSI I/O Traffic Analyzer pages can be viewed within the Web client.
- Traffic Analyzer can reside on a different server than Performance Manager.
- Performance Manager integrates with multiple servers running Traffic Analyzer.
- Instances of Traffic Analyzer servers can be discovered by Fabric Manager Server.
- Web client report lists SPAN destination ports and associations with Traffic Analyzers.

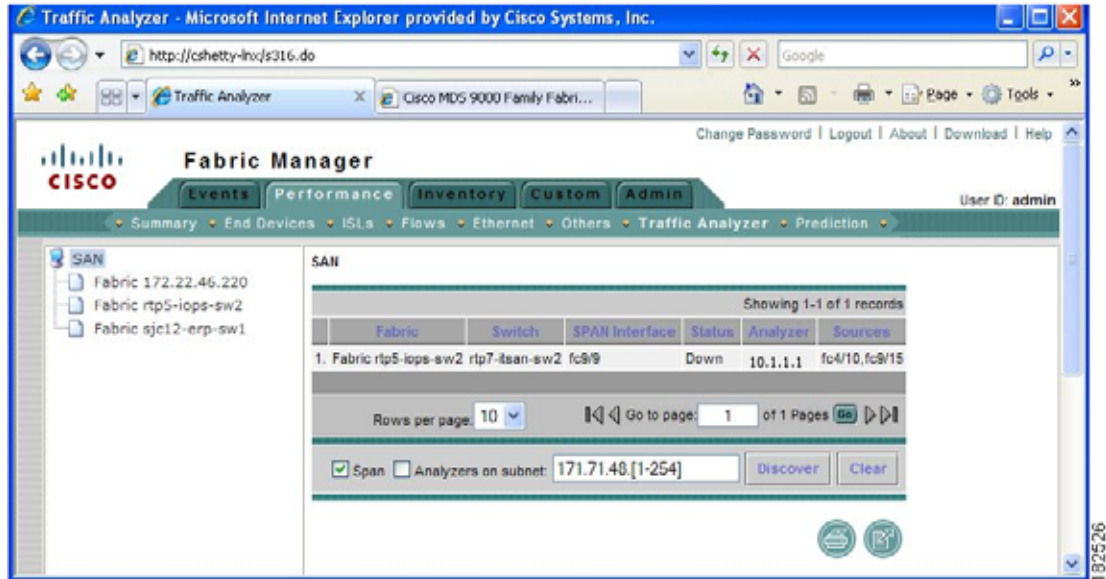
To access an instance of Traffic Analyzer running in your fabric using Fabric Manager Web Server, follow these steps:

- 
- Step 1** Click the **Performance** tab and then click the **Traffic Analyzer** tab.

You see a summary table of all SPAN destination ports and configured Traffic Analyzers in your fabric (see [Figure 9-3](#)). The source column shows the ports that are monitored by the SPAN destination port.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 9-3** Traffic Analyzer in Fabric Manager Web Server



**Step 2** Click a Traffic Analyzer to launch that Traffic Analyzer within Fabric Manager Web Server.

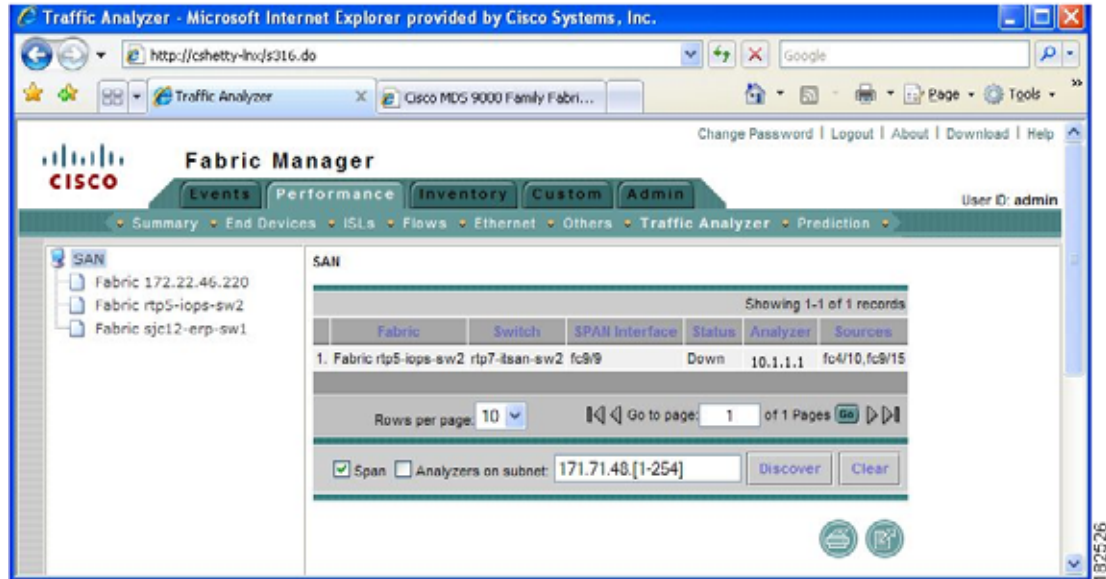
To rediscover instances of Traffic Analyzer running in your fabric using Fabric Manager Web Server, follow these steps:

**Step 1** Choose **Performance > Traffic Analyzer**.

You see a summary table of all SPAN destination ports and configured Traffic Analyzers in your fabric shown in [Figure 9-4](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 9-4** Traffic Analyzer in Fabric Manager Web Server



- Step 2** Navigate to the fabric or VSAN where you want to rediscover instances of Traffic Analyzer from the navigation bar.
- Step 3** Set Analyzers on Subnet to the subnet that you want to discover.
- Step 4** Click **Discover** to find instances of Traffic Analyzer within the selected fabric or VSAN and subnet.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*



## CHAPTER 10

# Network Monitoring

---

The primary purpose of Fabric Manager is to manage the network. In particular, SAN discovery and network monitoring are two of its key network management capabilities.

This chapter contains the following sections:

- [SAN Discovery and Topology Mapping, page 10-1](#)
- [Health and Event Monitoring, page 10-4](#)

## SAN Discovery and Topology Mapping

Fabric Manager provides extensive SAN discovery, topology mapping, and information viewing capabilities. Fabric Manager collects information on the fabric topology through SNMP queries to the switches connected to it. Fabric Manager recreates a fabric topology, presents it in a customizable map, and provides inventory and configuration information in multiple viewing options.

## Device Discovery

Once Fabric Manager is invoked, a SAN discovery process begins. Using information polled from a seed Cisco MDS 9000 Family switch, including Name Server registrations, Fibre Channel Generic Services (FC-GS), Fabric Shortest Path First (FSPF), and SCSI-3, Fabric Manager automatically discovers all devices and interconnects on one or more fabrics. All available switches, host bus adapters (HBAs), and storage devices are discovered. The Cisco MDS 9000 Family switches use Fabric-Device Management Interface (FMDI) to retrieve HBA model, serial number and firmware version, and host operating-system type and version discovery without host agents. Fabric Manager gathers this information through SNMP queries to each switch. The device information discovered includes device names, software revision levels, vendor, ISLs, PortChannels, and VSANs.

For a VSAN change involving a third-party switch, Fabric Manager will need a second discovery to show the correct topology due to the discovery dependency when there is any change in a mixed VSAN. The first discovery finds the third-party switch and the subsequent discovery will show the information on which VSAN it is going to join and can discover the end devices connected to it. You can wait for the subsequent discovery or trigger a manual discovery

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Topology Mapping

Fabric Manager is built upon a topology representation of the fabric. Fabric Manager provides an accurate view of multiple fabrics in a single window by displaying topology maps based on device discovery information. You can modify the topology map icon layout with an easy-to-use, drag-and-drop interface. The topology map visualizes device interconnections, highlights configuration information such as zones, VSANs, and ISLs exceeding utilization thresholds. The topology map also provides a visual context for launching command-line interface (CLI) sessions, configuring PortChannels, and opening device managers.

### Using the Topology Map

The Fabric Manager topology map can be customized to provide a view into the fabric that varies from showing all switches, end devices, and links, to showing only the core switches with single bold lines for any multiple links between switches. Use the icons along the left side of the topology map to control these views or right-click anywhere in the topology map to access the map controls.

You can zoom in or out on the topology map to see an overview of the SAN or focus on an area of importance. You can also open an overview window that shows the entire fabric. From this window, you can right-click and draw a box around the area you want to view in the main topology map view.

Another way to limit the scope of the topology display is to select a fabric or VSAN from the Logical Domains pane. The topology map displays only that fabric or VSAN.

Moving the mouse pointer over a link or switch provides a simple summary of that SAN component, along with a status indication. Right-clicking on the component brings up a pop-up menu. You can view the component in detail or access configuration or test features for that component.

Double-click a link to bring link status and configuration information to the information pane.

Double-click a switch to bring up Device Manager for that switch.

### Saving a Customized Topology Map Layout

Changes made to the topology map can be saved so that the customized view is available any time you open the Fabric Manager Client for that fabric.

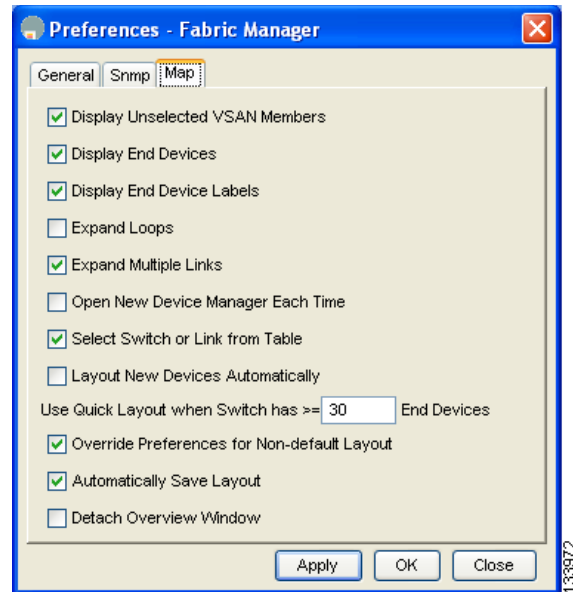
To save the customized layout using Fabric Manager, follow these steps:

- 
- Step 1** Click **File > Preferences** to open the Fabric Manager preferences dialog box.
  - Step 2** Click the **Map** tab and check the **Automatically Save Layout** check box to save any changes to the topology map as shown in [Figure 10-1](#).



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 10-1** Fabric Manager Preferences



**Step 3** Click **Apply**, and then click **OK** to save this change.

## Using Enclosures with Fabric Manager Topology Maps

Because not all devices are capable of responding to FC-GS-3 requests, different ports of a single server or storage subsystem may be displayed as individual end devices on the topology map. See the [“Modifying the Device Grouping” section on page 5-37](#) to group these ports into a single enclosure for Fabric Manager.

Clicking **Alias->Enclosure** displays hosts and storage elements in the Information pane. This is a shortcut to naming enclosures. To use this shortcut, highlight each row in the host or storage table that you want grouped in an enclosure then click **Alias -> Enclosure**. This automatically sets the enclosure names of each selected row with the first token of the alias.

## Mapping Multiple Fabrics

To log into multiple fabrics, the same username and password must be used. The information for both fabrics is displayed, with no need to select a seed switch. To see details of a fabric, click the tab for that fabric at the bottom of the Fabric pane, or double-click the fabric’s cloud icon. To continuously manage a fabric using Fabric Manager, follow the instructions in the [“Managing a Fabric Manager Server Fabric” section on page 3-6](#).

## Inventory Management

The Information pane in Fabric Manager shows inventory, configuration, and status information for all switches, links, and hosts in the fabric. Inventory management includes vendor name and model, and software or firmware versions. Select a fabric or VSAN from the Logical Domains pane, and then select

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

the **Summary** tab in the Information pane to get a count of the number of VSANS, switches, hosts, and storage elements in the fabric. See the “[Fabric Manager Client Quick Tour: Admin Perspective](#)” section on page 5-15 for more information on the Fabric Manager user interface.

## Using the Inventory Tab from Fabric Manager Web Server

If you have configured Fabric Manager Web Server, you can launch this application and access the Inventory tab to see a summary of the fabrics managed by the Fabric Manager Server. The Inventory tab shows an inventory of the selected SAN, fabric, or switch. See [Chapter 7, “Fabric Manager Web Client”](#) for more information on how to configure and use Fabric Manager Web Server.

To view system messages remotely using Fabric Manager Web Server, follow these steps:

- 
- Step 1** Point your browser at the Fabric Manager Web Server. See the “[Launching Fabric Manager Web Client](#)” section on page 7-7.
  - Step 2** Click the **Events** tab then the **Details** to view the system messages. The columns in the events table are sortable. In addition, you can use the Filter button to limit the scope of messages within the table.
- 

## Viewing Logs from Device Manager

You can view system messages from Device Manager if Device Manager is running from the same workstation as the Fabric Manager Server. Choose **Logs > Events > current** to view the system messages on Device Manager. The columns in the events table are sortable. In addition, you can use the Find button to locate text within the table.

You can view switch-resident logs even if you have not set up your local syslog server or your local PC is not in the switch's syslog server list. Due to memory constraints, these logs will wrap when they reach a certain size. The switch syslog has two logs: an NVRAM log that holds a limited number of critical and greater messages and a nonpersistent log that contains notice or greater severity messages. Hardware messages are part of these logs.



### Note

To view syslog local logs, you need to configure the IP address of the Fabric Manager Server in the syslog host.

## Health and Event Monitoring

Fabric Manager works with the Cisco MDS 9000 Family switches to show the health and status of the fabric and switches. Information about the fabric and its components is gathered from multiple sources, including Online System Health Management, Call Home, system messages, and SNMP notifications. This information is then made available from multiple menus on Fabric Manager or Device Manager.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Fabric Manager Events Tab

The Fabric Manager Events tab, available from the topology window, displays the events Fabric Manager received from sources within the fabric. These sources include SNMP events, RMON events, system messages, and system health messages. The Events tab shows a table of events, including the event name, the source and time of the event, a severity level, and a description of the event. The table is sortable by any of these column headings.

## Event Information in Fabric Manager Web Server Reports

The Fabric Manager web server client displays collections of information gathered by the Performance Manager. This information includes events sent to the Fabric Manager Server from the fabric. To open these reports, choose **Performance Manager > Reports**. This opens the web client in a web browser and displays a summary of all fabrics monitored by the Fabric Manager Server. Choose a fabric and then click the **Events** tab to see a summary or detailed report of the events that have occurred in the selected fabric. The summary view shows how many switches, ISLs, hosts, or storage elements are down on the fabric and how many warnings have been logged for that SAN entity. The detailed view shows a list of all events that have been logged from the fabric and can be filtered by severity, time period, or type.

## Events in Device Manager

Device Manager displays the events when you choose **Logs > Events**. Device Manager can display the current list of events or an older list of events that has been stored on the Fabric Manager host. The event table shows details on each event, including time, source, severity, and a brief description of the event.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*



# CHAPTER 11

## Performance Monitoring

---

Cisco Fabric Manager and Device Manager provide multiple tools for monitoring the performance of the overall fabric, SAN elements, and SAN links. These tools provide real-time statistics as well as historical performance monitoring.

This chapter contains the following sections:

- [Real-Time Performance Monitoring, page 11-1](#)
- [Historical Performance Monitoring, page 11-4](#)
- [Analyzing SAN Health, page 11-12](#)

## Real-Time Performance Monitoring

Device Manager provides an easy tool for monitoring ports on the Cisco MDS 9000 Family switches. This tool gathers statistics at a configurable interval and displays the results in tables or charts. Real-time performance statistics are useful for dynamic troubleshooting and fault isolation within the fabric. Real-time statistics gather data on parts of the fabric in user-configurable intervals and display these results in Fabric Manager and Device Manager. For a selected port, you can monitor any of a number of statistics including traffic in and out, errors, class 2 traffic, and FICON data.

## Device Manager Real-time Performance Monitoring

Device Manager provides an easy tool for monitoring ports on the Cisco MDS 9000 Family switches. This tool gathers statistics at a configurable interval and displays the results in tables or charts. These statistics show the performance of the selected port in real-time and can be used for performance monitoring and troubleshooting. For a selected port, you can monitor any of a number of statistics including traffic in and out, errors, class 2 traffic, and FICON data. You can set the polling interval from ten seconds to one hour, and display the results based on a number of selectable options including absolute value, value per second, and minimum or maximum value per second.

Device Manager checking for oversubscription on the host-optimized four-port groups on relevant modules. Right-click the port group on a module and choose **Check Oversubscription** from the pop-up menu.

Device manager provides two performance views: the Summary View tab and the configurable monitor option per port.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

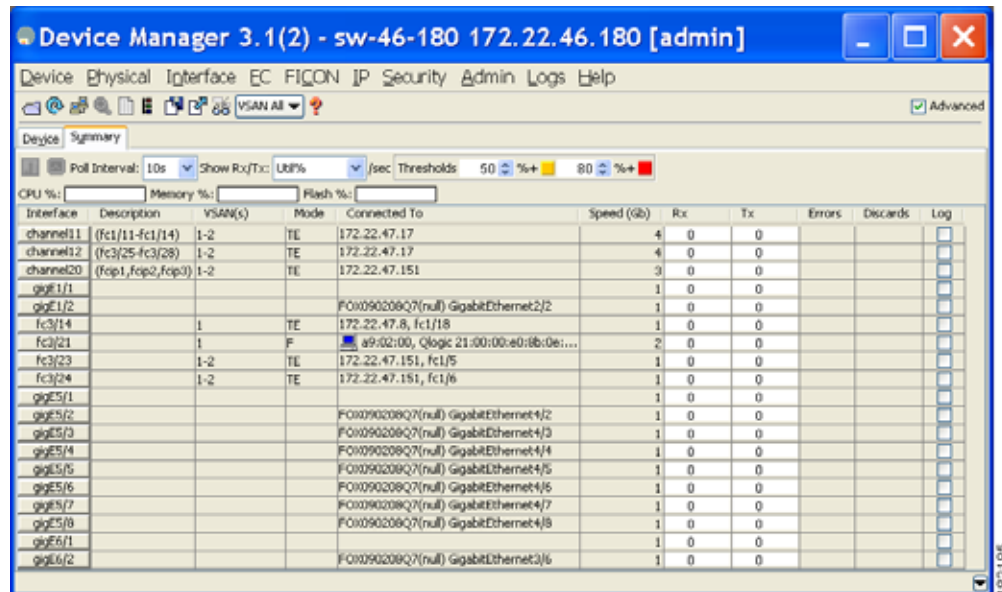
## Configuring the Summary View

To configure the summary view in Device Manager, follow these steps:

- Step 1** Click the **Summary** tab on the main display.

You see all of the active ports on the switch, as well as the configuration options available from the Summary view shown in [Figure 11-1](#).

**Figure 11-1** Device Manager Summary Tab



- Step 2** Select a value from the **Poll Interval** drop-down list.
- Step 3** Decide how you want your data to be interpreted by looking at the **Show Rx/Tx** drop-down menu. The table updates each polling interval to show an overview of the receive and transmit data for each active port on the switch.
- Step 4** Select a value from the **Show Rx/Tx** drop-down list. If you select **Util%**, you need to also select values from the two **Show Rx/Tx > %Util/sec** drop-down lists. The first value is the warning level and the second value is the critical threshold level for event reporting.

Note that you can also display percent utilization for a single port by selecting the port and clicking the **Monitor Selected Interface Traffic Util %** icon.

The configurable monitor per port option gives statistics for in and out traffic on that port, errors, class 2 traffic and other data that can be graphed over a period of time to give a real-time view into the performance of the port.

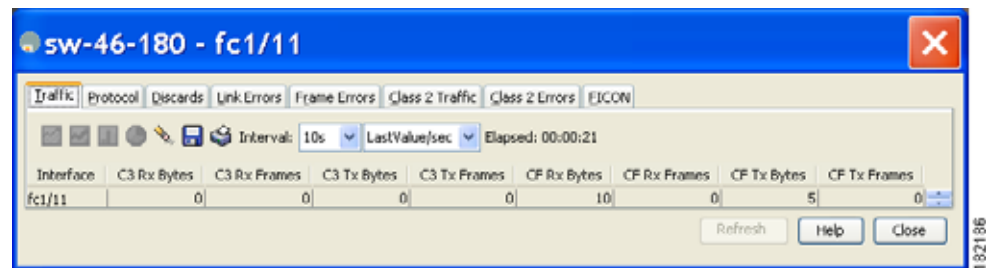
To configure per port monitoring using Device Manager, follow these steps:

- Step 1** Click the **Device** tab.
- Step 2** Right-click the port you are interested in and choose **Monitor** from the drop-down menu.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

You see the port real-time monitor dialog box shown in Figure 11-2.

**Figure 11-2** Device Manager Monitor Dialog Box



**Step 3** Select a value from the **Interval** drop-down list to determine how often data is updated in the table shown here.

**Step 4** Click a statistical value in the table then click one of the graphing icons to display a running graph of that statistic over time. You see a graph window that contains options to change the graph type.



**Tip** You can open multiple graphs for statistics on any of the active ports on the switch.

## Fabric Manager Real-Time ISL Statistics

You can configure Fabric Manager to gather ISL statistics in real time. These ISL statistics include receive and transmit utilization, bytes per second, as well as errors and discards per ISL.

To configure ISL statistics using Fabric Manager, follow these steps:

**Step 1** Choose **Performance > ISLs in Real-Time**.

You see any ISL statistics in the Information pane as shown in Figure 11-3.

**Figure 11-3** ISL Performance in Real Time

| From Switch     | From Interface | To Switch       | To Interface | Speed | Rx Util% | Rx Bytes | Rx Pkts | Tx Util% | Tx Bytes | Tx Pkts | Total Errors | Total Discards |
|-----------------|----------------|-----------------|--------------|-------|----------|----------|---------|----------|----------|---------|--------------|----------------|
| sw172-22-46-224 | fc1/17         | sw172-22-46-222 | fc2/17       | 2 Gb  | 0        | 953      | 7       | 0        | 523      | 9       | 0            | 0              |
| sw172-22-46-223 | fc1/7          | sw172-22-46-222 | fc1/7        | 2 Gb  | 0        | 50       | 0       | 0        | 6        | 0       | 0            | 0              |
| sw172-22-46-223 | fc1/10         | sw172-22-46-222 | fc1/10       | 2 Gb  | 0        | 73       | 1       | 0        | 531      | 5       | 0            | 0              |
| sw172-22-46-223 | fc1/11         | sw172-22-46-222 | fc1/11       | 2 Gb  | 0        | 88       | 1       | 0        | 547      | 5       | 0            | 0              |
| sw172-22-46-223 | fc1/12         | sw172-22-46-222 | fc1/12       | 2 Gb  | 0        | 395      | 6       | 0        | 46       | 1       | 0            | 0              |
| sw172-22-46-223 | fc1/14         | sw172-22-46-222 | fc1/14       | 2 Gb  | 0        | 64       | 0       | 0        | 28       | 0       | 0            | 0              |
| sw172-22-46-223 | fc1/16         | sw172-22-46-222 | fc1/16       | 2 Gb  | 0        | 156      | 2       | 0        | 70       | 1       | 0            | 0              |
| sw172-22-46-222 | fc1/1          | sw172-22-46-221 | fc2/29       | 2 Gb  | 0        | 1.308K   | 20      | 0        | 2.148K   | 17      | 0            | 0              |
| sw172-22-46-222 | fc1/4          | sw172-22-46-225 | fc1/4        | 2 Gb  | 0        | 1.026K   | 13      | 0        | 1.648K   | 16      | 0            | 0              |
| sw172-22-46-225 | fc1/3          | sw172-22-47-118 | fc1/20       | 2 Gb  | 0        | 0        | 0       | 0        | 0        | 0       | 0            | 0              |
| sw172-22-46-225 | fc1/5          | sw172-22-46-224 | fc1/5        | 2 Gb  | 0        | 362      | 3       | 0        | 341      | 4       | 0            | 0              |
| sw172-22-46-225 | fc1/9          | sw172-22-46-224 | fc1/9        | 2 Gb  | 0        | 244      | 3       | 0        | 364      | 4       | 0            | 0              |

**Step 2** Select a value from the **Poll Interval** drop-down list.

**Step 3** Select two values from the **Bandwidth** utilization thresholds drop-down lists, one value for the minor threshold and one value for the major threshold.

The table shown updates each polling interval to show the statistics for all configured ISLs in the fabric.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Step 4** Select a row in the table to highlight that ISL in blue in the Topology map.

---

## Historical Performance Monitoring

Performance Manager gathers network device statistics historically and provides this information using Fabric Manager client and web browser. It presents recent statistics in detail and older statistics in summary. Performance Manager also integrates with external tools such as Cisco Traffic Analyzer. See the [“Performance Manager Architecture” section on page 8-1](#) for an overview of Performance Manager.

### Creating a Flow with Performance Manager

With the Flow Configuration Wizard you can create host-to-storage, storage-to-host, or bidirectional flows. Once defined, you can add these flows to a collection configuration file to monitor the traffic between a host/storage element pair. The flows created become part of the collection options in the Performance Manager Configuration Wizard. See the [“Flow Statistics” section on page 8-6](#) for information on creating flows.

### Creating a Collection with Performance Manager

The Performance Manager Configuration Wizard steps you through the process of creating collections using configuration files. Collections are defined for one or all VSANs in the fabric. Collections can include statistics from the SAN element types described in [Table 11-1](#).

**Table 11-1** Performance Manager Collection Types

| Collection Type | Description                                                        |
|-----------------|--------------------------------------------------------------------|
| ISLs            | Collects link statistics for ISLs.                                 |
| Host            | Collects link statistics for SAN hosts.                            |
| Storage         | Collects link statistics for a storage elements.                   |
| Flows           | Collects flow statistics defined by the Flow Configuration Wizard. |

### Using Performance Thresholds

The Performance Manager Configuration Wizard allows you to set up two thresholds that trigger events when the monitored traffic exceeds the percent utilization configured. These event triggers can be set as either Critical or Warning events that are reported on the Fabric Manager web client Events browser page.

You must choose either absolute value thresholds or baseline thresholds that apply to all transmit or receive traffic defined in the collection. Click the **Use absolute values** radio button on the last screen of the Performance Manager Configuration Wizard to configure thresholds that apply directly to the statistics gathered. These statistics, as a percent of the total link capacity, are compared to the percent utilization configured for the threshold type. If the statistics exceed either configured threshold, an event is shown on the Fabric Manager web client Events tab.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

As an example, the collection has absolute value thresholds set for 60% utilization (for warning) and 80% utilization (for critical). If Performance Manager detects that the traffic on a 1-Gigabit link in its collection exceeds 600 Mbps, a warning event is triggered. If the traffic exceeds 800 Mbps, a critical event is triggered.

Baseline thresholds are defined for a configured time of day or week (1 day, 1 week, or 2 weeks). The baseline is created by calculating the average of the statistical results for the configured time each day, week, or every 2 weeks. [Table 11-2](#) shows an example of the statistics used to create the baseline value for a collection defined at 4 pm on a Wednesday.

**Table 11-2** *Baseline Time Periods for a Collection Started on Wednesday at 4pm*

| Baseline Time Window | Statistics Used in Average Calculation |
|----------------------|----------------------------------------|
| 1 day                | Every prior day at 4 pm                |
| 1 week               | Every prior Wednesday at 4 pm          |
| 2 weeks              | Every other prior Wednesday at 4 pm    |

Baseline thresholds create a threshold that adapts to the typical traffic pattern for each link for the same time window each day, week, or every 2 weeks. Baseline thresholds are set as a percent of the average (110% to 500%), where 100% equals the calculated average.

As an example, a collection is created at 4 pm on Wednesday, with baseline thresholds set for 1 week, at 150% of the average (warning) and 200% of the average (critical). Performance Manager recalculates the average for each link at 4 pm every Wednesday by taking the statistics gathered at that time each Wednesday since the collection started. Using this as the new average, Performance Manager compares each received traffic statistic against this value and sends a warning or critical event if the traffic on a link exceeds this average by 150% or 200% respectively.

[Table 11-3](#) shows two examples of 1-Gigabit links with different averages in our example collection and at what traffic measurements the Warning and Critical events are sent.

**Table 11-3** *Example of Events Generated for 1-Gigabit Links*

| Average  | Warning Event Sent at 150% | Critical Event Sent at 200% |
|----------|----------------------------|-----------------------------|
| 400 Mbps | 600 Mbps                   | 800 Mbps                    |
| 200 Mbps | 300 Mbps                   | 400 Mbps                    |

Set these thresholds on the last screen of the Collections Configuration Wizard by checking the **Send events if traffic exceeds threshold** check box.

## Using the Performance Manager Configuration Wizard

See the [“Creating Performance Collections”](#) section on page 7-61.

## Viewing Statics Using Fabric Manager

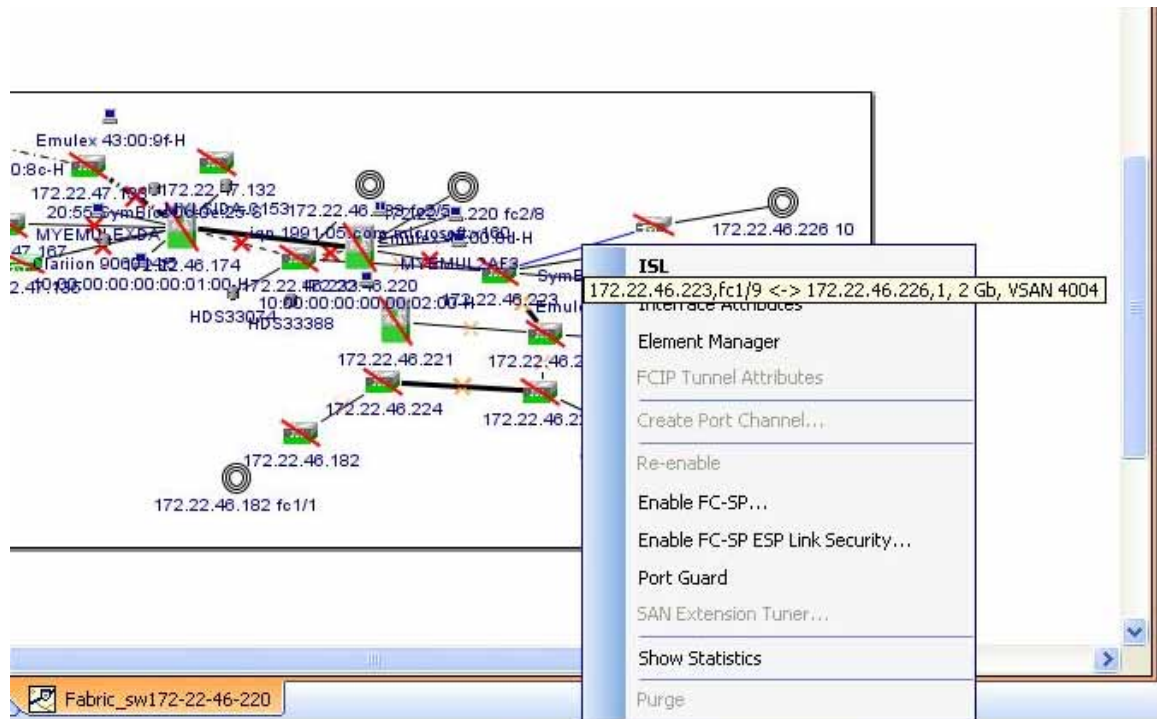
You can configure Fabric Manager to gather historic and real time statistics of ISLs or End devices. These statistics include receive and transmit utilization, bytes per second, as well as errors and discards per ISL or end device.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

To view the historic and real-time statistics of ISLs or end devices using Fabric Manager, follow these steps:

- Step 1** Right-click the ISL or end device in the Fabric pane.  
You see a context menu as shown in the [Figure 11-4](#).
- Step 2** Select **Show Statics**.

**Figure 11-4** Show Statics Menu



**Note** Show Statics menu will be enabled only if you add the fabric to the Performance Manager collection.

## Viewing Performance Manager Reports

You can view Performance Manager statistical data using preconfigured reports that are built on demand and displayed in a web browser. These reports provide summary information as well as detailed statistics that can be viewed for daily, weekly, monthly, or yearly results.

Choose **Performance > Reports** to access Performance Manager reports from Fabric Manager. This opens a web browser window showing the default Fabric Manager web client event summary report. Click the **Performance** tab to view the Performance Manager reports. Performance Manager begins reporting data ten minutes after the collection is started.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*



Note

Fabric Manager Web Server must be running for reports to work. See the “[Launching Fabric Manager Web Client](#)” section on page 7-7.

## Performance Summary

The Performance Summary page presents a dashboard display of the throughput and link utilization for hosts, ISLs, storage, and flows for the last 24-hour period. The summary provides a quick overview of the fabric’s bandwidth consumption and highlights any hotspots.

The report includes network throughput pie charts and link utilization pie charts. Use the navigation tree on the left to show summary reports for monitored fabrics or VSANs. The summary displays charts for all hosts, storage elements, ISLs, and flows. Each pie chart shows the percent of entities (links, hosts, storage, ISLs, or flows) that measure throughput or link utilization on each of six predefined ranges. Move the mouse over a pie chart section to see how many entities exhibit that range of statistics. Double-click any pie chart to bring up a table of statistics for those hosts, storage elements, ISLs, or flows.

## Performance Tables and Details Graphs

Click **Host**, **Storage**, **ISL**, or **Flow** to view traffic over the past day for all hosts, storage, ISLs, or flows respectively. A table lists all of the selected entities, showing transmit and receive traffic and errors and discards, if appropriate. The table can be sorted by any column heading. The table can also be filtered by day, week, month, or year. Tables for each category of statistics display average and peak throughput values and provide hot-links to more detailed information.

Clicking a link in any of the tables opens a details page that shows graphs for traffic by day, week, month, and year. If flows exist for that port, you can see which storage ports sent data. The details page also displays graphs for errors and discards if they are part of the statistics gathered and are not zero.

If you double-click a graph on a Detail report, it will launch the Cisco Traffic Analyzer for Fibre Channel, if configured. The aliases associated with hosts, storage devices, and VSANs in the fabric are passed to the Cisco Traffic Analyzer to provide consistent, easy identification.

## Viewing Performance of Host-Optimized Port Groups

You can monitor the performance of host-optimized port groups by selecting **Performance > End Devices** and selecting **Port Groups** from the Type drop-down list.

## Viewing Performance Manager Events

Performance Manager events are viewed through Fabric Manager Web Server. To view problems and events in Fabric Manager Web Server, choose a fabric and then click the **Events** tab to see a summary or detailed report of the problems and events that have occurred in the selected fabric.

## Generating Top10 Reports in Performance Manager

You can generate historical Top10 reports that can be saved for later review. These reports list the entities from the data collection, with the most active entities appearing first. This is a static, one-time only report that generates averages and graphs of the data collection as a snapshot at the time the report is

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

generated. These Top10 reports differ from the other monitoring tables and graphs in Performance Manager in that the other data is continuously monitored and is sortable on any table column. The Top10 reports are a snapshot view at the time the report was generated and are static. These are one-time reports that generate averages and graphs of the data collection as a snapshot at the time the report is generated.



#### Tip

Name the reports with a timestamp so that you can easily find the report for a given day or week.

These Top10 reports differ from the other monitoring tables and graphs in Performance Manager in that the other data is continuously monitored and is sortable on any table column. The Top10 reports are a snapshot view at the time the report was generated.



#### Note

Top10 reports require analyzing the existing data over an extended period of time and can take hours or more to generate on large fabrics.

See the [“Creating a Custom Report Template”](#) section on page 7-39 for information on creating a Top10 report.

## Generating Top10 Reports Using Scripts

You can generate Top10 reports manually by issuing the following commands:

- On UNIX, run the script:

```
"/<user_directory>/cisco_mds9000/bin/pm.sh display pm/pm.xml <output_directory>"
```

- On Windows, run the script:

```
"c:\Program Files\Cisco Systems\MDS 9000\bin\pm.bat display pm\pm.xml  
<output_directory>"
```

On UNIX, you can automate the generation of the Top10 reports on your Fabric Manager Server host by adding the following cron entry to generate the reports once an hour:

```
0 * * * * /<user_directory>/cisco_mds9000/bin/pm.sh display pm/pm.xml <output_directory>
```

If your crontab does not run automatically or Java complains about an exception similar to [Example 11-1](#), you need to add “-Djava.awt.headless=true” to the JVMARGS command in /<user\_directory>/cisco\_mds9000/bin/pm.sh.

### Example 11-1 Example Java Exception

```
in thread "main" java.lang.InternalError Can't connect to X11 window server using '0.0' as  
the value of the DISPLAY variable.
```

## Exporting Data Collections to XML Files

The RRD files used by Performance Manager can be exported to a freeware tool called rrdtool. The rrd files are located in pm/db on the Fabric Manager Server. To export the collection to an XML file, enter the following command at the operating system command-line prompt:

```
/bin/pm.bat xport xxx yyy
```

In this command, xxx is the RRD file and yyy is the XML file that is generated. This XML file is in a format that rrdtool is capable of reading with the command:

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

```
rrdtool restore filename.xml filename.rrd
```

You can import an XML file with the command:

```
bin/pm.bat pm restore <xmlFile> <rrdFile>
```

This reads the XML export format that rrdtool is capable of writing with the command:

```
rrdtool xport filename.xml filename.rrd.
```

The **pm xport** and **pm restore** commands can be found on your Fabric Manager Server at bin\PM.bat for Windows platforms or bin/PM.sh on UNIX platforms. For more information on the rrdtool, refer to the following website: <http://www.rrdtool.org>.

## Exporting Data Collections in Readable Format

You can export the RRD files used by Performance Manager to a freeware tool called rrdtool and export the collection to an XML file. Cisco MDS SAN-OS Release 2.1(1a) introduces the inability to export data collections in comma-separated format (CSV). This format can be imported to various tools, including Microsoft Excel. You can export these readable data collections either from the Fabric Manager Web Services menus or in batch mode from the command line on Windows or UNIX. Using Fabric Manager Web Services, you can export one file. Using batch mode, you can export all collections in the pm.xml file.



### Note

Fabric Manager Web Server must be running for this to work. See the “[Launching Fabric Manager Web Client](#)” section on page 7-7.

To export data collections to Microsoft Excel using Fabric Manager Web Server, follow these steps:

- 
- Step 1** Click the **Performance** tab on the main page.  
You see the overview table.
  - Step 2** Click the **Flows** sub-tab.
  - Step 3** Right-click the name of the entity you want to export and select **Export to Microsoft Excel**.  
You see the Excel chart for that entity in a pop-up window.
- 

To export data collections using command-line batch mode, follow these steps:

- 
- Step 1** Go to the installation directory on your workstation and then go to the bin directory.
  - Step 2** On Windows, enter **.\pm.bat export C:\Program Files\Cisco Systems\MDS 9000\pm\pm.xml <export directory>**. This creates the csv file (export.csv) in the *export directory* on your workstation.
  - Step 3** On UNIX, enter **./pm.sh export /usr/local/cisco\_mds9000/pm/pm.xml <export directory>**. This creates the csv file (export.csv) in the *export directory* on your workstation.
- 

When you open this exported file in Microsoft Excel, the following information displays:

- Title of the entity you exported and the address of the switch the information came from.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- The maximum speed seen on the link to or from this entity.
- The VSAN ID and maximum speed.
- The timestamp, followed by the receive and transmit data rates in bytes per second.

## Configuring Performance Manager for Use with Cisco Traffic Analyzer

Performance Manager works in conjunction with the Cisco Traffic Analyzer to allow you to monitor and manage the traffic on your fabric. Using Cisco Traffic Analyzer with Performance Manager requires the following components:

- A configured Fibre Channel Switched Port Analyzer (SPAN) destination (SD) port to forward Fibre Channel traffic.
- A Port Analyzer Adapter 2 (PAA-2) to convert the Fibre Channel traffic to Ethernet traffic.
- Cisco Traffic Analyzer software to analyze the traffic from the PAA-2.

To configure Performance Manager to work with the Cisco Traffic Analyzer, follow these steps:

- 
- Step 1** Set up the Cisco Traffic Analyzer according to the instructions in the *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*.
- Step 2** Get the following three items of information:
- The IP address of the management workstation on which you are running Performance Manager and Cisco Traffic Analyzer.
  - The path to the directory where Cisco Traffic Analyzer is installed.
  - The port that is used by Cisco Traffic Analyzer (the default is 3000).
- Step 3** Start the Cisco Traffic Analyzer.
- Choose **Performance > Traffic Analyzer > Open**.
  - Enter the URL for the Cisco Traffic Analyzer, in the format:  
`http://<ip address>:<port number>`  
*ip address* is the address of the management workstation on which you have installed the Cisco Traffic Analyzer  
*:port number* is the port that is used by Cisco Traffic Analyzer (the default is :3000).
  - Click **OK**.
  - Choose **Performance > Traffic Analyzer > Start**.
  - Enter the location of the Cisco Traffic Analyzer, in the format:  
`D:\<directory>\ntop.bat`  
*D*: is the drive letter for the disk drive where the Cisco Traffic Analyzer is installed.  
*directory* is the directory containing the ntop.bat file.
  - Click **OK**.
- Step 4** Create the flows you want Performance Manager to monitor, using the Flow Configuration Wizard. See the [“Creating a Flow with Performance Manager” section on page 11-4](#)

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 5** Define the data collection you want Performance Manager to gather, using the Performance Manager Configuration Wizard. See the [“Creating a Collection with Performance Manager”](#) section on page 11-4.
- Choose the VSAN you want to collect information for or choose **All VSANs**.
  - Check the types of items you want to collect information for (Hosts, ISLs, Storage Devices, and Flows).
  - Enter the URL for the Cisco Traffic Analyzer in the format:  
`http://<ip address>/<directory>`  
 where:  
*ip address* is the address of the management workstation on which you have installed the Cisco Traffic Analyzer, and *directory* is the path to the directory where the Cisco Traffic Analyzer is installed.
  - Click **Next**.
  - Review the data collection on this and the next section to make sure this is the data you want to collect.
  - Click **Finish** to begin collecting data.

**Note**

Data is not collected for JBOD or for virtual ports. If you change the data collection configuration parameters during a data collection, you must stop and restart the collection process for your changes to take effect.

- Step 6** Choose **Performance > Reports** to generate a report. Performance Manager Web Server must be running. See the [“Launching Fabric Manager Web Client”](#) section on page 7-7. You see Web Services; click **Custom** then select a report template.

**Note**

It takes at least five minutes to start collecting data for a report. Do not attempt to generate a report in Performance Manager during the first five minutes of collection.

- Step 7** Click **Cisco Traffic Analyzer** at the top of the Host or Storage detail pages to view the Cisco Traffic Analyzer information, or choose **Performance > Traffic Analyzer > Open**. The Cisco Traffic Analyzer page will not open unless ntop has been started already.

**Note**

For information on capturing a SPAN session and starting a Cisco Traffic Analyzer session to view it, refer to the *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*.

**Note**

For information on viewing and interpreting your Performance Manager data, see the [“Historical Performance Monitoring”](#) section on page 11-4.

For information on viewing and interpreting your Cisco Traffic Analyzer data, refer to the *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

For performance drill-down, Fabric Manager Server can launch the Cisco Traffic Analyzer in-context from the Performance Manager graphs. The aliases associated with hosts, storage devices, and VSANs are passed to the Cisco Traffic Analyzer to provide consistent, easy identification.

## Analyzing SAN Health

The SAN Health Advisor tool is a utility that used to monitor the performance and collect the statistics. You can perform the following tasks with this tool:

- Run Performance Monitor to collect I/O statistics
- Collect fabric inventory (switches and other devices)
- Create a graphical layout of fabric topology
- Create reports of error conditions and statistical data

You can install this tool at any SAN environment to collect I/O statistics for the specified time (usually 24 hours), generate health reports and automatically send reports to the designated system administrator for review at regular intervals.

When you start SAN Health Advisor tool, it runs in wizard mode, and prompts for inputs such as seed switch credentials, IP address of the server to which the data to be sent and all the necessary information for the software setup. As soon as the fabric is discovered, the tool starts capturing performance data, I/O statistics and error conditions.

The reports generated from the collection is stored in the **\$INSTALLDIR/dcm/fm/reports** directory. These reports are automatically sent to the designated SAN administrator for review. In a situation where the tool fails to collect the data, it generates a report with an error message or exception. After sending the reports the tool automatically uninstalls itself and terminates all the processes that it established on the host machine.

The report that SAN Health Advisor tool generates will have the following details:

- Events
- System messages
- Analysis of connectivity
- Zone discrepancy
- System configuration
- Interface status
- Domain information
- Security settings

## Installing the SAN Health Advisor Tool

SAN Health Advisor tool can be installed and run on Windows, UNIX, and Solaris platforms. Install the package that contains the .jar file with JRE version 6.0.



**Note** The SAN Health tool is not installed by default when you install Fabric Manager software.

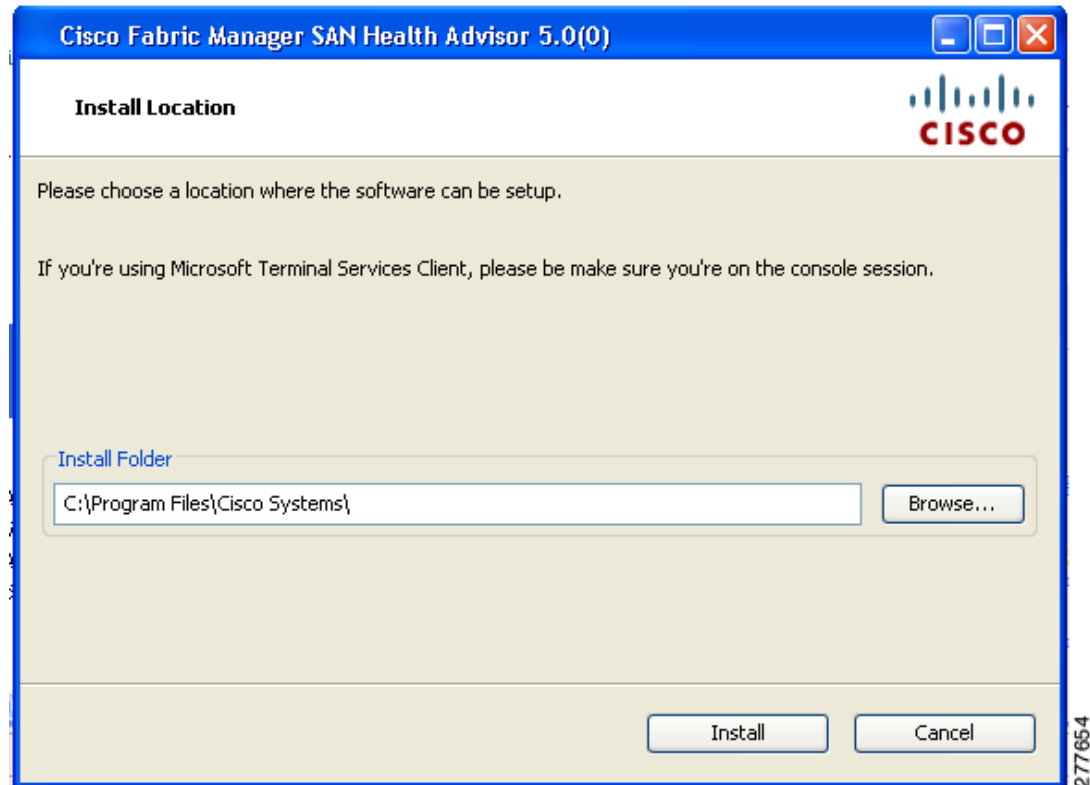


*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

To install the SAN Health Advisor tool on Windows, follow these steps:

- Step 1** Double-click the San Health Advisor tool installer.  
You see the San Health Advisor tool Installer window as shown in [Figure 11-5](#).

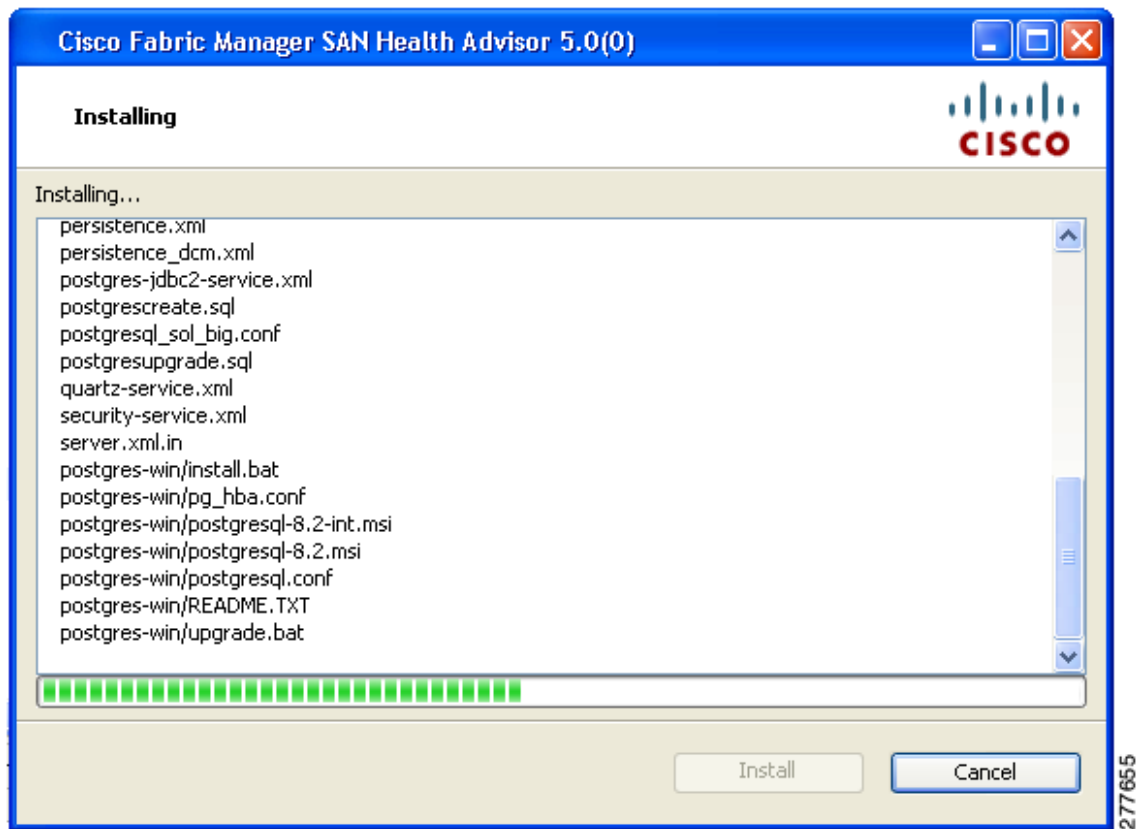
**Figure 11-5** SAN Health Advisor: Installer



- Step 2** Select an installation folder on your workstation for SAN Health Advisor.  
On Windows, the default location is **C:\Program Files\Cisco Systems\**.
- Step 3** Click **Install** to start the installation.  
You see the installation progressing as shown in [Figure 11-6](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 11-6 SAN Health Advisor: Installation in Progress**



You see the Fabric Options dialog box as shown in [Figure 11-7](#)

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 11-7 SAN Health Advisor: Fabric Options**

**Cisco Fabric Manager SAN Health Advisor 5.0(0)**

**Fabric Options**  
Please enter the IP address of at least one fabric seed switch and provide its SNMP credential.

Seed Switch:

Seed Switch 2 (Optional):

SNMPv3 Username:

SNMPv3 Password:

Auth-Privacy: MD5

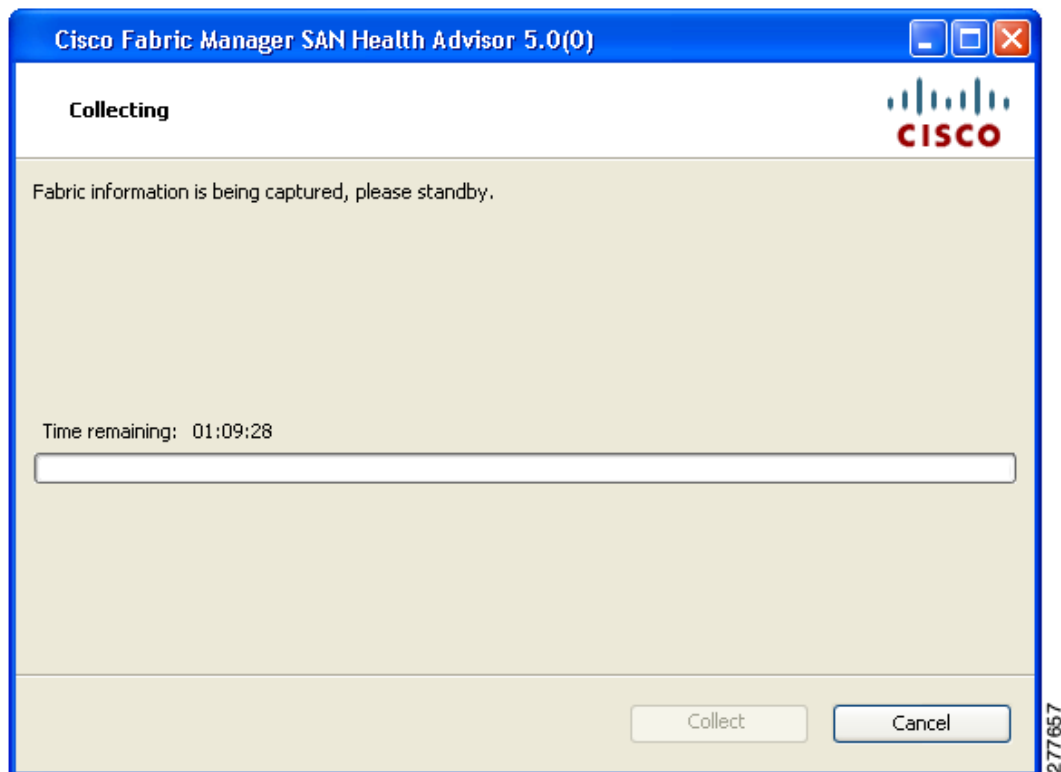
Performance Collection: ☐ (Performance Collection will run for 24 hours)

277656

- Step 4** In the **Seed Switch** text box, enter the IP address of the seed switch.
- Step 5** Enter the user name and password for the switch.
- Step 6** Select the authentication privacy option from the **Auth-Privacy** drop-down list box.
- Step 7** Click the **Performance Collection** check box to enable the process to run for 24 hours.
- Step 8** Click **Collect** to start gathering performance information.
- You see the collecting dialog box as shown in [Figure 11-8](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

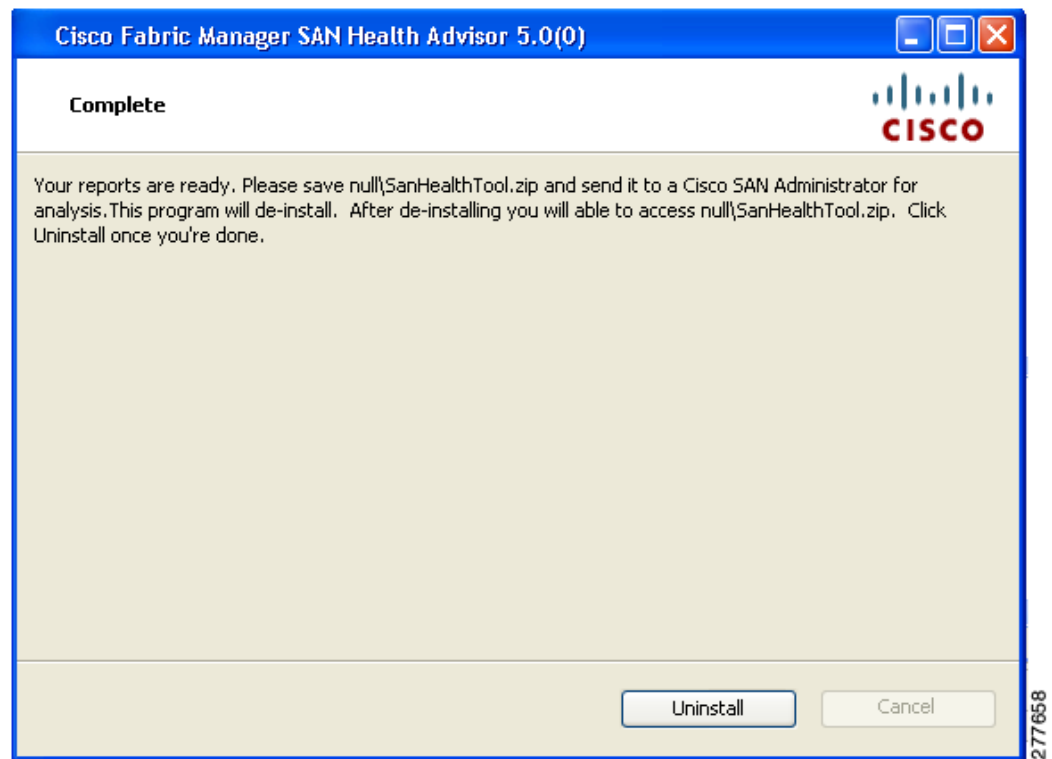
**Figure 11-8** SAN Health Advisor: Collecting



If you want to stop gathering information in the middle of the process, click Cancel. You see the message indicating performance collection is complete as shown in [Figure 11-9](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 11-9** SAN Health Advisor: Performance Collection Complete



**Step 9** Click **Uninstall** to remove the SAN Health Advisor software.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*



# CHAPTER 12

## Software Images

---

This chapter describes how to install and upgrade Cisco MDS software images. It includes the following sections:

- [About Software Images, page 12-1](#)
- [Essential Upgrade Prerequisites, page 12-3](#)
- [Software Upgrade Methods, page 12-5](#)
- [Automated Upgrades, page 12-6](#)
- [Using the Software Install Wizard, page 12-8](#)
- [Nondisruptive Upgrades on Fabric and Modular Switches, page 12-15](#)
- [Maintaining Supervisor Modules, page 12-16](#)
- [Installing Generation 2 Modules in Generation 1 Chassis, page 12-18](#)
- [Replacing Modules, page 12-18](#)
- [Default Settings, page 12-19](#)

## About Software Images

Each switch is shipped with a Cisco MDS NX-OS or SAN-OS operating system for Cisco MDS 9000 Family switches. The Cisco MDS NX-OS consists of two images—the kickstart image and the system image. To upgrade the switch to a new image, you must specify the variables that direct the switch to the images.

- To select the kickstart image, use the KICKSTART variable.
- To select the system image, use the SYSTEM variable.

The images and variables are important factors in any install procedure. You must specify the variable and the image to upgrade your switch. Both images are not always required for each install.



**Note**

Unless explicitly stated, the software install procedures in this chapter apply to any switch in the Cisco MDS 9000 Family.

## Dependent Factors for Software Installation

The software image install procedure is dependent on the following factors:

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Software images—The kickstart and system image files reside in directories or folders that can be accessed from the Cisco MDS 9000 Family switch prompt.
- Image version—Each image file has a version.
- Flash disks on the switch—The bootflash: resides on the supervisor module and the CompactFlash disk is inserted into the slot0: device.
- Supervisor modules—There are single or dual supervisor modules.

## Selecting the Correct Software Images for Cisco MDS 9100 Series Switches

The Supervisor-1 and Supervisor-2 modules supported by Cisco MDS 9100 Series switches require different system and kickstart images. You can determine which images to use on your switch by the naming conventions shown in [Table 12-1](#) and [Table 12-2](#).

**Table 12-1 Supervisor Module Software Image Naming Conventions for MDS 9100 Series**

| Cisco MDS 9100 Series Switch Type                                                                          | Supervisor Module Type | Naming Convention                |
|------------------------------------------------------------------------------------------------------------|------------------------|----------------------------------|
| 9124, 9124e, 9134, Cisco Fabric Switch for HP c-Class BladeSystem, Cisco Fabric Switch for IBM BladeCenter | Supervisor-2 module    | Filename begins with m9100-s2ek9 |

**Table 12-2 Software Image Naming Conventions for MDS 9100 Series**

| Cisco MDS 9100 Series Switch Type       | Supervisor Module Type | Naming Convention                 |
|-----------------------------------------|------------------------|-----------------------------------|
| Cisco MDS 9148 Multilayer Fabric Switch | Supervisor-2 module    | Filename begins with m9100-s3ek9. |
| Cisco MDS 9124 Multilayer Fabric Switch | Supervisor-2 module    | Filename begins with m9100-s3ek9. |

## Selecting the Correct Software Images for Cisco MDS 9200 Series Switches

The Supervisor-1 and Supervisor-2 modules supported by Cisco MDS 9200 Series switches require different system and kickstart images. You can determine which images to use on your switch by the naming conventions shown in [Table 12-3](#).

**Table 12-3 Supervisor Module Software Image Naming Conventions for MDS 9200 Series**

| Cisco MDS 9200 Series Switch Type | Supervisor Module Type | Naming Convention                |
|-----------------------------------|------------------------|----------------------------------|
| 9222i                             | Supervisor-2 module    | Filename begins with m9200-s2ek9 |
| 9216, 9216A or 9216i              | Supervisor-1 module    | Filename begins with m9200-s1ek9 |



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Selecting the Correct Software Images for Cisco MDS 9500 Family Switches

The Supervisor-1 and Supervisor-2 modules supported by Cisco MDS 9500 Family switches require different system and kickstart images. You can determine which images to use on your switch by the naming conventions shown in [Table 12-4](#).

**Table 12-4 Supervisor Module Software Image Naming Conventions for MDS 9500 Series**

| Cisco MDS 9500 Series Switch Type | Supervisor Module Type | Naming Convention                 |
|-----------------------------------|------------------------|-----------------------------------|
| 9513                              | Supervisor-2 module    | Filename begins with m9500-sf2ek9 |
| 9506 or 9509                      | Supervisor-2 module    | Filename begins with m9500-sf2ek9 |

## Essential Upgrade Prerequisites



### Note

During a software upgrade to Cisco SAN-OS 3.1(3), the CompactFlash CRC Checksum test runs automatically in the background. All modules that are online are tested and the installation stops if any modules are running with a faulty CompactFlash. When this occurs, the switch can not be upgraded until the situation is corrected. A system message displays the module information and indicates that you must issue the **system health cf-crc-check module** CLI command to troubleshoot. For descriptions of new commands supported by the CompactFlash checksum feature, refer to the *Cisco MDS 9000 Family Command Reference*.

Before attempting to migrate to any software image version, follow these guidelines:

- Customer Service

Before performing any software upgrade, contact your respective customer service representative to review your software upgrade requirements and to provide recommendations based on your current operating environment.



### Note

If you purchased Cisco support through a Cisco reseller, contact the reseller directly. If you purchased support directly from Cisco Systems, contact Cisco Technical Support at this URL: <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

- Scheduling

Schedule the upgrade when the fabric is stable and steady. Ensure that everyone who has access to the switch or the network is not configuring the switch or the network during this time. All configurations are disallowed at this time.

- Space

Verify that sufficient space is available in the location where you are copying the images. This location includes the active and standby supervisor module bootflash: (internal to the switch).

- Standby supervisor module bootflash: file system.
- Internal bootflash: offers approximately 200 MB of user space.

- Hardware

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

Avoid power interruption during any install procedure. These kinds of problems can corrupt the software image.

- Connectivity (to retrieve images from remote servers)
  - Configure the IPv4 address or IPv6 address for the 10/100/1000 BASE-T Ethernet port connection (interface mgmt0).



**Note** 1000 BASE-T Ethernet is only available on Supervisor-2 modules.

- Ensure the switch has a route to the remote server. The switch and the remote server must be in the same subnetwork if you do not have a router to route traffic between subnets.
- Images
  - Ensure that the specified system and kickstart images are compatible with each other.
  - If the kickstart image is not specified, the switch uses the current running kickstart image.
  - If you specify a different system image, ensure that it is compatible with the running kickstart image.
  - Retrieve images in one of two ways:
    - Local file—Images are locally available on the switch.
    - Network file—Images are in a remote location and the user specifies the destination using the remote server parameters and the file name to be used locally.
- Terminology

[Table 12-5](#) summarizes terms used in this chapter with specific reference to the install and upgrade process.

**Table 12-5 Terms Specific to This Chapter**

| Term         |           | Definition                                                            |
|--------------|-----------|-----------------------------------------------------------------------|
| bootable     |           | The modules ability to boot or not boot based on image compatibility. |
| impact       |           | The type of software upgrade mechanism—disruptive or nondisruptive.   |
| install-type | reset     | Resets the module.                                                    |
|              | sw-reset  | Resets the module immediately after switchover.                       |
|              | rolling   | Upgrades each module in sequence.                                     |
|              | copy-only | Updates the software for BIOS, loader, or bootrom.                    |

- Tools
  - Verify connectivity to the remote server by clicking **Verify Remote Server** in the Software Install Wizard in Fabric Manager.
  - Ensure that the required space is available for the image files to be copied by using Software Install Wizard to check free disk space.
  - We recommend the Software Install Wizard in Fabric Manager to upgrade your software. This wizard upgrades all modules in any Cisco MDS 9000 Family switch (see the [“Benefits of Using the Software Install Wizard”](#) section on page 12-6).
  - Run only one installation on a switch at any time.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Do not issue another command while running the installation.
- Do the installation on the active supervisor module, not the standby supervisor module.

**Note**

Prior to Cisco SAN-OS Release 3.0, to preserve the FC IDs in your configuration, verify that the persistent FC ID feature is enabled before rebooting. This feature is enabled by default. In earlier releases, the default is disabled.

## Software Upgrade Methods

You can upgrade software without any disruptions using the Cisco MDS NX-OS software designed for mission-critical high availability environments. To realize the benefits of nondisruptive upgrades on the Cisco MDS 9500 Directors, we highly recommend that you install dual supervisor modules.

You can upgrade any switch in the Cisco MDS 9000 Family using one of the following methods:

- Automatic—You can use the Fabric Manager Software Install Wizard for Cisco MDS NX-OS switches as described in the [“Using the Software Install Wizard” section on page 12-8](#).
- Manual—For information on manual upgrades, see the *Cisco MDS 9020 Switch Configuration Guide and Command Reference*.

In some cases, regardless of which process you use, the software upgrades may be disruptive. These exception scenarios can occur under the following conditions:

- A single supervisor module system with kickstart or system image changes.
- A dual supervisor module system with incompatible system software images.

**Note**

For high availability, you need to connect the ethernet port for both active and standby supervisors to the same network or virtual LAN. The active supervisor owns the one IP address used by these Ethernet connections. On a switchover, the newly activated supervisor takes over this IP address.

## Determining Software Compatibility

If the running image and the image you want to install are incompatible, the software reports the incompatibility. In some cases, you may decide to proceed with this installation. If the active and the standby supervisor modules run different versions of the image, both images may be HA compatible in some cases and incompatible in others.

Compatibility is established based on the image and configuration:

- Image incompatibility—The running image and the image to be installed are not compatible.
- Configuration incompatibility—There is a possible incompatibility if certain features in the running image are turned off as they are not supported in the image to be installed. The image to be installed is considered incompatible with the running image if one of the following statements is true:
  - An incompatible feature is enabled in the image to be installed and it is not available in the running image and may cause the switch to move into an inconsistent state. In this case, the incompatibility is *strict*.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- An incompatible feature is enabled in the image to be installed and it is not available in the running image and does not cause the switch to move into an inconsistent state. In this case, the incompatibility is *loose*.



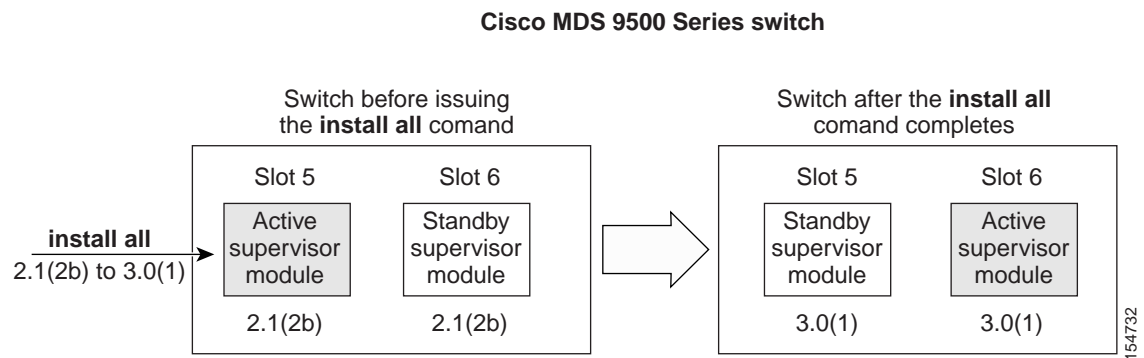
**Tip**

The **Software Install Wizard** compares and presents the results of the compatibility before proceeding with the installation. You can exit if you do not want to proceed with these changes.

## Automated Upgrades

The Software Install Wizard upgrades all modules in any Cisco MDS 9000 Family switch. [Figure 12-1](#) provides an overview of the switch status before and after using Software Install Wizard.

**Figure 12-1**      *The Effect of the Software Install Wizard*



The Software Install Wizard automatically verifies if the standby supervisor module is functioning (if present). If it is not functioning, it reloads that module and uses the **force download** option to force it to function.

## Benefits of Using the Software Install Wizard

The Software Install Wizard provides the following benefits:

- You can upgrade the entire switch using just one procedure command.
- You can receive descriptive information on the intended changes to your system before you continue with the installation.
- You can upgrade the entire switch using the least disruptive procedure.
- You can see the progress of this command on the console, Telnet, and SSH screens:
  - After a switchover process, you can see the progress from both the supervisor modules.
  - Before a switchover process, you can only see the progress from the active supervisor module.
- The Software Install Wizard automatically checks the image integrity. This includes the running kickstart and system images.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- The Software Install Wizard performs a platform validity check to verify that a wrong image is not used. For example, to check if an MDS 9500 Series image is used inadvertently to upgrade an MDS 9200 Series switch.
- After issuing the installation, if any step in the sequence fails, the wizard completes the step in progress and ends.

For example, if a switching module fails to be updated for any reason (for example, due to an unstable fabric state), then the command sequence disruptively updates that module and ends. In such cases, you can verify the problem on the affected switching module and upgrade the other switching modules.

## Recognizing Failure Cases

The following situations cause the installation to end:

- If the standby supervisor module bootflash: file system does not have sufficient space to accept the updated image.
- If the specified system and kickstart images are not compatible.
- If the fabric or switch is configured while the upgrade is in progress.
- If a module is removed while the upgrade is in progress.
- If the switch has any power disruption while the upgrade is in progress.
- If the entire path for the remote location is not specified accurately.
- If images are incompatible after an upgrade. For example, a switching module image may be incompatible with the system image, or a kickstart image may be incompatible with a system image. This is also identified by the Software Install Wizard compatibility check.



### Caution

If the installation is ended, be sure to verify the state of the switch at every stage and reissue the command after 10 seconds. If you reissue the installation within the 10-second span, it is rejected with an error message indicating that an installation is currently in progress.



### Tip

All configurations are disallowed while the installation is in progress. However, configurations coming through the CFS applications are allowed and may affect the upgrade procedure.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Using the Software Install Wizard

You can use the Software Install Wizard to install Cisco NX-OS images on supported switches.



**Note**

The Software Install Wizard supports installation and upgrade for Cisco MDS 9020 Fabric Switch or Cisco FabricWare. For successful installation and upgrade, specify the TFTP server address that the Cisco MDS 9020 Fabric Switch should use.



**Note**

Before you use this wizard, be sure the standby supervisor management port is connected.

To use the Software Install Wizard, follow these steps:

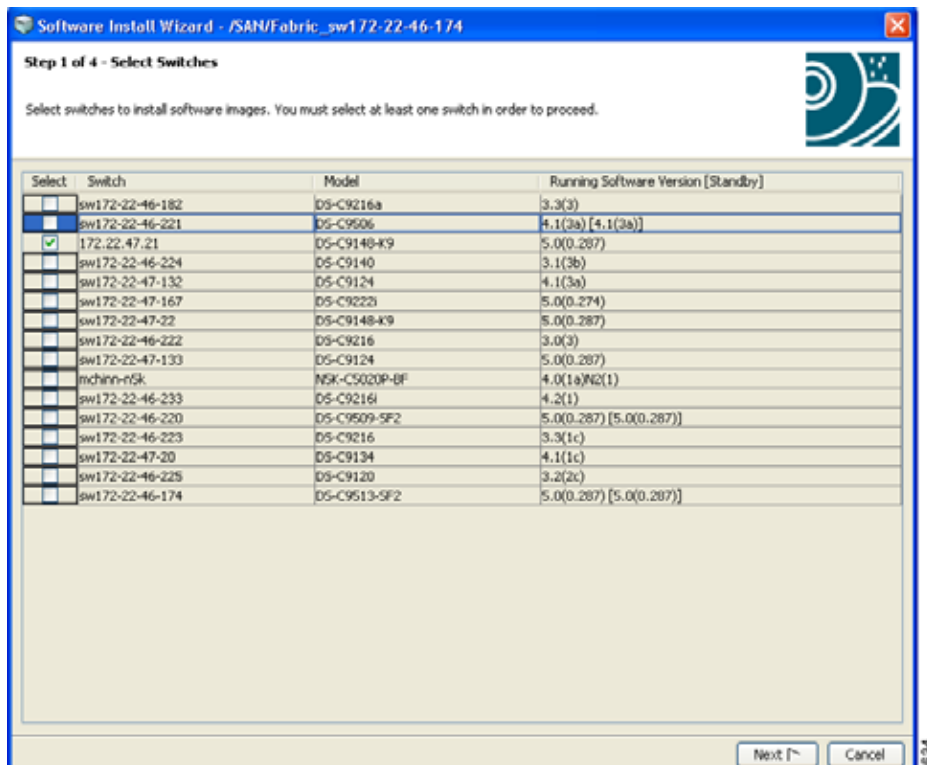
- Step 1** Click the Software Install Wizard icon in the toolbar (see [Figure 12-2](#)).

**Figure 12-2** Software Install Wizard Icon



You see the Select Switches dialog box with all switches selected by default.

**Figure 12-3** Select Switches Dialog Box



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 2** Deselect the check box for the switch(es) for which you do not want to install images on. You must have at least one switch selected to proceed (see [Figure 12-3](#)).
- Step 3** Click **Next** when finished.
- Step 4** (Optional) Check the **Skip Image Download** check box and click **Next** to use images that are already downloaded (the file is already on the bootflash). Proceed to [Step 11](#).

You see the Specify Software Image(s) by Model Dialog Box shown in [Figure 12-4](#).

**Figure 12-4 Specify Software Image(s) by Model Dialog Box**

**Software Install Wizard - /SAN/Fabric\_MDS9509**

**Step 2 of 4 - Specify Software Image(s) by Model**

For each switch model, specify the new images to use. You must specify at least one image for each model by double-clicking on the table cell. The total space required on the bootflash to copy the image is shown in the 'Required Flash Space' column. To use images that are already downloaded, check 'Skip Image Download'. Press 'Verify' to validate remote server settings and filenames (SSHv2 only); be patient, this can take awhile. Please manually copy ssi image to switch.

☐ Use Saved Settings (displayed settings will be saved when mouse click "Next" button)

Transfer files from: ☐ Local FM TFTP ☒ Remote

**Remote Options**

Copy Files Via: ☐ TFTP ☒ SFTP ☐ SCP ☐ FTP

Server:

UserName:

Password:

Flash Space:  1,512 MB

**Image(s)**

Version String:  e.g. 4.2.1 for 4.2(1)

Image Path:

| Model        | System                        | Kickstart                             | Ssi |
|--------------|-------------------------------|---------------------------------------|-----|
| DS-C9100-S2  | m9100-s2ek9-mz.4.2.1.bin.S20  | m9100-s2ek9-kickstart-mz.4.2.1.bi...  |     |
| DS-C9500-SF2 | m9500-sf2ek9-mz.4.2.1.bin.S20 | m9500-sf2ek9-kickstart-mz.4.2.1.bi... |     |

☐ Skip Image Download

- Step 5** Click the **Use Saved Settings** check box to save the settings you specify. These settings will be saved for future use when you click Next.
- Step 6** Click the radio button for either:
- Local FM TFTP** to transfer files from local computer.
  - Remote** to transfer files from a remote computer.
- Step 7** If you select Local FM TFTP, proceed to [Step 10](#).
- Step 8** If you select Remote, click one of the Copy Files Via radio buttons transfers files (SFTP, SCP, FTP).
- Step 9** Enter the server name, user name and password.
- Step 10** Enter the version and the image path and then click **Apply**.



**Note**

You can manually provide the file name, if you had chosen **Local FM TFTP** in step 6. To do that you may double-click the table, and choose the file from the Open dialog box or manually type the file name in the cell under system.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

When you enter the version string and image path, Fabric Manager tries to retrieve the default file name and calculate the flash space required to accommodate the image file. Version string should be the current version of the version to be installed. Image path is the path to locate the software image as shown in the following example:

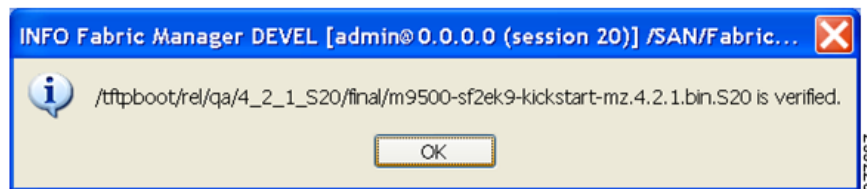
```
Image URI: /tftpboot/rel/qa/5_0_0_201/gdb/m9500-sf2ek9-mzg.5.0.0.201.bin.S2
Path - /tftpboot/rel/qa/5_0_0_201/gdb
Version String - 5.0.0.201.S2
```

**Step 11** Click the row under the System, Kickstart or SSI columns to enter image URIs. You must specify at least one image for each switch to proceed.

**Step 12** Click **Verify Remote Server and Path**.

Fabric Manager will validate the file path and server credentials. You see the output as shown in [Figure 12-5](#)

**Figure 12-5 Validation Result**



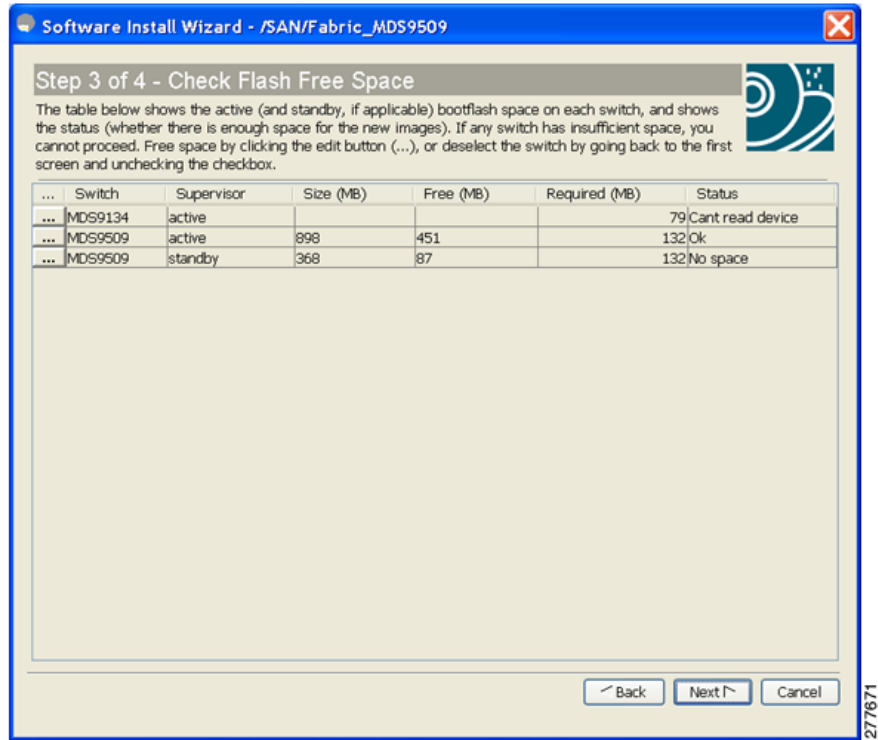
**Step 13** Click **OK** and then click **Next** in the Specify Software Images by Model dialog box.

You see the Check Flash Free Space dialog box (see [Figure 12-6](#)). This dialog box shows the active (and standby, if applicable) bootflash space on each switch, and shows the status (whether there is enough space for the new images). If any switch has insufficient space, you cannot proceed. Deselect the switch without enough bootflash by going back to the first screen and unchecking the check box for that switch.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 12-6** Check Flash Free Space Dialog Box

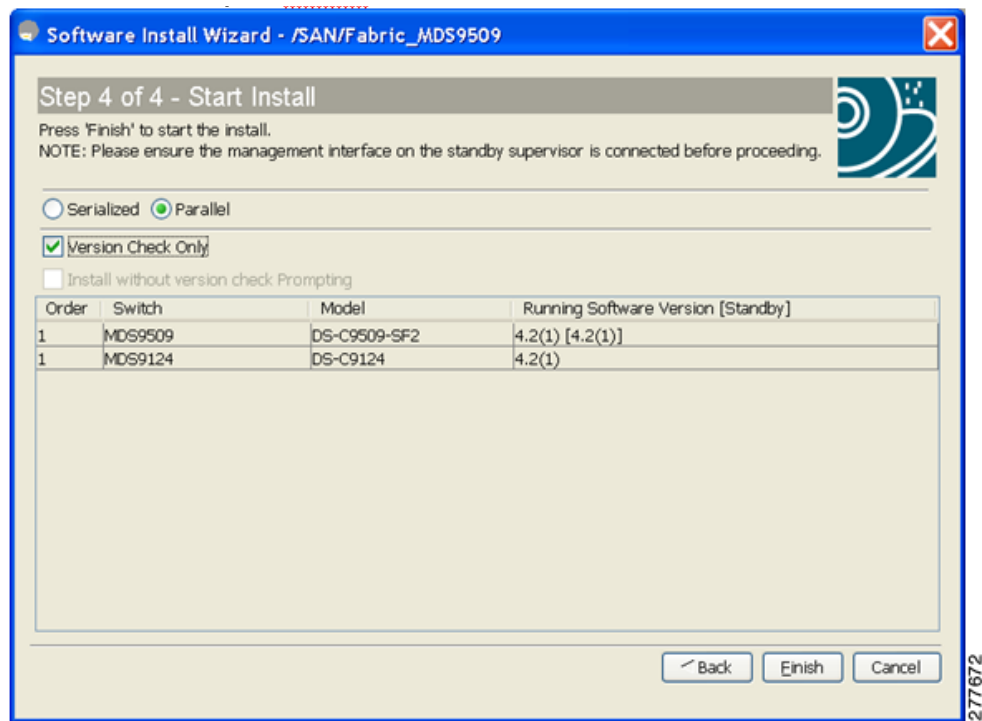


**Step 14** Click **Next**.

You see the Start Install dialog box shown in [Figure 12-7](#).

**Figure 12-7** Start Install Dialog Box

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

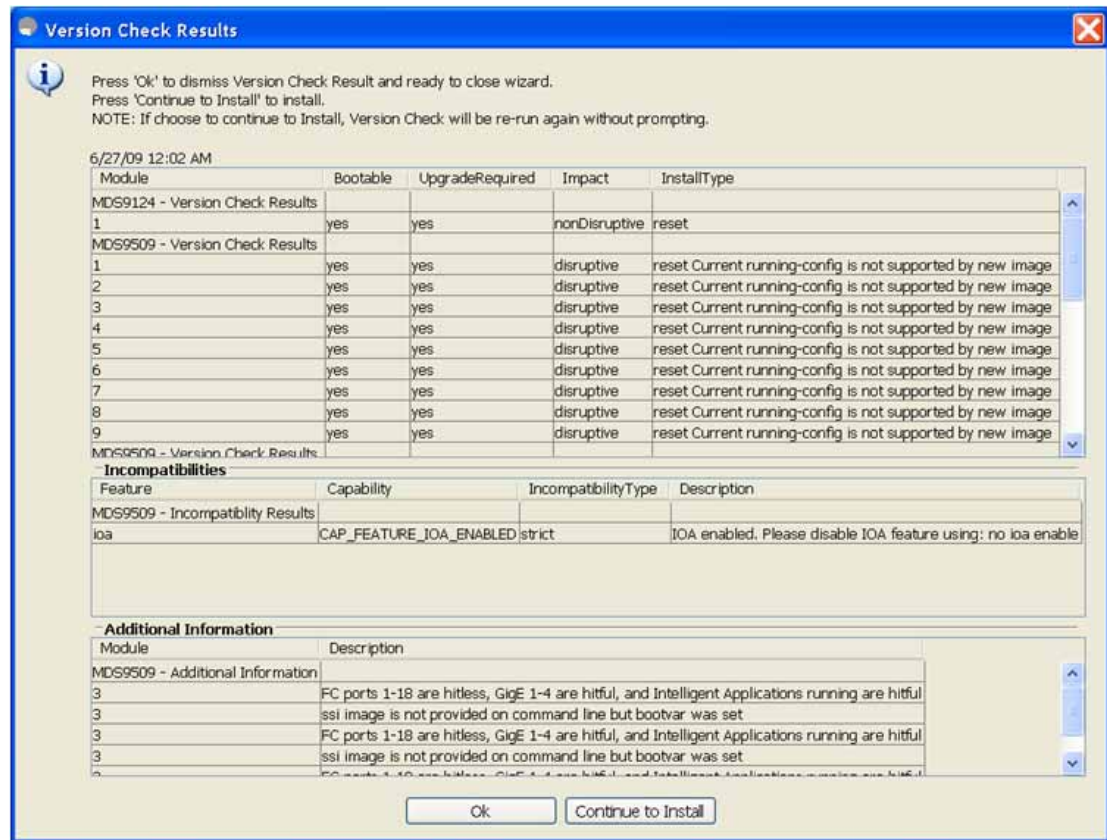


**Note** There is no limit on the number of switches you can upgrade.

- Step 15** Click one of the the radio buttons:
- Serialized** to upgrade one switch at a time.
  - Parallel** to simultaneously upgrade multiple switches.
- Step 16** (Optional) Check the **Version Check Only** check box to complete the version check first and then prompt for your input to continue with installation.
- Step 17** (Optional) Click **Finish** to start installation.
- You see the Version Check Results dialog box shown in [Figure 15-8](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 12-8** Version Check Results Dialog box



- Step 18** (Optional) Check the **Install without Version check Prompting** check box to continue with the installation.



**Note**

The version check provides information about the impact of the upgrade for each module on the switch. It also shows any incompatibilities that might result. You see a final dialog box at this stage, prompting you to confirm that this check should be performed. We recommend that you do not ignore the version check results.



**Caution**

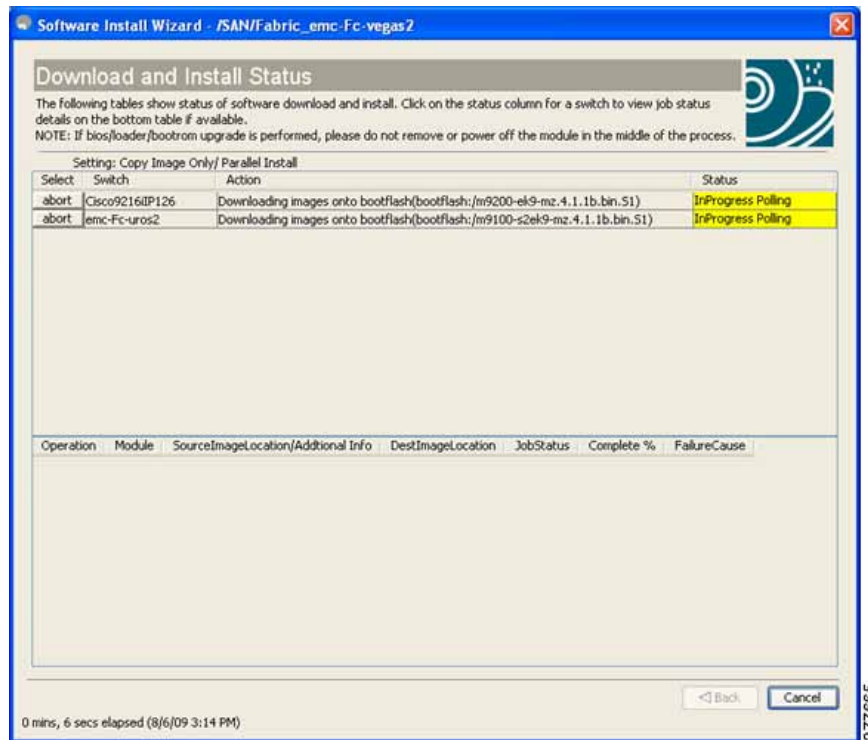
If **Install without Version check Prompting** is checked, the upgrade will proceed even if the current switch version is newer than the version you are installing.

- Step 19** Click **OK** to close the wizard.
- Step 20** Click **Continue to install** to start the installation.

You see the Download and Install Status dialog box shown in [Figure 12-9](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 12-9** Download and Install Status Dialog Box



**Note**

On hosts where the TFTP server cannot be started, a warning is displayed. The TFTP server may not start because an existing TFTP server is running or because access to the TFTP port 69 has been denied for security reasons (the default setting on Linux). In these cases, you cannot transfer files from the local host to the switch.



**Note**

Before exiting the session, be sure the upgrade process is complete. The wizard will display a status as it goes along. Check the lower left-hand corner of the wizard for the status message Upgrade Finished. First, the wizard displays the message Success followed a few seconds later by InProgress Polling. Then the wizard displays a second message Success before displaying the final Upgrade Finished.

## Upgrading Services Modules

Any Fibre Channel switching module supports nondisruptive upgrades. The 14/2-port Multiprotocol Services (MPS-14/2)) module supports nondisruptive upgrades for the Fibre Channel ports. Any software upgrade for the two Gigabit Ethernet ports in this module is disruptive.

Any software upgrade for the Caching Services Module (CSM) and the IP Storage (IPS) services modules is disruptive.

CSMs and IPS modules use a rolling upgrade install mechanism to guarantee a stable state for each module in the switch:

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Each IPS module in a switch requires a 5-minute delay before the next IPS module is upgraded.
- Each CSM module requires a 30-minute delay before the next CSM module is upgraded. See the *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide* for more information on CSMs.

## Nondisruptive Upgrades on Fabric and Modular Switches

This section describes how to perform nondisruptive upgrades on the following Cisco Fabric Switches:

- Cisco MDS 9124 Multilayer Fabric Switch
- Cisco MDS 9134 Multilayer Fabric Switch
- Cisco MDS 9222i Multiservice Modular Switch
- Cisco Fabric Switch for HP c-Class BladeSystem
- Cisco Fabric Switch for IBM BladeCenter

This section includes the following topics:

- [Preparing for a Nondisruptive Upgrade on Fabric and Modular Switches, page 12-15](#)
- [Performing a Nondisruptive Upgrade on a Fabric Switch, page 12-16](#)

## Preparing for a Nondisruptive Upgrade on Fabric and Modular Switches

You can upgrade software on the following without any disruptions using the Software Install Wizard for the system software images.

- Cisco MDS 9124 Multilayer Fabric Switch
- Cisco MDS 9134 Multilayer Fabric Switch
- Cisco MDS 9222i Multiservice Modular Switch
- Cisco Fabric Switch for HP c-Class BladeSystem
- Cisco Fabric Switch for IBM BladeCenter

When completed, the supervisor kickstart image, supervisor system image, the linecard image and the system BIOS are all updated.

Nondisruptive upgrades on these fabric switches take down the control plane for not more than 80 seconds. In some cases, when the upgrade has progressed past the point at which it cannot be stopped gracefully, or if a failure occurs, the software upgrade may be disruptive.



### Note

During the upgrade the control plane is down, but the data plane remains up. So new devices will be unable to log in to the fabric via the control plane, but existing devices will not experience any disruption of traffic via the data plane.

Before attempting to upgrade any software images on these fabric switches, follow these guidelines:

- During the upgrade, the fabric must be stable. None of the following configuration activities are allowed:
  - Zoning changes
  - Telnet sessions

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Schedule changes
- Switch cabling
- Addition or removal of physical devices
- Configure the FSPF timers to the default value of 20 seconds.
- If there are any CFS commits pending in the fabric, the upgrade is aborted.
- If there is a zone server merge in progress, the upgrade is aborted.
- Check whether there is sufficient space available in the system to load the new images using the Software Install Wizard. At this point you need to either abort the upgrade or proceed with a disruptive upgrade.
- On the Cisco MDS 18/4-port multiservice module, upgrades of the 4-Gigabit Ethernet ports for the hybrid Supervisor 18/4 line card will be disruptive.

## Performing a Nondisruptive Upgrade on a Fabric Switch

- Cisco MDS 9124 Multilayer Fabric Switch
- Cisco MDS 9134 Multilayer Fabric Switch
- Cisco MDS 9222i Multiservice Modular Switch
- Cisco Fabric Switch for HP c-Class BladeSystem
- Cisco Fabric Switch for IBM BladeCenter

You can use the Software Install Wizard to perform nondisruptive upgrades on Cisco MDS 9124 Fabric Switches. See [“Using the Software Install Wizard” section on page 12-8](#) for more information on using the Software Install Wizard.



### Caution

It is recommended that you enable port-fast on the Ethernet interface of the Catalyst switch to which the management interface of the fabric switch is connected. This is to avoid spanning-tree convergence time on the Catalyst switch and packets from the fabric switch are forwarded immediately during the nondisruptive upgrade.



### Note

When selecting images during the upgrade, ASM-SFN and SSI are not supported on the Cisco MDS 9124 Switch and the Cisco MDS 9134 Multilayer Fabric Switch.

## Maintaining Supervisor Modules

This section includes general information about replacing and using supervisor modules effectively.

This section includes the following topics:

- [Replacing Supervisor Modules, page 12-17](#)
- [Migrating from Supervisor-1 Modules to Supervisor-2 Modules, page 12-17](#)
- [Standby Supervisor Module Boot Variable Version, page 12-17](#)
- [Standby Supervisor Module Bootflash Memory, page 12-17](#)
- [Standby Supervisor Module Boot Alert, page 12-18](#)

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Replacing Supervisor Modules

To avoid packet loss when removing a supervisor module from a Cisco MDS 9500 Series Director, take the supervisor modules out of service before removing the supervisor module.



Note

You must remove and reinsert or replace the supervisor module to bring it into service.

## Migrating from Supervisor-1 Modules to Supervisor-2 Modules

Cisco MDS NX-OS Release 4.1(1a) requires the Supervisor-2 modules on the Cisco MDS 9509 and 9506 Directors both active and standby. You must upgrade from Supervisor-1 modules to Supervisor-2 modules before upgrading to MDS NX-OS Release 4.1(1a) or later, using the Cisco MDS SAN-OS Release 3.3(1c) or earlier.

Supervisor-1 modules and Supervisor-2 modules cannot be used in the same switch, except for migration purposes. Both the active and standby supervisor modules must be of the same type, either Supervisor-1 or Supervisor-2 modules. For Cisco MDS 9513 Directors, both supervisor modules must be Supervisor-2 modules.



Caution

Migrating your supervisor modules is a disruptive operation. When migration occurs from a Supervisor 1 to a Supervisor 2 module, a cold switchover occurs and both modules are reloaded. When the Supervisor 1 attempts to come up as the standby with the Supervisor 2 as the active supervisor, the standby is not brought up.

For step-by-step instructions about migrating from Supervisor 1 modules to Supervisor 2 modules, refer to the *Cisco MDS 9000 Family NX-OS and SAN-OS Software Upgrade and Downgrade Guide*.



Note

Migrating from Supervisor-2 modules to Supervisor-1 modules is not supported.

## Standby Supervisor Module Boot Variable Version

If the standby supervisor module boot variable images are not the *same* version as those running on the active supervisor module, the software forces the standby supervisor module to run the same version as the active supervisor module.

If you specifically set the boot variables of the standby supervisor module to a different version and reboot the standby supervisor module, the standby supervisor module will only load the specified boot variable if the same version is also running on the active supervisor module. At this point, the standby supervisor module is *not* running the images set in the boot variables.

## Standby Supervisor Module Bootflash Memory

When updating software images on the standby supervisor module, verify that there is enough space available for the image. It is a good practice to remove older versions of Cisco MDS NX-OS images and kickstart images.

To verify the space on the standby supervisor using Device Manager, follow these steps:

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- 
- Step 1** Click **Admin > Flash Files**.
- Step 2** Select the standby supervisor from the Partition drop-down list.
- At the bottom of the Flash Files dialog box, you see the space used and free space.
- 

## Standby Supervisor Module Boot Alert

If a standby supervisor module fails to boot, the active supervisor module detects that condition and generates a Call Home event and a system message and reboots the standby supervisor module approximately 3 to 6 minutes after the standby supervisor module moves to the loader> prompt.

The following system message is issued:

```
%DAEMON-2-SYSTEM_MSG:Standby supervisor failed to boot up.
```

This error message is also generated if one of the following situations apply:

- You remain at the loader> prompt for an extended period of time.
- You do not set the boot variables appropriately.

## Installing Generation 2 Modules in Generation 1 Chassis

The Generation 2 modules have the following installation restrictions:

- Supervisor-2 modules can be installed on all Cisco MDS 9500 Series Directors.



**Note** The Cisco MDS 9513 Director does not support Supervisor-1 modules.

---

- Generation 2 switching modules can be installed on all Cisco MDS 9000 Family switches, except the Cisco MDS 9216 switch.
- Generation 1 modules can be used with Cisco MDS 9000 Family switches. However, installing Generation 1 modules in combination with Generation 2 switching modules in the same chassis reduces the capabilities of the Generation 2 switching modules (see the [“Combining Generation 1, Generation 2, and Generation 3 Modules”](#) section on page 15-26).
- Generation 1 and Generation 2 switching modules can be installed on Cisco MDS 9500 Family switches with either Supervisor-1 modules or Supervisor-2 modules.

## Replacing Modules

When you replace any module (supervisor, switching, or services module), you must ensure that the new module is running the same software version as the rest of the switch.

Refer to *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide* for configuration details on replacing the Caching Services Module (CSM).



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Note**

When a spare standby supervisor module is inserted, it uses the same image as the active supervisor module. The Cisco NX-OS software image is not automatically copied to the standby flash device.

**Tip**

Use the Software Install Wizard to copy the Cisco NX-OS software image to the standby supervisor bootflash device.

Using the Software Install Wizard after replacing any module, ensures the following actions:

- The proper system and kickstart images are copied on the standby bootflash: file system.
- The proper boot variables are set.
- The loader and the BIOS are upgraded to the same version available on the active supervisor module.

To replace a module in any switch in the Cisco MDS 9200 Series or 9500 Series using Device Manager, follow these steps:

- Step 1** Create a backup of your existing configuration file, if required, by clicking **Admin > Copy Configuration** and selecting **runningConfig** to **startupConfig**.
- Step 2** Replace the required module as specified in the *Cisco MDS 9200 Series Hardware Installation Guide* or the *Cisco MDS 9500 Series Hardware Installation Guide*.
- Step 3** Verify that space is available on the standby supervisor bootflash by clicking **Admin > Flash Files** and selecting the **sup-standby**. It is a good practice to remove older versions of Cisco MDS NX-OS images and kickstart images.
- Step 4** Use the Software Install Wizard to ensure that the new module is running the same software as the rest of the switch.
- Step 5** Wait until the new module is online and then ensure that the replacement was successful by clicking **Physical > Modules** in Device Manager.

## Default Settings

Table 12-6 lists the default image settings for all Cisco MDS 9000 Family switches.

**Table 12-6**      *Default Image Settings*

| Parameters      | Default                |
|-----------------|------------------------|
| Kickstart image | No image is specified. |
| System image    | No image is specified. |

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*



## CHAPTER 13

# Management Software FAQ

---

This chapter answers some of the most frequently asked questions about Cisco Fabric Manager and Device Manager. This chapter contains the following topics:

- [Installation Issues, page 13-3](#)
  - [When installing Fabric Manager from windows, why does clicking install fail?, page 13-3](#)
  - [Why do I have trouble launching Fabric Manager on Solaris?, page 13-3](#)
  - [What do I do if my browser prompts to save JNLP files?, page 13-3](#)
  - [What do I do if I see a "Java Web Start not detected" error?, page 13-4](#)
  - [What do I do if my desktop shortcuts not visible?, page 13-4](#)
  - [How do I upgrade to a newer version of Fabric Manager or Device Manager?, page 13-4](#)
  - [How do I downgrade Fabric Manager or Device Manager?, page 13-4](#)
  - [What do I do if an upgrade is not working?, page 13-4](#)
  - [What do I do if Java Web Start hangs on the download dialog?, page 13-5](#)
  - [How do I manually configure a browser for Java Web Start?, page 13-5](#)
  - [How do I run Java Web Start from the command line?, page 13-5](#)
  - [How do I clear the Java Web Start cache?, page 13-6](#)
  - [What do I do if my login does not work in Fabric Manager or Device Manager?, page 13-6](#)
  - [What do I do if I cannot install Fabric Manager or Device Manager, or run Java, when pcAnyWhere is running?, page 13-6](#)
  - [What do I do if the Fabric Manager or Performance Manager service shows up as “disabled” in the Services menu?, page 13-6](#)
  - [What do I do if I am unable to install Fabric Manager or Device Manager, or run Java, when McAfee Internet Suite 6.0 Professional is running?, page 13-7](#)
- [General, page 13-7](#)
  - [What do I do if I see errors while monitoring Area chart graphing?, page 13-7](#)
  - [What do I do if I see "gen error" messages?, page 13-7](#)
  - [What do I do if disk images in the Device Manager Summary View are not visible?, page 13-7](#)
  - [What do I do if I am unable to set both the D\\_S\\_TOV and E\\_D\\_TOV timers in Device Manager?, page 13-7](#)
  - [What do I do if columns in Device Manager tables are too small?, page 13-8](#)

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- What do I do if fabric changes are not propagated onto the map (for example, links don't disappear)?, page 13-8
- What do I do if the PortChannel creation dialog becomes too small after several uses?, page 13-8
- What do I do if I see errors after IPFC configuration?, page 13-8
- What do I do if Fabric Manager or Device Manager is using the wrong network interface?, page 13-8
- What do I do if I see display anomalies in Fabric Manager or Device Manager?, page 13-8
- Why is the active zone set in edit zone always shown in bold (even after successful activation)?, page 13-9
- Can I create a zone with prefix IVRZ or a zone set with name nozonset?, page 13-9
- What do I do when One-Click License Install fails, and I cannot connect to the Cisco website?, page 13-9
- What do I do when Fabric Manager client and Device Manager cannot connect to the switch?, page 13-10
- How do I increase the log window size in Fabric Manager Client?, page 13-10
- When do I do when the FM Server Database fails to start or has a file locking error?, page 13-10
- Windows Issues, page 13-11
  - What do I do when text fields show up too small, and I cannot enter any data?, page 13-11
  - What do I do when printing causes an application crash?, page 13-11
  - What do I do when Windows XP hangs (or I see a blue screen)?, page 13-11
  - What do I do when Fabric Manager and Device Manager Icons Disappear?, page 13-11
  - What do I do when Device Manager or Fabric Manager window content disappears in Windows XP?, page 13-11
  - What do I do when SCP/SFTP fails when a file is copied from local machine to the switch?, page 13-12
- UNIX Issues, page 13-12
  - What do I do when the parent Menus Disappear?, page 13-12
  - What do I do when the web browser cannot find web server even it is running?, page 13-12
  - How do I fix a "too many open files" error?, page 13-12
- Other, page 13-13
  - How do I set the map layout so it stays after Fabric Manager restarted?, page 13-13
  - What do I do when two switches show on the map, but there is only one switch?, page 13-13
  - What does a red/orange/dotted line through the switch mean?, page 13-13
  - How do I upgrade without losing map settings?, page 13-19
  - How do I preserve historical data when moving Fabric Manager server to new host?, page 13-19
  - Are there restrictions when using Fabric Manager across FCIP?, page 13-19
  - How do I fix a "Please insure that FM server is running on localhost" message?, page 13-20
  - How do I run Cisco Fabric Manager with multiple interfaces?, page 13-20
  - How do I configure an HTTP proxy server?, page 13-21

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- [How do I clear the topology map?, page 13-21](#)
- [How can I use Fabric Manager in a mixed software environment?, page 13-22](#)
- [How do I fix a "corrupted jar file" error when Launching Fabric Manager?, page 13-22](#)
- [How do I search for Devices in a Fabric?, page 13-22](#)
- [How does Fabric Manager Server licensing work?, page 13-24](#)
- [How do I manage Multiple Fabrics?, page 13-24](#)
- [How can I clear an Orange X Through a Switch caused by license expiration?, page 13-24](#)

## Installation Issues

### When installing Fabric Manager from windows, why does clicking install fail?

To make sure that Java Web Start is installed properly, follow these steps:

- 
- |               |                                                                                                                                                                                |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Go to the Programs menu and see if Java Web Start is there.                                                                                                                    |
| <b>Step 2</b> | Start the <b>Java Web Start</b> program to make sure there is no problem with the Java Runtime installation.                                                                   |
| <b>Step 3</b> | Click the <b>Preferences</b> tab, and make sure the proxies settings are fine for Web Start.                                                                                   |
| <b>Step 4</b> | Check that your browser is set up to handle JNLP settings properly (see the <a href="#">“How do I manually configure a browser for Java Web Start?”</a> section on page 13-5). |
- 

If you had older versions of the application and you see an error pop-up window saying cannot open the JNLP file (in the error details), this could be because the Java Web Start cache is messed up. To work around this, clear the cache and retry. To clear the cache, see the [“How do I clear the Java Web Start cache?”](#) section on page 13-6.

### Why do I have trouble launching Fabric Manager on Solaris?

If you are using Solaris 2.8 and are logged in as root and are using Netscape Navigator 6, you will not be able to register the mime-type. Regular users can register the mime-type with Netscape Navigator 6 by manually adding it. Netscape 4.x works fine for all users.

### What do I do if my browser prompts to save JNLP files?

Your browser may not be set up to launch Java Web Start for JNLP mime types. Java Web Start is probably not installed or configured properly (see the [“How do I manually configure a browser for Java Web Start?”](#) section on page 13-5).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## What do I do if I see a "Java Web Start not detected" error?

If you installed Java Web Start but still see an error message (in red) saying "Java Web Start not detected..." on the switch home page, it could be a simple JavaScript error. We try to detect a Java Web Start installation by running some JavaScript code tested for Internet Explorer and Mozilla (newer versions). On some browsers (for example, Netscape 6.0, Opera) this code does not work properly although the links still work.

- First, try clicking on the install links.
- If that does not work, check to see if the browser helper applications settings are correct (for example, for Netscape 6.0 **Edit > Preferences > Navigator > Helper Applications**). See the ["How do I manually configure a browser for Java Web Start?"](#) section on page 13-5.

## What do I do if my desktop shortcuts not visible?

For Windows 2000 and Windows NT, we create Program Menu entries (under a new Cisco MDS 9000 program menu) and desktop shortcuts for Fabric Manager and Device Manager. The desktop shortcuts and start menu entries for Fabric Manager and Device Manager are called FabricManager and DeviceManager respectively. In other versions of Windows, including XP, we just create batch files on the desktop called FabricManager.bat and DeviceManager.bat. For UNIX, we create shell scripts called FabricManager.sh and DeviceManager.sh under the \$HOME/.cisco\_mds9000/bin directory. Note that on Windows, installations run under Mozilla variants of browsers, and the desktop shortcuts do not get created. The workaround is to manually create desktop shortcuts.

## How do I upgrade to a newer version of Fabric Manager or Device Manager?

To upgrade to a newer version of Fabric Manager or Device Manager, follow these steps:

- 
- Step 1** Close all running instances of Fabric Manager or Device Manager.
  - Step 2** Point your browser at the switch running the new version and click the appropriate install link. Fabric Manager or Device Manager prompts you to upgrade if the switch is running a newer version.
- The installer checks your local copies and updates any newer versions of the software.
- 

## How do I downgrade Fabric Manager or Device Manager?

As of Cisco MDS NX-OS Release 4.x, downgrades are not supported through the installer. To downgrade Fabric Manager or Device Manager to an earlier release, you need to manually uninstall first and then install the previous version of Fabric Manager or Device Manager.

## What do I do if an upgrade is not working?

If you are trying to upgrade because Fabric Manager or Device Manager prompted you saying that the switch version is higher, and the upgrade failed, it might be because your default browser settings are incorrect. Some error must have occurred during your last browser upgrade/install. To work around this, launch the browser independently and click on install.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

On rare occasions, we have seen the upgrade happen but the version does not change. This is because of HTTP caching in the network. During the upgrade, HTTP requests for files on the switch get cached in the local machine. Even though the switch is in a higher version, the management software installed is at the old version. The workaround for this is to uninstall the Fabric/Device Manager, clear the Java Web Start cache, and then do a clean install.

## What do I do if Java Web Start hangs on the download dialog?

To make sure Java Web Start is set up to access the switch in the same way your browser is set up, follow these steps:

- 
- |        |                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Start Java Web Start ( <b>javaws.exe</b> or <b>javaws</b> ). You see the Java Web Start Application Manager.                                                 |
| Step 2 | Choose <b>File &gt; Preferences &gt; General</b> and make sure your proxy settings are correct. For example, if you are using an HTTP proxy, set it up here. |
| Step 3 | Choose <b>Use Browser</b> .                                                                                                                                  |
| Step 4 | Click <b>OK</b> .                                                                                                                                            |
- 

## How do I manually configure a browser for Java Web Start?

For browsers like Opera, certain versions of Mozilla, or Konqueror, you must manually register Java Web Start as the helper application for the JNLP files. To do this, the data you need is:

- Description=Java Web Start
- File Extension=jnlp
- Mime Type=application/x-java-jnlp-file
- Application=path-to-javaws (e.g. /usr/local/javaws/javaws)

After setting this up, you may need to restart the browser. If you see "Java Web Start not detected" warnings, you can ignore them. These warnings are based on JavaScript, and not all browsers behave well with JavaScript. Click on the install links to install Fabric Manager or Device Manager.



### Note

For Windows Users: To set up Java Web Start on \*.jnlp files, select **Windows Explorer > Tools > Folder Options > File Types**. Either change the existing setting for JNLP or add one so that \*.jnlp files are opened by javaws.exe. This executable is under Program Files\Java Web Start

## How do I run Java Web Start from the command line?

If you cannot get your browser to run Java Web Start, you can still run Java Web Start from the command line (javaws.exe or javaws) giving it the URL of the Fabric Manager or Device Manager on the switch as an argument. For example, if your switch IP address is 10.0.0.1, you would use these commands to start Fabric Manager and Device Manager:

```
javaws http://10.0.0.1/cgi-bin/fabric-manager.jnlp
javaws http://10.0.0.1/cgi-bin/element-manager.jnlp
```

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## How do I clear the Java Web Start cache?

To clear the Java Web Start cache, follow these steps:

- 
- |        |                                                                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Start the Java Web Start Application Manager ( <b>javaws.exe</b> or <b>javaws</b> ).                                                                                                                                                    |
| Step 2 | Go to <b>File &gt; Preferences &gt; Advanced</b> and clear the applications folder or cache. You can manually delete the .javaws or cache directory. On Windows this is under Documents and Settings, and on UNIX this is under \$HOME. |
- 

## What do I do if during a Fabric Manager upgrade, the installer doesn't display a prompt to create a shortcut?

Clear the Java Web Start cache as described in *How do I clear the Java Web Start cache?* in this chapter.

## What do I do if my login does not work in Fabric Manager or Device Manager?

Make sure you have done the Initial Setup Routine on the switch. Refer to the *Cisco MDS 9000 Family Fabric Manager Fundamentals Configuration Guide*. Quick checks:

- Make sure that the management interface on the switch is up (**show interface mgmt0**).
- Check whether you can connect to the management interface (**ping**).
- Verify the username is valid (**show snmp user**). You can also add/edit the users through the CLI.
- If you have multiple network interfaces, see the [“What do I do if Fabric Manager or Device Manager is using the wrong network interface?”](#) section on page 13-8

## What do I do if I cannot install Fabric Manager or Device Manager, or run Java, when pcAnyWhere is running?

You can either stop the pcAnyWhere service and install Fabric Manager or Device Manager, or install/update DirectX. For more information, refer to the website at <http://java.sun.com/>

## What do I do if the Fabric Manager or Performance Manager service shows up as “disabled” in the Services menu?

This could happen if:

- The service menu for Fabric Manager or Performance Manager was open during an uninstall/upgrade.
- The Fabric Manager client or Device Manager was running while doing an uninstall/upgrade.

This error happens when Windows is unable to delete a service completely. A reboot of the host should fix the problem.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## What do I do if I am unable to install Fabric Manager or Device Manager, or run Java, when McAfee Internet Suite 6.0 Professional is running?

The McAfee internet suite comes with a virus scanner, firewall, antispam, and privacy management. The privacy management can interfere with the Fabric Manager server-client interactions. To work around this you must shut down the privacy service.

## General

### What do I do if I see errors while monitoring Area chart graphing?

When doing the area chart graphing from the monitor window, if you move the mouse over the Area chart before the first data comes back, you see a `java.lang.ArrayIndexOutOfBoundsException` error on the message log from JChart `getX()`. This is because JChart tries to locate a value that does not exist yet. This might be fixed in a future version of JChart.

### What do I do if I see "gen error" messages?

Usually a "gen error" means that the SNMP agent on the switch had an unexpected error in the process of serving an SNMP request. However, when you are accessing the switch through a VPN connection or any sort of NAT scheme, all errors are reported as gen error. This is a known problem and will be fixed in a future release. You can verify whether this was the reason behind your gen error by trying to reproduce this error in an environment where there is no network address translation (where you are on the same network as the switch).

### What do I do if disk images in the Device Manager Summary View are not visible?

On some occasions the Summary View table in the Device Manager does not show the icons for disks attached to a Fx port. This is because the FC4 features are empty for this port. A LUN discovery must be issued to discover information about these hosts/disks that do not register their FC4 types. You can do this in the Device Manager by clicking **FC > Advanced > LUNs**.

### What do I do if I am unable to set both the D\_S\_TOV and E\_D\_TOV timers in Device Manager?

If you modify both E\_D\_TOV and D\_S\_TOV at the same time, and the new D\_S\_TOV value is larger than the old E\_D\_TOV value, you will get a WrongValue error. To work around this, you must change the values separately.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## What do I do if columns in Device Manager tables are too small?

If Device Manager is trying to display a large table and your switch is running slowly, the table will come up with the tabs being hidden. To work around this, you must resize the window to see the data.

## What do I do if fabric changes are not propagated onto the map (for example, links don't disappear)?

Fabric Manager shows that a device or port is down by displaying a red cross on that port or device. However, Fabric Manager does not remove any information that's already discovered. You must rediscover to correctly update the map.

## What do I do if the PortChannel creation dialog becomes too small after several uses?

After several uses, the MemberList TextBox (in the PortChannel Create Window) does not display as it should. It changes from a long TextBox with a ComboBox for choosing ports, to a small square TextBox that is too small to choose ports. This is a known problem and will be fixed in a future release. To work around this problem, stop and restart Fabric Manager or Device Manager.

## What do I do if I see errors after IPFC configuration?

When IPFC and out of band management are configured, the Device Manager might not work using SNMPv3 if you use the IPFC address. The workaround is either to use the management interface (mgmt0) address, or to use SNMPv1/v2c over IPFC.

## What do I do if Fabric Manager or Device Manager is using the wrong network interface?

The problem happens because the underlying Java library picks a local interface arbitrarily. To work around this, supply a command line argument before starting the Fabric/Device Manager. In the desktop shortcut or shell script or batch file, add the following parameter "-Device Managers.nmsAddress="

For example, in Windows the line looks like ".javaw.exe -Device Managers.nmsAddress=X.X.X.X -cp .".

In desktop shortcuts, this length could exceed the maximum characters allowed. If this happens, delete the "-Dsun.java2d.dboffscreen=false" portion to make more space. Newer versions of Fabric Manager (Release 1.2 and later) allow you to pick a preferred network interface.

## What do I do if I see display anomalies in Fabric Manager or Device Manager?

If you see Fabric Manager or Device Manager submenus detached from menus, the mouse pointer in Fabric Manager Map is slow to react to mouse movement, or a wrong tooltip is displayed, these are display anomalies, not problems with Fabric Manager or Device Manager.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

Some older video cards exhibit these display anomalies. To fix this, first try updating the video drivers. If this doesn't solve the problem, replace the video card.

## What do I do if most of my Physical Attributes categories disappear?

You have somehow turned off advanced features. Look for the check box Advanced Features in the upper right of the Fabric Manager screen. Check the box.

## What do I do if I can't see the Information pane?

The information pane should be in the upper half of the screen above the map in Fabric Manager. The map may be covering it. Drag the edge of the map window down or use the black triangles to reorganize the display.

## Why is the active zone set in edit zone always shown in bold (even after successful activation)?

A member of this VSAN must be participating in IVR zoning. Because the IVR zones get added to active zones, the active zone set configuration is always different from the local zone set configuration with the same name. The zone set name is always bold.

## Can I create a zone with prefix IVRZ or a zone set with name nozonset?

Do not use these special names. These names are used by the system for identifying IVR zones.

## What do I do when One-Click License Install fails, and I cannot connect to the Cisco website?

The one-click license install tries to open an HTTP connection to the Cisco website. If you do your browsing using an HTTP proxy then the following command-line variables need to be added to your Fabric Manager client scripts:

```
-Dhttps.proxyHost and -Dhttps.proxyPort.
```

In case your one-click install URL starts with "http://" (and not "https://"), the variables are:

```
-Dhttp.proxyHost and -Dhttp.proxyPort.
```

For example, in Windows, edit the MDS 9000\bin\FabricManager.bat file and add to the JVMARGS "-Dhttps.proxyHost=HOSTADDRESS -Dhttps.proxyPort=HOSTPORT".

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## What do I do when Fabric Manager client and Device Manager cannot connect to the switch?

Fabric Manager or Device Manager using SNMPv3 at Cisco MDS SAN-OS Release 1.3(3) or earlier can't manage a switch running Release 1.3(4) or later. This might affect a software upgrade using Fabric Manager from Release 1.3(3) to Release 1.3(4).

## How do I increase the log window size in Fabric Manager Client?

To limit the memory usage by FM Client, the log window is limited to 500 lines by default. If you want to increase this, edit `sm.properties` in `<install directory>/db/<user>` directory and change `LogBufferSize`.

## When do I do when the FM Server Database fails to start or has a file locking error?

In the database log (`FMPersist.log`) you will see an error message "The database is already in use by another process". The HsqlDB 1.7.1 version has this problem. The file lock problem seems to happen occasionally, and can be resolved by shutdown and restart of the db server. On windows this can be done by stopping and starting the `FMPersist` service and on Unix just run the `FMPersist.sh` script with the argument `restart`.

## How do I re-synchronize Fabric Manager Client with Fabric Manager Server?

On some occasions, when the Fabric Manager Client is not in sync with the Fabric Manager Server, you may need to re-synchronize the client and server. To re-synchronize Fabric Manager Client with Fabric Manager Server, click **Resync All Open Fabrics** from the **File** menu,

## How do I rediscover the current fabric?

When the Fabric Manager Server is not in sync with the switches in the fabric, you may need to initiate an on-demand discovery to update the Fabric Manager Client with the most recent changes from the switches in the fabric. To rediscover the fabric switches, click **Rediscover** from the **File** menu.

## How do I rediscover SCSI Targets?

When the Fabric Manager Server is not in sync with the SCSI Target switches in the fabric, you may need to initiate an on-demand discovery to update the Fabric Manager Client with the most recent changes from the SCSI Target switches in the fabric. To rediscover the fabric switches, click **Rediscover SCSI Targets** from the **File** menu.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Windows Issues

### What do I do when text fields show up too small, and I cannot enter any data?

When Reflection X is running, certain text fields in the Fabric Manager and Device Manager are not rendered to the full width of the field. Resize the dialog box to see the text fields properly.

### What do I do when printing causes an application crash?

On Windows NT there is a known Sun JVM bug - the printservice crashes the VM. The solution suggested by Sun is to update NT with SP 6. For more details refer to:  
<http://developer.java.sun.com/developer/bugParade/bugs/4530428.html>.

### What do I do when Windows XP hangs (or I see a blue screen)?

Windows XP with the ATI Radeon AGP graphics cards has known to freeze (hang) when a Java application exits. The newer drivers from ATI seem to have fixed this problem. The other workaround is to run the application with "-Dsun.java2d.noddraw=true". We do this today in the shortcut and shell scripts we create. For more details refer to:  
<http://developer.java.sun.com/developer/bugParade/bugs/4713003.html>.

### What do I do when Fabric Manager and Device Manager icons disappear?

On certain versions of Windows, certain images disappear. This is a Java bug. We have a workaround that is already in place (disable DirectDraw acceleration) - but there are still cases where this problem might arise. For more details refer to:  
<http://developer.java.sun.com/developer/bugParade/bugs/4664818.html>.

### What do I do when Device Manager or Fabric Manager window content disappears in Windows XP?

Device Manager or Fabric Manager main window content disappears in Windows XP due to a Java bug. Refer to the following website:  
[http://bugs.sun.com/bugdatabase/view\\_bug.do?bug\\_id=4919780](http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=4919780).

Minimize or maximize the window and restore to the normal size to restore the window content. Disabling Direct Draw may also prevent this from happening by adding "-Dsun.java2d.noddraw=true" to JVMARGS in <FM-install-dir>/bin/FabricManager.bat and DeviceManager.bat

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## What do I do when SCP/SFTP fails when a file is copied from local machine to the switch?

If there are embedded spaces in the file path, then windows scp/sftp might fail. You will get a copyDeviceBusy error from the switch. In tools such as the License Wizard either make sure tftp copy can be done or pick filenames with no spaces.

## UNIX Issues

### What do I do when the parent menus disappear?

Displaying a submenu may occasionally cause the parent menu to disappear. For more details on this bug, refer to: <http://developer.java.sun.com/developer/bugParade/bugs/4470374.html>.

### What do I do when the web browser cannot find web server even it is running?

This can happen when web browser uses proxy server. To check that for Internet Explorer, choose tools in menu, then choose internet options, then choose connection subpanel, then click Lan Setting. A dialog comes up, verify the proxy setting.

### How do I fix a "too many open files" error?

If you are running the JVM (Java Virtual Machine) on Linux and the drive where Java is installed or your home directory is NFS mounted, there is an open bug against the Sun JDK about errors acquiring file locks. The symptoms for the Fabric Manager are that launching a Device Manager or saving/opening files will fail, giving a "too many open files" I/O or socket exception. The JVM keeps trying to open a file on the NFS mounted drives, fails, and keeps trying to do it until it hits the 1024 file descriptors limit. Workarounds (assuming /tmp is a local disk - replace it with your tmp area):

- System Preferences

Make sure the system level preferences are stored on a local disk. The system preferences are stored in \$JAVA\_HOME/.systemPrefs where JAVA\_HOME is where you have installed the JDK. If this directory is NFS mounted, then just do the following:

```
$ rm -rf $JAVA_HOME/.systemPrefs<
$ mkdir /tmp/.systemPrefs
$ ln -s /tmp/.systemPrefs $JAVA_HOME/.systemPrefs
```

The problem with this workaround is that you have to make sure /tmp/.systemPrefs exists on every box where you are using \$JAVA\_HOME. We recommend installing the JVM as root and on a local disk.

- User Preferences

If your home directory is NFS mounted and you are getting this problem. Do the following:

```
$ rm -rf $HOME/.java
$ mkdir /tmp/.java.$USER
$ ln -s /tmp/.java.$USER $HOME/.java
```

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

For further details, see the following URLs:

<http://developer.java.sun.com/developer/bugParade/bugs/4673298.html>

<http://developer.java.sun.com/developer/bugParade/bugs/4635353.html>

## Other

### How do I set the map layout so it stays after Fabric Manager restarted?

If you have arranged the map to your liking and would like to “freeze” the map so that the objects stay as they are even after you stop Fabric Manager and restart it again, follow these steps:

- 
- Step 1** Right-click in a blank space in the map. You see a menu.
- Step 2** Select **Layout > Fix All Nodes** from the menu.
- 

### What do I do when two switches show on the map, but there is only one switch?

If two switches show on your map, but you only have one switch, it may be that you have two switches in a non-contiguous VSAN that have the same Domain ID. Fabric Manager uses <vsanId><domainId> to look up a switch, and this can cause the fabric discovery to assign links incorrectly between these errant switches.

The workaround is to verify that all switches use unique domain IDs within the same VSAN in a physically connected fabric. (The fabric configuration checker will do this task.)

### What does a red/orange/dotted line through the switch mean?

If a red line shows through your switch, this means Fabric Manager sees something wrong with the switch. Choose **Switches** in the Physical Attributes pane to see a status report in the information pane. A module, fan, or power supply has failed or is offline and plugged in.

If a dotted orange line shows through your switch, this indicates a minor status warning for that switch. Usually it means an issue with one of the modules. The tooltip should say exactly what is wrong. Hold the mouse over the switch to see the tooltip.

Below are tables of color settings and tooltip definitions for Fabric Manager and Device Manager.

**Table 13-1** *Fabric Manager and Device Manager Color Definitions*

| Fabric Manager Color | Definition                                                                                                         |
|----------------------|--------------------------------------------------------------------------------------------------------------------|
| Red Slash            | Cannot communicate with a switch via SNMP.                                                                         |
| Red X                | Cannot communicate with or see a switch in the Domain Manager/Fabric Configuration Server list of fabric switches. |
| Device Manager Color | Definition                                                                                                         |

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Table 13-1 Fabric Manager and Device Manager Color Definitions (continued)**

| Fabric Manager Color                                   | Definition                                      |
|--------------------------------------------------------|-------------------------------------------------|
| Green Square with Mode (e.g., F, T, TE, U/I for FICON) | Port up.                                        |
| Orange Square with Mode                                | Trunk incomplete.                               |
| Orange Cross                                           | Ols or Nos received.                            |
| Brown Square                                           | Port is administratively down.                  |
| Light Gray Square                                      | Port is not manageable.                         |
| Red Cross                                              | HardwareFailure/LoopbackDiagFailure/LinkFailure |
| Red Square                                             | Any other kind of configuration failure.        |
| No Square or Black Square                              | Port not yet configured.                        |

**Table 13-2 Device Manager Tooltip Definitions**

| Tooltip                          | Definition                                                                                                                                                                                                  |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| adminDown                        | The port is administratively down.                                                                                                                                                                          |
| bitErrRTThresExceeded            | Bit error rate too high.                                                                                                                                                                                    |
| bundleMisCfg                     | Misconfiguration in PortChannel membership detected.                                                                                                                                                        |
| channelAdminDown                 | This port is a member of a PortChannel and that PortChannel is administratively down.                                                                                                                       |
| channelConfigurationInProgress   | This port is undergoing a PortChannel configuration.                                                                                                                                                        |
| channelOperSuspended             | This port is a member of a PortChannel and its operational parameters are incompatible with the PortChannel parameters.                                                                                     |
| deniedDueToPortBinding           | Suspended due to port binding.                                                                                                                                                                              |
| domainAddrAssignFailureIsolation | The elected principal switch is not capable of performing domain address manager functions so no Nx_port traffic can be forwarded across switches, hence all Interconnect_Ports in the switch are isolated. |
| domainInvalidRCFReceived         | Invalid RCF received.                                                                                                                                                                                       |
| domainManagerDisabled            | Domain manager is disabled.                                                                                                                                                                                 |
| domainMaxReTxFailure             | Domain manager failure after maximum retries.                                                                                                                                                               |
| domainOtherSideEportIsolation    | The peer E port is isolated.                                                                                                                                                                                |
| domainOverlapIsolation           | There is a overlap in domains while attempting to connect two existing fabrics.                                                                                                                             |
| elpFailureClassFParamErr         | Isolated for ELP failure due to class F parameter error.                                                                                                                                                    |



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Table 13-2 Device Manager Tooltip Definitions (continued)**

| Tooltip                       | Definition                                                                                                                                                   |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| elpFailureClassNParamErr      | Isolated for ELP failure due to class N parameter error.                                                                                                     |
| elpFailureInvalidFlowCTLParam | Isolated for ELP failure due to invalid flow control parameter.                                                                                              |
| elpFailureInvalidPayloadSize  | Isolated for ELP failure due to invalid payload size.                                                                                                        |
| elpFailureInvalidPortName     | Isolated for ELP failure due to invalid port name.                                                                                                           |
| elpFailureInvalidSwitchName   | Isolated for ELP failure due to invalid switch name.                                                                                                         |
| elpFailureInvalidTxBBCredit   | Isolated for ELP failure due to invalid transmit B2B credit.                                                                                                 |
| elpFailureIsolation           | During a port initialization the prospective Interconnect_Ports find incompatible link parameters.                                                           |
| elpFailureLoopbackDetected    | Isolated for ELP failure due to loopback detected.                                                                                                           |
| elpFailureRatovEdtovMismatch  | Isolated for ELP failure due to R_A_TOV or E_D_TOV mismatch.                                                                                                 |
| elpFailureRevMismatch         | Isolated for ELP failure due to revision mismatch.                                                                                                           |
| elpFailureUnknownFlowCTLCode  | Isolated for ELP failure due to invalid flow control code.                                                                                                   |
| ePortProhibited               | Port down because FICON prohibit mask in place for E/TE port.                                                                                                |
| eppFailure                    | Trunk negotiation protocol failure after maximum retries.                                                                                                    |
| errorDisabled                 | The port is not operational due to some error conditions that require administrative attention.                                                              |
| escFailureIsolation           | During a port initialization the prospective Interconnect_Ports are unable to proceed with initialization as a result of Exchange Switch Capabilities (ESC). |
| fabricBindingDBMismatch       | fabric binding active database mismatch with peer.                                                                                                           |
| fabricBindingDomainInvalid    | Peer domain ID is invalid in fabric binding active database.                                                                                                 |
| fabricBindingNoRspFromPeer    | Fabric binding no response from peer.                                                                                                                        |
| fabricBindingSWWNNotFound     | Peer switch WWN not found in fabric binding active database.                                                                                                 |
| fcipPortAdminCfgChange        | FCIP port went down due to configuration change.                                                                                                             |
| fcipPortKeepAliveTimerExpire  | FCIP port went down due to TCP keep alive timer expired.                                                                                                     |

[Send documentation comments to fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)

**Table 13-2 Device Manager Tooltip Definitions (continued)**

| Tooltip                       | Definition                                                                                                                      |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| fcipPortMaxReTx               | FCIP port went down due to max TCP retransmissions reached the configured limit.                                                |
| fcipPortPersistTimerExpire    | FCIP port went down due to TCP persist timer expired.                                                                           |
| fcipPortSrcAdminDown          | FCIP port went down because the source ethernet link was administratively shutdown.                                             |
| fcipPortSrcLinkDown           | FCIP port went down due to ethernet link down.                                                                                  |
| fcipSrcModuleNotOnline        | FCIP port went down due to source module not online.                                                                            |
| fcipSrcPortRemoved            | FCIP port went down due to source port removal.                                                                                 |
| fcotChksumErr                 | FSP SPROM checksum error.                                                                                                       |
| fcotNotPresent                | SFP (GBIC) not present.                                                                                                         |
| fcotVendorNotSupported        | FSP (GBIC) vendor is not supported.                                                                                             |
| fcspAuthenfailure             | Fibre Channel security protocol authorization failed.                                                                           |
| ficonBeingEnabled             | FICON is being enabled.                                                                                                         |
| ficonNoPortnumber             | No FICON port number.                                                                                                           |
| ficonNotEnabled               | FICON not enabled.                                                                                                              |
| ficonVsanDown                 | FICON VSAN is down.                                                                                                             |
| firstPortNotUp                | In a over subscribed line card, first port cannot be brought up in E mode when the other ports in the group are up.             |
| firstPortUpAsEport            | In a over subscribed line card, when the first port in a group is up in E mode, other ports in that group cannot be brought up. |
| hwFailure                     | Hardware failure.                                                                                                               |
| incomAdminRxBBCreditPerBuf    | Disabled due to incompatible admin port rxbbcredit, performance buffers.                                                        |
| incompatibleAdminMode         | Port admin mode is incompatible with port capabilities.                                                                         |
| incompatibleAdminRxBBCredit   | Receive BB credit is incompatible.                                                                                              |
| incompatibleAdminRxBufferSize | Receive buffer size is incompatible.                                                                                            |
| incompatibleadminSpeed        | Port speed is incompatible with port capabilities.                                                                              |
| initializing                  | The port is being initialized.                                                                                                  |
| interfaceRemoved              | Interface is being removed.                                                                                                     |
| invalidAttachment             | Invalid attachment.                                                                                                             |
| invalidConfig                 | This port has a misconfiguration with respect to port channels.                                                                 |
| invalidFabricBindExh          | Invalid fabric binding exchange.                                                                                                |

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Table 13-2**      *Device Manager Tooltip Definitions (continued)*

| Tooltip                      | Definition                                                                                  |
|------------------------------|---------------------------------------------------------------------------------------------|
| linkFailCreditLoss           | Link failure due to excessive credit loss indications.                                      |
| linkFailCreditLossB2B        | Link failure when link reset (LR) operation fails due to queue not empty.                   |
| linkFailDebounceTimeout      | Link failure due to re-negotiation failed.                                                  |
| linkFailLineCardPortShutdown | Link failure due to port shutdown.                                                          |
| linkFailLinkReset            | Link failure due to link reset.                                                             |
| linkFailLIPF8Rcvd            | Link failure due to F8 LIP received.                                                        |
| linkFailLIPRcvdB2B           | Link failure when loop initialization (LIP) operation fails due to non empty receive queue. |
| linkFailLossOfSignal         | Link failure due to loss of signal.                                                         |
| linkFailLossOfSync           | Link failure due to loss of sync.                                                           |
| linkFailLRRcvdB2B            | Link failure when link reset (LR) operation fails due to non-empty receive queue.           |
| linkFailNOSRcvd              | Link failure due to non-operational sequences received.                                     |
| linkFailOLSRcvd              | Link failure due to offline sequences received.                                             |
| linkFailOPNyRETB2B           | Link failure due to open primitive signal returned while receive queue not empty.           |
| linkFailOPNyTMOB2B           | Link failure due to open primitive signal timeout while receive queue not empty.            |
| linkFailPortInitFail         | Link failure due to port initialization failure.                                            |
| linkFailPortUnusable         | Link failure due to port unusable.                                                          |
| linkFailRxQOverflow          | Link failure due to receive queue overflow.                                                 |
| linkFailTooManyINTR          | Link failure due to excessive port interrupts.                                              |
| linkFailure                  | Physical link failure.                                                                      |
| loopbackDiagFailure          | Loopback diagnostics failure.                                                               |
| loopbackIsolation            | Port is connected to another port in the same switch.                                       |
| noCommonVsanIsolation        | Trunk is isolated because there are no common vsans with peer.                              |
| none                         | No failure.                                                                                 |
| nonParticipating             | During loop initialization, the port is not allowed to participate in loop operations       |
| offline                      | Physical link is in offline state as defined in the FC-FS standards.                        |
| ohmsExtLBTest                | Link suspended due to external loopback diagnostics failure.                                |
| other                        | Undefined reason.                                                                           |

[Send documentation comments to fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)

**Table 13-2**      *Device Manager Tooltip Definitions (continued)*

| Tooltip                      | Definition                                                                                                                                                                                               |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| parentDown                   | The physical port to which this interface is bound is down.                                                                                                                                              |
| peerFCIPPortClosedConnection | Port went down because peer FCIP port closed TCP connection.                                                                                                                                             |
| peerFCIPPortResetConnection  | Port went down because the TCP connection was reset by the peer FCIP port.                                                                                                                               |
| portBindFailure              | Port got isolated due to port bind failure.                                                                                                                                                              |
| portBlocked                  | Port blocked due to FICON.                                                                                                                                                                               |
| portChannelMembersDown       | No operational members.                                                                                                                                                                                  |
| portFabricBindFailure        | Port isolated due to fabric bind failure.                                                                                                                                                                |
| portGracefulShutdown         | Port shutdown gracefully.                                                                                                                                                                                |
| portVsanMismatchIsolation    | An attempt is made to connect two switches using non-trunking ports having different port VSANs.                                                                                                         |
| rcfInProgress                | An isolated xE_port is transmitting a reconfigure fabric, requesting a disruptive reconfiguration in an attempt to build a single, non-isolated fabric. Only the Interconnect_Ports can become isolated. |
| srcPortNotBound              | No source port is specified for this interface.                                                                                                                                                          |
| suspendedByMode              | Port that belongs to a port channel is suspended due to incompatible operational mode.                                                                                                                   |
| suspendedBySpeed             | Port that belongs to a port channel is suspended due to incompatible operational speed.                                                                                                                  |
| suspendedByWWN               | Port that belongs to a port channel is suspended due to incompatible remote switch WWN.                                                                                                                  |
| swFailure                    | Software failure.                                                                                                                                                                                        |
| tooManyInvalidFLOGIs         | Suspended due to too many invalid FLOGIs.                                                                                                                                                                |
| tovMismatch                  | Link isolation due to TOV mismatch                                                                                                                                                                       |
| trunkNotFullyActive          | Some of the VSANs which are common with the peer are not up.                                                                                                                                             |
| upgradeInProgress            | Line card upgrade in progress.                                                                                                                                                                           |
| vsanInactive                 | Port VSAN is inactive. The port becomes operational again when the port VSAN is active.                                                                                                                  |
| vsanMismatchIsolation        | This VSAN is not configured on both sides of a trunk port.                                                                                                                                               |
| zoneMergeFailureIsolation    | The two Interconnect_Ports cannot merge zoning configuration after having exchanged merging request for zoning.                                                                                          |
| zoneRemoteNoRespIsolation    | Isolation due to remote zone server not responding.                                                                                                                                                      |

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## How do I upgrade without losing map settings?

When you upgrade from one version of Fabric Manager to another, there is a way to prevent the loss of map settings (enclosure names, placement on the map, etc.)

The MDS 9000/db directory contains subfolders for each user (and one for fmserver). In these subfolders are files for all discovered fabrics (\*.dat) and maps (\*.map). These are upgradable between versions. If you need to clear the fabric cache, you should first export the enclosures to a file to avoid losing them. Everything else aside from enclosures and map coordinates are stored on the switch. The preferences, last opened, and site\_ouis.txt format doesn't change from release to release.

## How do I preserve historical data when moving Fabric Manager server to new host?

To preserve your data when moving Fabric Manager Server to a new host, follow these steps:

- 
- |               |                                                                                                                                                                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Export the enclosures to a file.                                                                                                                                                                                                       |
| <b>Step 2</b> | Reinstall Fabric Manager (if you are installing on a new host, install Fabric Manager).                                                                                                                                                |
| <b>Step 3</b> | After the installation is complete, stop Fabric Manager Server.                                                                                                                                                                        |
| <b>Step 4</b> | Copy the RRD files from the old host to the new host. Place it in the MDS 9000 directory (on a Windows PC, the default installation location for this directory is C:\Program Files\Cisco Systems\DCM).                                |
| <b>Step 5</b> | On the new host, run <b>PMUpgrade.bat</b> from the MDS 9000\bin folder. This creates files and a new directory structure. There is a directory for each switch for which you have collected data.                                      |
| <b>Step 6</b> | Continue to collect data on a specific switch by copying the db subfolder from that switch's folder to the pm folder.                                                                                                                  |
| <b>Step 7</b> | On the new host, restart the Performance Manager Service (Windows) or Daemon (UNIX). You can use the <b>bin/PM.bat</b> file to do this, or you can choose <b>Performance &gt; Collector &gt; Restart</b> from the Fabric Manager menu. |
| <b>Step 8</b> | Re-import the enclosures on the new host.                                                                                                                                                                                              |
| <b>Step 9</b> | Be sure to turn off the original service on the old host.                                                                                                                                                                              |
- 

## Are there restrictions when using Fabric Manager across FCIP?

Fabric Manager will work with no restriction across an FCIP tunnel, as long as the tunnel is up. However, Fabric Manager cannot automatically discover a Cisco SN5428 mgmt IP address in the fabric. For that switch, it will display a red slash through an FCIP device because of a timeout error. It will still see all targets, initiators, and ISLs attached to a Cisco SN5428 (or any other switch) as long as they appear in the name server or FSPF.

To work around this, you can manually enter the IP address in the Switches table, and click Apply. If the community string is correct, the red slash will go away. Even if the community string is incorrect, double-clicking on the Cisco SN5428 will launch the web tool.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## How do I fix a "Please insure that FM server is running on localhost" message?

You may see this error message if you cannot connect to the fabric and your PC has multiple network interface cards. The problem may be that Fabric Manager is trying to communicate through the wrong interface (you can verify this by checking the FMServer.log file).

Generally it is best to let Fabric Manager choose the interface on startup. If you are getting the above error, something may have gone wrong.

To reset Fabric Manager so that it chooses the interface next time it starts, follow these steps:

- 
- |        |                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Open the server.properties file in the Fabric Manager installation directory. On a Windows platform, this file is in C:\Program Files\Cisco Systems\MDS 9000 by default. |
| Step 2 | Comment out the line: snmp.localaddress.                                                                                                                                 |
| Step 3 | Save and exit the file.                                                                                                                                                  |
| Step 4 | Restart Fabric Manager.                                                                                                                                                  |
- 



### Note

There are some cases where you would not want to do this, and should manually select the interface that Fabric Manager uses. For more information, see the [“How do I run Cisco Fabric Manager with multiple interfaces?”](#) section on page 13-20.

---

## How do I run Cisco Fabric Manager with multiple interfaces?

If your PC has multiple interfaces (NICs), the four Cisco Fabric Manager applications detect these interfaces automatically (ignoring loopback interfaces). Fabric Manager Client and Device Manager detect all interfaces on your PC each time you launch them, and allow you to select one. Fabric Manager Server and Performance Manager detect on initial install, and allows you to select one. You are not prompted again to choose an interface with these two applications.

There may be circumstances where you will want to change the interface you are using. For example:

- If you add an interface after you have installed Fabric Manager Server and/or Performance Manager
- If you decide to use a different interface than the one you initially selected
- If for any reason one of the Cisco Fabric Manager applications did not detect multiple interfaces

Refer to the following sections, depending on which application you want to recognize the interface.

- [Manually specifying an interface for Fabric Manager Server, page 13-20](#)
- [Manually specifying an interface for Fabric Manager Client or Device Manager, page 13-21](#)

## Manually specifying an interface for Fabric Manager Server

To specify an interface for Fabric Manager Server (including Performance Manager and Fabric Manager Web Services), follow these steps:

- 
- |        |                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Go to the MDS 9000 folder. On a Windows platform, this folder is at C:\Program Files\Cisco Systems\MDS 9000 by default. |
|--------|-------------------------------------------------------------------------------------------------------------------------|
-

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 2** Edit the server.properties file with a text editor.
  - Step 3** Scroll until you find the line: snmp.localaddress.
  - Step 4** If the line is commented, remove the comment character.
  - Step 5** Set the local address value to the IP address or interface name of the NIC you want to use.
  - Step 6** Save the file.
  - Step 7** Stop and restart Fabric Manager Server.
- 

## Manually specifying an interface for Fabric Manager Client or Device Manager

To specify an interface for the Fabric Manager Client or Device Manager, follow these steps:

- Step 1** Go to the MDS 9000/bin folder. On a Windows platform, this folder is at C:\Program Files\Cisco Systems\MDS 9000 by default.
  - Step 2** Edit the DeviceManager.bat file or the FabricManager.bat file.
  - Step 3** Scroll to the line that begins with set JVMARGS=
  - Step 4** Add the parameter -Device Managerds.nmsaddress=ADDRESS, where ADDRESS is the IP address or interface name of the NIC you want to use.
  - Step 5** Save the file and relaunch Fabric Manager Client or Device Manager.
- 

## How do I configure an HTTP proxy server?

If your network uses a proxy server for HTTP requests, make sure the Java Web Start Application Manager is properly configured with the IP address of your proxy server.

To configure a proxy server in the Java Web Start Application Manager, follow these steps:

- Step 1** Launch the Java Web Start application.
  - Step 2** Choose **File > Preferences** from the Java WebStart Application Manager.
  - Step 3** Choose the **Manual** radio button and enter the IP address of the proxy server in the HTTP Proxy field.
  - Step 4** Enter the HTTP port number used by your proxy service in the **HTTP Port** field.
  - Step 5** Click **OK**.
- 

## How do I clear the topology map?

If you have a switch that you have removed from the fabric, there will be a red X through the switch's icon. You can clear this information from the Fabric Manager client, or from the Fabric Manager server (which will clear the information for all clients) without having to reboot the switch.

To clear information from topology maps using Fabric Manager, follow these steps:

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

---

**Step 1** Click the **Refresh Map** icon in the Fabric pane.

This clears the information from the client.

**Step 2** Click **Purge Down Elements** in the Server menu.

This clears the information from the server.



**Caution**

---

Any devices not currently accessible (may be offline) are purged.

---

## How can I use Fabric Manager in a mixed software environment?

You can use Fabric Manager version 2.0(x) to manage a mixed fabric of Cisco MDS 9000 switches. Certain 2.0 feature tabs will be empty for any switches running a software version that does not support those features.

## How do I fix a "corrupted jar file" error when launching Fabric Manager?

If you get the following error:

```
An error occurred while launching the application Fabric Manager.
```

```
download error:corrupted jar file at <ipaddress>\Device Managerboot.jar
```

(Where <ipaddress> is that of the switch)

The error message you are getting indicates that the Java Web Start cache is corrupted. You can try clearing your Java Web Start cache first. To clear the Cache either run Java Web Start (from the Programs menu) and under the **preferences** select **clear cache**. Or do it manually by first making sure all Fabric Manager or Device Manager instances are closed and then deleting .javaws/cache. In the newer JREs this directory is created under Documents and Settings\USERNAME and in the older ones it used to be under Program Files\Java Web Start.

You can also browse beneath the cache folder and delete the offending IPAddress folder (e.g. cache/http/D10.0.0.1).

Also, check to make sure that the host is not running a virus checker / java blocker?

You also can run the uninstall program and delete .cisco\_mds directory, and then reinstall Fabric Manager.

## How do I search for devices in a fabric?

In Fabric Manager, you can search for one or more devices by different attributes, including pWWN. To perform a search in Fabric Manager, follow these steps:

---

**Step 1** Right-click the map and choose **Find Elements** from the drop-down menu.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

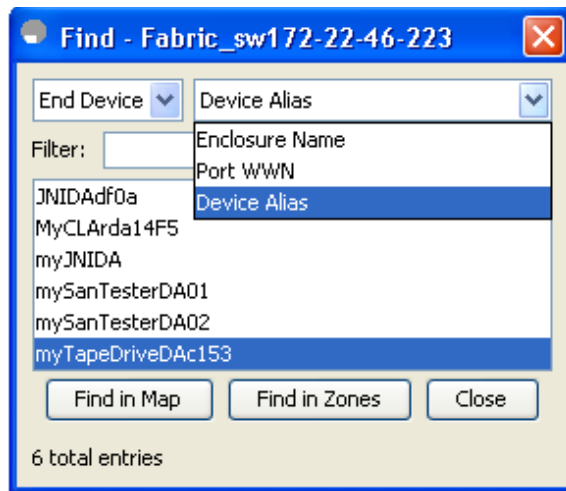
You see the Find Fabric dialog box as shown in [Figure 13-1](#).

**Step 2** Choose **End Device** from the left drop-down list.

**Step 3** Choose **Port WWN** from the right drop-down list.

You can also enter only part of the WWN and use a wildcard (\*) character (for example, you can enter **\*fb\*f8**).

**Figure 13-1 Find Fabric Dialog Box with End Device and Port WWN Selected**



**Step 4** Click **Find in Map**.

To search for devices in a zone, click **Find in Zones**. You see the device highlighted in the Fabric pane. Right-click any device to see the attributes for that device. You can also select a link leading to a device to see the attributes for the link.

## How do I search in a table?

In Fabric Manager, you can search for devices having one or more attributes. You can enter a search string in the Find dialog box and then use Next and Previous buttons to navigate through the results.

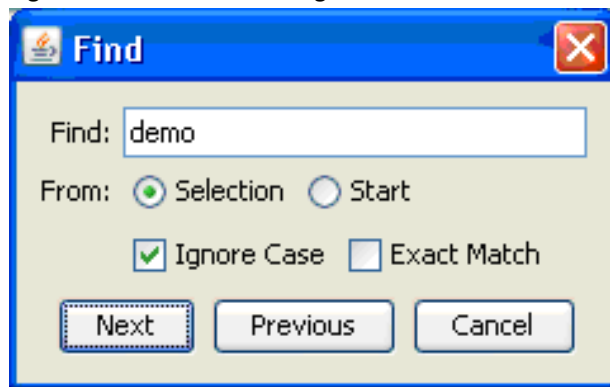
To perform a search inside a table in Fabric Manager, follow these steps:

**Step 1** Click the Find icon from the tool bar.

You see the Find dialog box as shown in [Figure 13-2](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 13-2 Find Dialog Box**



- Step 2** Enter the search string in the Find text box.
- Step 3** Click **Selection** to search in selected row(s).
- Step 4** Check **Ignore Case** to ignore case sensitivity.
- Step 5** Check **Exact Match** to search for the data value exactly matching the search string.
- Step 6** Click **Next** to search.
- Step 7** Click **Cancel** to close the dialog box.

## How does Fabric Manager Server licensing work?

You must install a Cisco MDS 9000 Family Cisco Fabric Manager Server package on at least one switch in each fabric where you intend to manage switches, if you intend to use the enhanced management capabilities the license package provides. You must also license all switches you plan to monitor with the Performance Manager (historical performance monitoring) feature. Failure to license all switches can prevent effective use of the Flow performance monitoring, so it is recommended to license all switches in each fabric managed by Cisco Fabric Manager Server.

You are free to try Cisco Fabric Manager Server capabilities prior to installing a license, but the those extended functions will stop working after the 120-day grace period expires. Standard Cisco Fabric Manager configuration and management capabilities will continue to be accessible without any licensed switches after the grace period expires.

## How do I manage multiple fabrics?

To monitor and manage multiple fabrics, you must persist one or more fabrics. Do this by checking the **Persist** checkbox on the **Server>Admin** dialog Fabric tab. You must also use switches running SAN-OS Release 1.3.x or later in both fabrics, and you must use the same user/password on both fabrics. Both fabrics must not be physically connected.

## How can I clear an orange X through a switch caused by license expiration?

If you are using a licensed feature and that license is allowed to expire, Fabric Manager shows a license violation, and an orange X is placed through the switch on the Fabric Manager map.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

To clear the license violation message and the orange X, stop the Cisco Fabric Manager service on the host, and restart it again.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*



## APPENDIX A

# Launching Fabric Manager in Cisco SAN-OS Releases Prior to 3.2(1)

---

This appendix provides instructions for launching Fabric Manager Client in Cisco SAN-OS releases prior to 3.2(1).

This Appendix contains the following sections:

- [Setting the Seed Switch in Cisco SAN-OS Releases 3.1\(1\) to 3.2\(1\), page A-1](#)
- [Setting the Seed Switch in Releases Prior to Cisco SAN-OS Release 3.1\(1\), page A-3](#)

## Setting the Seed Switch in Cisco SAN-OS Releases 3.1(1) to 3.2(1)



### Note

As of Cisco SAN-OS Release 3.1(1), the Fabric Manager login procedure changed. If you are running a version of Cisco SAN-OS that is earlier than Cisco SAN-OS 3.1(1), follow the login instructions in the [“Setting the Seed Switch in Releases Prior to Cisco SAN-OS Release 3.1\(1\)” section on page A-3](#).

From Cisco SAN-OS Release 3.1(1) to Release 3.2(1), you must log in to Fabric Manager Server before you discover or open fabrics, and these fabrics can have different user credentials. You can specify different SNMP communities per switch on the Web Server.



### Note

The default user name is **admin** and the default password is **password** for your initial login. This information is stored in the database. Both the Fabric Manager Server and the Web Server share the same user credential database.

To log in to Fabric Manager Server and to open a fabric, follow these steps:

### Step 1

Double-click the **Fabric Manager Client** icon on your workstation.

You see the Fabric Manager Server Login dialog box shown in [Figure A-1](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure A-1** Fabric Manager Server Login Dialog Box



- Step 2** Set FM Server to the IP address where you installed Fabric Manager Server, or set it to **localhost** if you installed Fabric Manager Server on your local workstation.

If you forget your password, you can run one of the following scripts:

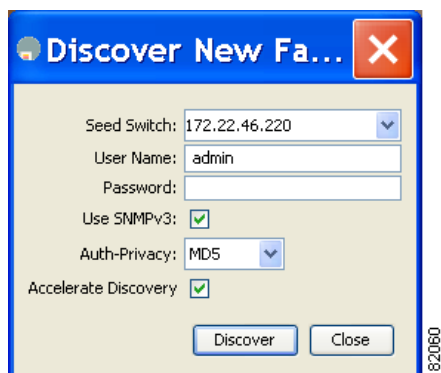
- **bin\webUserAdd.bat admin password** adds a user name and password to the Fabric Manager Server database.
- **bin\DBReset.bat** resets the database back to the initial state and removes any discovered fabrics.

Both of these scripts are available as UNIX .sh files.

- Step 3** Enter the Fabric Manager Server user name and password.
- Step 4** Check the **Use SNMP Proxy** check box if you want Fabric Manager Client to communicate with Fabric Manager Server through a TCP-based proxy server.
- Step 5** Click **Login**. After you successfully log in to Fabric Manager Server, you can set the seed switch and open the fabrics that you are entitled to access.

You see the Discover New Fabric dialog box shown in [Figure A-2](#).

**Figure A-2** Discover New Fabric Dialog Box



- Step 6** Set the fabric seed switch to the Cisco MDS 9000 Family switch that you want Fabric Manager to use.
- Step 7** Enter the user name and password for the switch.
- Step 8** Choose the Auth-Privacy option MD5-DES (default) when you log in.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

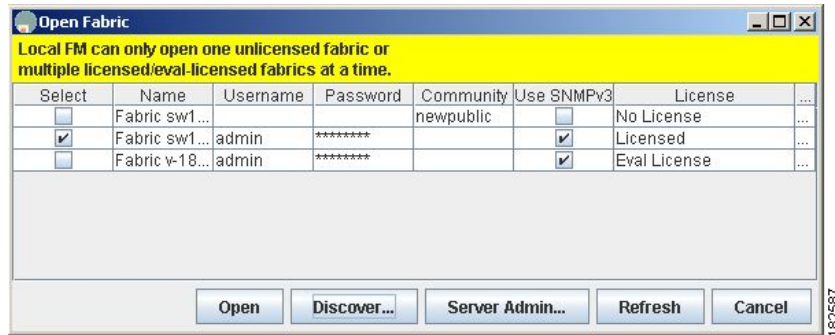
**Note**

The Accelerate Discovery check box should remain checked for normal operation. Uncheck this only if you have changed switch IP addresses. You may experience problems with SAN IDs in Fabric Manager if you uncheck this check box.

**Step 9** Click **Discover**.

You see the Open Fabric dialog box shown in [Figure A-3](#).

**Figure A-3** Open Fabric Dialog Box



**Step 10** Check the check box(es) next to the fabric(s) you want to open in the Select column, or click the **Discover** button to add a new fabric.

**Note**

As of Cisco SAN-OS Release 3.1(1) and later, opening multiple fabrics is a licensed feature. You will get a message if any of the fabrics discovered does not have a license.

**Note**

As of Cisco SAN-OS Release 3.1(2b), a license can be a permanent license, an evaluation license, or there are no licenses (all evaluation licenses have expired).

**Step 11** Click **Open** to open the fabric.

## Setting the Seed Switch in Releases Prior to Cisco SAN-OS Release 3.1(1)

**Note**

As of Cisco SAN-OS Release 3.1(1), the Fabric Manager login procedure changed. If you are running Cisco SAN-OS Releases 3.1(1) to 3.2(1), then follow the login instructions in the [“Setting the Seed Switch in Cisco SAN-OS Releases 3.1\(1\) to 3.2\(1\)”](#) section on page A-1.

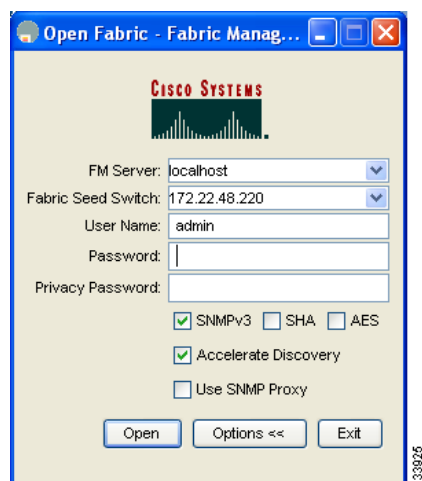
*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

When you run Fabric Manager, you must select a switch for Fabric Manager to use to discover the fabric. For releases earlier than Cisco SAN-OS Release 3.1(1), use the same user name and password on each of the multiple fabrics that you open, then log in directly to the MDS 9000 Family switch that you want Fabric Manager to use.

To set the seed switch if you are running a version of Cisco SAN-OS that is earlier than Cisco SAN-OS Release 3.1(1), follow these steps:

- 
- Step 1** Double-click the **Fabric Manager Client** icon on your workstation.  
You see the Fabric Manager Login dialog box shown in [Figure A-4](#).

**Figure A-4** Open Fabric Dialog Box



- Step 2** Click the **Options** button if necessary to expand the optional settings in this dialog box.
- Step 3** Set FM Server to the IP address where you installed Fabric Manager Server, or set it to **localhost** if you installed Fabric Manager Server on your local workstation.
- Step 4** Set the fabric seed switch to the MDS 9000 Family switch that you want Fabric Manager to use.
- Step 5** Enter the user name and password for the switch.
- Step 6** Check the **Use SNMP Proxy** check box if you want Fabric Manager Client to communicate with Fabric Manager Server through a TCP-based proxy server.




---

**Note** The Accelerate Discovery check box should remain checked for normal operation. Uncheck this only if you have changed switch IP addresses. You may experience problems with out of sync SAN IDs in Fabric Manager if you uncheck this check box.

---

- Step 7** Click **Open** to open the fabric.
-





# APPENDIX B

## Cisco Fabric Manager Unsupported Feature List

This appendix contains a list of features and functions not supported by Cisco Fabric Manager or Device Manager. This list is organized according to the chapter in which the feature would be described if it were supported. (See [Table B-1](#).)

**Table B-1**      *Features Not Supported by Cisco Fabric Manager or Device Manage*

| Part                                                 | Chapter/Category                  | Procedure                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2 Cisco MDS NX-OS Installation and Switch Management | Obtaining and Installing Licenses | Backing Up License Files<br>Moving Licences Between Switches                                                                                                                                                                                                                                    |
|                                                      | Initial Configuration             | Starting a Switch (Initial Setup)<br>Configuring Console Settings<br>Configuring COM1 and Modem Settings<br>Adjusting for Daylight Savings Time<br>Configuring the Initialization String<br>Basic Switch Configuration<br>Terminal Settings<br>File System Commands<br>Displaying File Contents |
|                                                      |                                   |                                                                                                                                                                                                                                                                                                 |
|                                                      | Software Images                   | Manual Upgrade on a Dual Supervisor Switch<br>Corrupted Bootflash Recovery                                                                                                                                                                                                                      |

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Table B-1**      **Features Not Supported by Cisco Fabric Manager or Device Manage (continued)**

| Part                            | Chapter/Category                      | Procedure                                                                                                                                                                                                                                                                                           |
|---------------------------------|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 | Working with Configuration Files      | Formatting External CompactFlash<br>Compressing and Uncompressing Files<br>Displaying the Last Lines in a File<br>Executing Commands Specified in a Script<br>Setting the Delay Time<br>Displaying Configuration Files<br>Unlocking the Startup Configuration File<br>Accessing Remote File Systems |
|                                 | Configuring High Availability         | Copying Images to the Standby Supervisor                                                                                                                                                                                                                                                            |
|                                 | Managing System Hardware              | Clock Modules                                                                                                                                                                                                                                                                                       |
|                                 | Managing Modules                      | Connecting to a Module<br>Preserving Module Configuration<br>Purging Module Configuration<br>EPLD Configuration<br>Configuring SSI Boot Image<br>Managing SSMs                                                                                                                                      |
| 3 Switch Configuration          | Configuring Interfaces                | Displaying the ALPA Cache Contents<br>Clearing the ALPA Cache<br>N-Port Identifier Virtualization (NPIV)                                                                                                                                                                                            |
|                                 | Scheduling Tasks                      | Schedule Configuration                                                                                                                                                                                                                                                                              |
| 4 Fabric Configuration          | Inter-VSAN Routing Configuration      | Inter-VSAN Routing (IVR) FICON Support<br>IVR Service Groups                                                                                                                                                                                                                                        |
| 6 IP Services                   | Configuring FCIP                      | Displaying and Clearing ARP Caches                                                                                                                                                                                                                                                                  |
|                                 | Configuring the SAN Extension Tuner   | Tuning Configuration                                                                                                                                                                                                                                                                                |
|                                 | Configuring IP Storage                | IPS Module Core Dumps                                                                                                                                                                                                                                                                               |
| 8 Network and Switch Monitoring | Monitoring Network Traffic Using SPAN | Remote SPAN                                                                                                                                                                                                                                                                                         |

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Table B-1**      *Features Not Supported by Cisco Fabric Manager or Device Manage (continued)*

| Part               | Chapter/Category                     | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10 Troubleshooting | Troubleshooting Your Fabric          | Loop Monitoring<br>Configuring CIM<br>CFS for FC Timers<br>Local Text Based Capture<br>Capturing FC Analyzer Frames Locally<br>Sending Captured FC Analyzer Frames to a Remote IP Address<br>Clearing Configured FC Analyzer Information<br>Displaying a List of Hosts Configured for Remote Capture<br>Using Fabric Analyzer Display Filters                                                                                                                                                                                                                                                                                                   |
|                    | Monitoring System Processes and Logs | Saving the Last Core to Flash<br>Kernel Core Dumps<br>System Health Initiation<br>Loopback Test Configuration Frequency<br>Hardware Failure Action<br>Tests for a Specified Module<br>Clearing Previous Error Reports<br>Online Health Management System <ul style="list-style-type: none"> <li>• Enabling and Disabling the OHMS</li> <li>• Enabling and Disabling Hardware Failure Action</li> <li>• Configuring Onboard Failure Logging</li> <li>• Clearing Previous Error Reports</li> <li>• Performing Tests for a Specified Module</li> <li>• Configuring Automatic Loopback Tests</li> <li>• Performing SERDES Loopback Tests</li> </ul> |

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*



## APPENDIX C

## Interface Nonoperational Reason Codes

If the administrative state for an interface is up and the operational state is down, the reason code differs based on the nonoperational reason code as described in [Table C-1](#).

**Table C-1** Reason Codes for Nonoperational States

| Reason Code                    | Description                                                                                                                                                                                                                                                                                                                                                                                                               | Applicable Modes |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| Link failure or not connected  | Physical layer link is not operational.                                                                                                                                                                                                                                                                                                                                                                                   | All              |
| SFP not present                | The small form-factor pluggable (SFP) hardware is not plugged in.                                                                                                                                                                                                                                                                                                                                                         |                  |
| Initializing                   | The physical layer link is operational and the protocol initialization is in progress.                                                                                                                                                                                                                                                                                                                                    |                  |
| Reconfigure fabric in progress | The fabric is currently being reconfigured.                                                                                                                                                                                                                                                                                                                                                                               |                  |
| Offline                        | Cisco MDS SAN-OS waits for the specified R_A_TOV time before retrying initialization.                                                                                                                                                                                                                                                                                                                                     |                  |
| Inactive                       | The interface VSAN is deleted or is in a suspended state.<br><br>To make the interface operational, assign that port to a configured and active VSAN.                                                                                                                                                                                                                                                                     |                  |
| Hardware failure               | A hardware failure is detected.                                                                                                                                                                                                                                                                                                                                                                                           |                  |
| Error disabled                 | Error conditions require administrative attention. Interfaces may be error-disabled for various reasons. For example: <ul style="list-style-type: none"><li>• Configuration failure.</li><li>• Incompatible buffer-to-buffer credit configuration.</li></ul> To make the interface operational, you must first fix the error conditions causing this state; and next, administratively shut down or enable the interface. |                  |

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Table C-1 Reason Codes for Nonoperational States (continued)**

| Reason Code                                     | Description                                                                                                                                                                                                | Applicable Modes            |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| Isolation due to ELP failure                    | Port negotiation failed.                                                                                                                                                                                   | Only E ports and TE ports   |
| Isolation due to ESC failure                    | Port negotiation failed.                                                                                                                                                                                   |                             |
| Isolation due to domain overlap                 | The Fibre Channel domains (fcdomain) overlap.                                                                                                                                                              |                             |
| Isolation due to domain ID assignment failure   | The assigned domain ID is not valid.                                                                                                                                                                       |                             |
| Isolation due to other side E port isolated     | The E port at the other end of the link is isolated.                                                                                                                                                       |                             |
| Isolation due to invalid fabric reconfiguration | The port is isolated due to fabric reconfiguration.                                                                                                                                                        |                             |
| Isolation due to domain manager disabled        | The fcdomain feature is disabled.                                                                                                                                                                          |                             |
| Isolation due to zone merge failure             | The zone merge operation failed.                                                                                                                                                                           |                             |
| Isolation due to VSAN mismatch                  | The VSANs at both ends of an ISL are different.                                                                                                                                                            |                             |
| Nonparticipating                                | FL ports cannot participate in loop operations. It may happen if more than one FL port exists in the same loop, in which case all but one FL port in that loop automatically enters nonparticipating mode. | Only FL ports and TL ports  |
| PortChannel administratively down               | The interfaces belonging to the PortChannel are down.                                                                                                                                                      | Only PortChannel interfaces |
| Suspended due to incompatible speed             | The interfaces belonging to the PortChannel have incompatible speeds.                                                                                                                                      |                             |
| Suspended due to incompatible mode              | The interfaces belonging to the PortChannel have incompatible modes.                                                                                                                                       |                             |
| Suspended due to incompatible remote switch WWN | An improper connection is detected. All interfaces in a PortChannel must be connected to the same pair of switches.                                                                                        |                             |



## APPENDIX D

# Managing Cisco FabricWare

---

The Cisco FabricWare software running on the MDS 9020 Switch offers Fibre Channel switching services that realize maximum performance. Cisco FabricWare provides networking features such as zoning, advanced security, nondisruptive software upgrades, diagnostics, a CLI with syntax resembling Cisco IOS, and standard interfaces for management applications.

This appendix contains the following sections:

- [Fibre Channel Support, page D-1](#)
- [Zone Configuration, page D-1](#)
- [Security, page D-2](#)
- [Events, page D-2](#)
- [Managing Cisco FabricWare with Fabric Manager, page D-3](#)

## Fibre Channel Support

Cisco FabricWare supports autoconfigured Fibre Channel ports capable of up to 4-Gbps bandwidth. Cisco FabricWare supports the following port types:

- E
- F
- FL
- Fx
- Auto

Cisco FabricWare supports Fabric Shortest Path First (FSPF) as the standard path selection protocol used by Fibre Channel fabrics. The FSPF feature is enabled by default on all Fibre Channel switches. Except in configurations that require special consideration, you do not need to configure any FSPF services. FSPF automatically calculates the best path between any two switches in a fabric.

## Zone Configuration

Zoning enables you to set up access control between storage devices or user groups. If you have administrator privileges in your fabric, you can create zones to increase network security and to prevent data loss or corruption. Zoning is enforced by examining the source-destination ID field. Cisco FabricWare does not support QoS, broadcast, LUN, or read-only zones.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

You can use the Fabric Manager zone configuration tool to manage zone sets, zones, and zone membership for switches running Cisco FabricWare. Cisco FabricWare supports zone membership by pWWN. Refer *Cisco MDS 9000 Family Fabric Manager Fabric Configuration Guide*.

## Security

Cisco FabricWare supports the following security features:

- RADIUS
- SSH
- User-based roles
- IP access control lists

Cisco FabricWare can use the RADIUS protocol to communicate with remote AAA servers. RADIUS is a distributed client/server protocol that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco MDS 9000 Family switches and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

You can access the CLI using the console (serial connection), Telnet, or Secure Shell (SSH). For each management path (console or Telnet and SSH), you can configure one or more of the following security control options: **local**, **remote (RADIUS)**, or **none**.

Using these access methods, you can configure the roles that each authenticated user receives when they access the switch. Cisco FabricWare supports two fixed roles: network administrator and network operator.

IP access lists (IP-ACLs) control management traffic over IP by regulating the traffic types that are allowed or denied to the switch. IP-ACLs can only be configured for the mgmt0 port.

Fabric Manager Server uses SNMPv1 and SNMPv2 to communicate with Cisco FabricWare.

## Events

You can monitor fabric and switch status for Cisco FabricWare switches through either a syslog server or an SNMP trap receiver.

The syslog, or system message logging software, saves messages in a log file or directs the messages to other devices. This feature provides you with the following capabilities:

- Provides logging information for monitoring and troubleshooting
- Allows you to select the types of captured logging information
- Allows you to select the destination server to forward the captured logging information

By default, the switch logs normal but significant system messages to a log file and sends these messages to the system console. You can specify which system messages should be saved based on the type of facility and the severity level. You can access logged system messages using the CLI or by saving them to a properly configured system message logging server.

You can configure the Cisco MDS 9020 Switch using the CLI to send notifications to SNMP managers when particular events occur. You can send these notifications as traps.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

# Managing Cisco FabricWare with Fabric Manager

Fabric Manager supports switches running Cisco FabricWare.

Table D-1 shows the supported features and where to find more information on that feature.

**Table D-1 FabricWare Features in Fabric Manager**

| Feature                            | FabricWare Capabilities                                                                                                                          | Guide                                                                                          |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Zones                              | Zone configuration<br>Zone membership by pWWN<br>No Cisco FabricWare support for QoS, broadcast, LUN, or read-only zones                         | Refer to the <i>Cisco MDS 9000 Family Fabric Manager Fabric Configuration Guide</i>            |
| Interfaces                         | 1/2/4 Fibre Channel autonegotiating ports                                                                                                        | Refer to the <i>Cisco MDS 9000 Family Fabric Manager Interfaces Configuration Guide</i>        |
| SNMP                               | SNMPv1 and SNMPv2c                                                                                                                               | Refer to the <i>Cisco MDS 9000 Family Fabric Manager System Management Configuration Guide</i> |
| Software images                    | Automated upgrades<br>Manual upgrades                                                                                                            | Refer to the <i>Cisco MDS 9000 Family Fabric Manager System Management Configuration Guide</i> |
| FLOGI, name server, FDMI, and RSCN | Displaying FLOGI details<br>Registering name server proxies<br>Displaying FDMI<br>RSCN statistics                                                | Refer to the <i>Cisco MDS 9020 Switch Configuration Guide and Command Reference</i> .          |
| Security                           | Configuring RADIUS<br>Configuring server groups<br>Configuring role-based authorization<br>Configuring user accounts<br>Configuring SSH services | Refer to the <i>Cisco MDS 9000 Family Fabric Manager Security Configuration Guide</i> .        |
| Fibre Channel routing              | FSPF global configuration<br>FSPF interface configuration                                                                                        | Refer to the <i>Cisco MDS 9020 Switch Configuration Guide and Command Reference</i> .          |
| IP services                        | IP access control lists on mgmt0                                                                                                                 | Refer to the <i>Cisco MDS 9000 Family Fabric Manager Security Configuration Guide</i> .        |
| System messages                    | System message logging configuration                                                                                                             | Refer to the <i>Cisco MDS 9000 Family Fabric Manager Fundamentals Configuration Guide</i> .    |
| Advanced configuration             | FC timer                                                                                                                                         | Refer to the <i>Cisco MDS 9000 Family Fabric Manager Fabric Configuration Guide</i>            |

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*



## INDEX

---

### A

#### AAA

- configuring information [7-57](#)

#### accounting

- viewing lists [7-10](#)

#### adapters

- Fibre Channel-to-Ethernet [9-2](#)

#### adminDown tooltip [13-14](#)

#### administrator passwords

- default [2-5](#)

#### Admin tab

- description [7-49](#)

#### aliases

- switching between global device aliases and fcalias [3-10](#)

- using as enclosure names [5-38, 5-39](#)

- using with Fabric Manager [3-10](#)

#### ALPA caches

- clearing [B-2](#)

- displaying contents [B-2](#)

#### ANSI T11 FC-GS-3

- support [2-17](#)

#### applications

- management [2-17](#)

#### ARP caches

- clearing [B-2](#)

- displaying [B-2](#)

#### authentication

- Fabric Manager Web Services [4-4](#)

---

### B

#### BB\_credits

- reason codes [C-1](#)

#### bitErrRTThresExceeded tooltip [13-14](#)

#### bootflash:

- file system [12-2](#)

- recovering from corruption [B-1](#)

- space requirements [12-3](#)

buffer-to-buffer credits. See BB\_credits

#### bundleMisCfg tooltip [13-14](#)

---

### C

#### CAs

- Fabric Manager Web Services [7-5](#)

#### channelAdminDown tooltip [13-14](#)

#### channelConfigurationInProgress tooltip [13-14](#)

#### channelOperSuspended tooltip [13-14](#)

#### CIM

- configuring [B-3](#)

- support [2-17](#)

#### Cisco MDS 9000 Family

- initial setup [2-2 to 2-12](#)

- starting a switch [2-1](#)

#### Cisco MDS SAN-OS

- software images [12-1](#)

#### Cisco Traffic Analyzer

- configuring with Performance Manager [11-10](#)

- description [9-3](#)

- installing (procedure) [9-3](#)

- using with Fabric Manager [9-2](#)

#### CLI

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- accessing [D-2](#)
- firewall [4-2](#)
- clients
  - disconnecting [7-54](#)
  - viewing [7-54](#)
- clock modules
  - managing [B-2](#)
- COM1 ports
  - configuring [B-1](#)
- command schedulers
  - configuring [B-2](#)
- command scripts
  - executing [B-2](#)
- communities
  - adding [7-55](#)
  - removing [7-56](#)
- CompactFlash
  - slot0: [12-2](#)
- configuration files
  - displaying [B-2](#)
- configurations
  - changing initial [2-12](#)
- connectivity
  - troubleshooting tool [5-41](#)
- console ports
  - parameters [2-2](#)
- console settings
  - configuring [B-1](#)
- core dumps
  - IPS modules [B-2](#)
- core files
  - saving to CompactFlash [B-3](#)
- custom reports
  - creating a template [7-39](#)
  - modifying a template [7-46](#)
- Custom tab
  - description [7-39](#)

---

## D

- D\_S\_TOV
  - errors when setting [13-7](#)
- data
  - management [2-17](#)
- database files
  - resolving lock errors [7-49](#)
- daylight saving time
  - adjusting for [B-1](#)
- default networks
  - configuring [2-7, 2-10](#)
- default users
  - description [2-3](#)
- deniedDueToPortBinding tooltip [13-14](#)
- desktops
  - shortcuts not visible [13-4](#)
- Device Manager
  - color definitions [6-6](#)
  - connection failures [13-10](#)
  - context menus [6-7](#)
  - description [2-15, 6-1](#)
  - disk images not visible [13-7](#)
  - downgrading [13-4](#)
  - FAQs [13-1](#)
  - icons [6-4](#)
  - installation failures [13-6, 13-7](#)
  - label definitions [6-6](#)
  - launching (procedure) [6-2](#)
  - login failure recovery [13-6](#)
  - managing ports [6-7](#)
  - PortChannels [6-7](#)
  - preferences [6-8](#)
  - setting preferences [6-8](#)
  - tabs [6-5](#)
  - trunking [6-7](#)
  - upgrade failures [13-4](#)
  - upgrading [13-4](#)
  - using interface (figure) [6-3](#)

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- viewing port status [6-6](#)
  - viewing supervisor modules [6-7](#)
  - viewing switch modules [6-7](#)
  - devices
    - discovery [10-1](#)
    - management [2-17](#)
    - modifying groupings (procedure) [5-37](#)
    - searching in Fabric Manager [13-22](#)
  - DirectX
    - installing [13-6](#)
  - DNS
    - configuring [2-7, 2-10](#)
    - configuring IP addresses [2-7](#)
  - documentation
    - related documents [i-lxiii](#)
  - domainAddrAssignFailureIsolation tooltip [13-14](#)
  - domain IDs
    - duplicates causing errors [13-13](#)
    - failures [C-2](#)
  - domainInvalidRCFReceived tooltip [13-14](#)
  - domainManagerDisabled tooltip [13-14](#)
  - domainMaxReTxFailure tooltip [13-14](#)
  - domain names
    - configuring [2-7](#)
  - domainOtherSideEportIsolation tooltip [13-14](#)
  - domainOverlapIsolation tooltip [13-14](#)
  - domains
    - overlap isolations [C-2](#)
  - DPVM
    - wizard [5-40](#)
  - drill down reports
    - description [7-1](#)
- 
- ## E
- E\_D\_TOV
    - errors when setting [13-7](#)
  - elpFailureClassFParamErr tooltip [13-14](#)
  - elpFailureClassNParamErr tooltip [13-15](#)
  - elpFailureInvalidFlowCTLParam tooltip [13-15](#)
  - elpFailureInvalidPayloadSize tooltip [13-15](#)
  - elpFailureInvalidPortName tooltip [13-15](#)
  - elpFailureInvalidTxBBCredit tooltip [13-15](#)
  - elpFailureIsolation tooltip [13-15](#)
  - elpFailureLoopbackDetected tooltip [13-15](#)
  - elpFailureRatovEdtovMismatch tooltip [13-15](#)
  - elpFailureRevMismatch tooltip [13-15](#)
  - ELP failures
    - reason codes [C-2](#)
  - elpFailureUnknownFlowCTLCode tooltip [13-15](#)
  - enclosure names
    - aliases [5-38, 5-39](#)
  - end devices
    - viewing storage port traffic and errors [7-16](#)
  - EPLD images
    - configuring [B-2](#)
  - ePortProhibited tooltip [13-15](#)
  - E ports
    - isolation [C-2](#)
  - eppFailure tooltip [13-15](#)
  - errorDisabled tooltip [13-15](#)
  - error messages
    - gen error messages [13-7](#)
  - error reports
    - clearing previous [B-3](#)
  - escFailureIsolation tooltip [13-15](#)
  - ESC failures
    - reason codes [C-2](#)
  - Ethernet interfaces
    - viewing performance information [7-24](#)
  - events
    - displaying using Device Manager [10-5](#)
    - displaying using Fabric Manager [10-5](#)
    - displaying using Fabric Manager Web Services [10-5](#)
    - viewing [7-10](#)
  - exchange link parameter failures. See ELP failures
  - exporting
    - Performance Manager reports as CSV [11-9](#)

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

external CompactFlash

formatting [B-2](#)

## F

fabric

editing monitoring [7-52](#)

Fabric Analyzer

using display filters [B-3](#)

fabricBindingDBMismatch tooltip [13-15](#)

fabricBindingDomainInvalid tooltip [13-15](#)

fabricBindingNoRspFromPeer tooltip [13-15](#)

fabricBindingSWWNNotFound tooltip [13-15](#)

Fabric Manager

authentication [4-1 to ??](#)

browser support [2-20](#)

Cisco Traffic Analyzer [9-2](#)

connection failures [13-10](#)

corrupted jar file errors [13-22](#)

description [2-1, 2-14](#)

detachable tables [5-27](#)

downgrading [13-4](#)

downloading software [2-19](#)

error recovery [13-7](#)

FAQs [13-1](#)

FCIP [13-19](#)

installation failures [13-6, 13-7](#)

installing [2-18](#)

integrating with other tools [2-41](#)

ISL statistics [11-3](#)

Java support [2-19](#)

launching troubleshooting [13-3](#)

login failure recovery [13-6](#)

missing Information pane [13-9](#)

mixed software environments [13-22](#)

network discovery [5-35](#)

preinstallation tasks [2-19](#)

problems with map changes [13-8](#)

running behind firewalls [2-41](#)

running with multiple NICs [13-20](#)

searching for devices [13-22](#)

setting preferences [5-33](#)

shows as disabled service [13-6](#)

support operating systems [2-19](#)

uninstalling [2-44](#)

upgrade failures [13-4](#)

upgrading [2-39, 13-4](#)

Fabric Manager authentication

description [4-1](#)

discovery best practices [4-3](#)

Web Server support [4-4](#)

Fabric Manager Clients

advanced mode [5-2](#)

description [2-14, 5-1](#)

displaying physical attributes [5-23](#)

Fabric pane [5-27](#)

filtering [5-23](#)

Information pane [5-26](#)

main menu [5-16](#)

setting preferences [5-33](#)

status bar [5-33](#)

toolbar icons (table) [5-20](#)

troubleshooting tools [5-41](#)

using interface (figure) [5-15](#)

wizards [5-40](#)

Fabric Manager Server

authentication [4-2](#)

configuring preferences [7-55](#)

continuously monitoring fabrics [3-6](#)

database failed to start [13-10](#)

description [2-14, 3-1](#)

disk space requirements [3-1](#)

fabric discovery [4-3](#)

features [3-1](#)

full fabric rediscovery [3-10](#)

installation overview [3-2](#)

installing [3-2](#)

licensing [3-5](#)

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- local host error messages [13-20](#)
- modifying settings [3-9](#)
- passwords [3-10](#)
- performing administrative tasks [7-49](#)
- performing configuration tasks [7-49](#)
- polling periods [3-10](#)
- properties files [3-7](#)
- Red Hat Linux support [3-1](#)
- Solaris support [3-1](#)
- user names [3-10](#)
- viewing logs [7-66](#)
- Windows support [3-1](#)
- Fabric Manager Web Server
  - authentication [4-4](#)
  - configuring RADIUS authentication [4-4](#)
  - configuring TACACS+ authentication [4-5](#)
  - description [2-16](#)
- Fabric Manager Web Services
  - configuring communities [7-55](#)
  - configuring users [7-57](#)
  - description [7-1](#)
  - exporting performance data [7-3](#)
  - initial screen [7-9](#)
  - installing [7-3](#)
  - launching [7-7](#)
  - navigating [7-2](#)
  - printing [7-3](#)
  - recovering passwords [7-49](#)
  - TCP ports [7-4, 7-5](#)
  - using with SSL [7-5](#)
- fabrics
  - discovery [5-35](#)
  - management [2-17](#)
  - monitoring [3-6](#)
- FabricWare
  - events [D-2](#)
  - Fabric Manager support (table) [D-3](#)
  - Fibre Channel support [D-1](#)
  - installing Fabric Manager Web Services [7-3](#)
  - roles [D-2](#)
  - security [D-2](#)
  - SNMP traps [D-2](#)
  - syslog traps [D-2](#)
  - zoning support [D-1](#)
- FAQs
  - Device Manager [13-1](#)
  - Fabric Manager [13-1](#)
- fcaliases
  - using with Fabric Manager [3-10](#)
- FC-GS-3 requests
  - device grouping support [5-37](#)
- FCIP
  - restrictions [13-19](#)
- fcipPortAdminCfgChange tooltip [13-15](#)
- fcipPortKeepAliveTimerExpire tooltip [13-15](#)
- fcipPortMaxReTx tooltip [13-16](#)
- fcipPortPersistTimerExpire tooltip [13-16](#)
- fcipPortSrcAdminDown tooltip [13-16](#)
- fcipPortSrcLinkDown tooltip [13-16](#)
- fcipSrcModuleNotOnline tooltip [13-16](#)
- fcipSrcPortRemoved tooltip [13-16](#)
- FCoE
  - wizard [5-40](#)
- fcotChksumErr tooltip [13-16](#)
- fcotNotPresent tooltip [13-16](#)
- fcotVendorNotSupported tooltip [13-16](#)
- fcspAuthenfailure tooltip [13-16](#)
- fctimers
  - configuring CFS [B-3](#)
- Fibre Channel analyzers
  - capturing frames locally [B-3](#)
  - clearing configured information [B-3](#)
  - sending frames to remote IP addresses [B-3](#)
- FICON
  - Fabric Manager Client support [5-2](#)
- ficonBeingEnabled tooltip [13-16](#)
- ficonNoPortnumber tooltip [13-16](#)
- ficonNotEnabled tooltip [13-16](#)

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

ficonVsanDown tooltip [13-16](#)

## FICP

wizard [5-40](#)

## files

compressing [B-2](#)

displaying contents [B-1](#)

displaying last lines [B-2](#)

uncompressing [B-2](#)

## filtering

end port groups [5-32](#)

switch groups [5-32](#)

## firewalls

configuring [2-14](#)

running with Fabric Manager [2-41](#)

firstPortNotUp tooltip [13-16](#)

firstPortUpAsEport tooltip [13-16](#)

## flows

performance statistics [8-1](#)

viewing performance information [7-23](#)

## FL ports

nonparticipating codes [C-2](#)

frequently asked questions. See FAQs

## FSPF

flow statistics [8-6 to ??](#)

path selection protocol [D-1](#)

support [2-17](#)

## FTP

support [2-16](#)

## G

### Generation 2 switching modules

installing in Generation 1 chassis [12-17](#)

### Gigabit Ethernet interfaces

viewing performance information [7-24](#)

## H

### hardware

viewing list [7-10](#)

### hardware failures

configuring actions [B-3](#)

### Health tab

description [7-9](#)

### high availability

software upgrades [12-5](#)

### historical data

preserving [13-19](#)

### hosts

performance statistics [8-1](#)

## HTTP

port used [2-42](#)

support [2-16](#)

### HTTP proxy servers

configuring [13-21](#)

## HTTPS

support [2-16](#)

hwFailure tooltip [13-16](#)

## I

### icons

Device Manager [6-4](#)

### IDs

login IDs [2-6](#)

### images

See kickstart images; software images; system images

Software Installation Wizard [12-8](#)

images. See kickstart images; software images; system images

### in-band access

configuring [2-9](#)

IPFC [2-13](#)

### in-band management

configuring [2-9, 2-10](#)



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Ethernet connection [2-18](#)
- IPFC connection [2-18](#)
- logical interface [2-9](#)
- incomAdminRxBBCreditPerBuf tooltip [13-16](#)
- incompatibleAdminMode tooltip [13-16](#)
- incompatibleAdminRxBBCredit tooltip [13-16](#)
- incompatibleAdminRxBufferSize tooltip [13-16](#)
- incompatibleadminSpeed tooltip [13-16](#)
- initialization string
  - configuring [B-1](#)
- initializing tooltip [13-16](#)
- install all command
  - failure cases [12-7](#)
- interfaceRemoved tooltip [13-16](#)
- interfaces
  - nonoperational reason codes [C-1](#)
  - reason codes [C-1](#)
- Internet Explorer
  - Fabric Manager support [2-20](#)
- invalidAttachment tooltip [13-16](#)
- invalidConfig tooltip [13-16](#)
- invalidFabricBindExh tooltip [13-16](#)
- inventories
  - managing [10-3](#)
  - viewing details for switches [7-32](#)
  - viewing details for VSANs [7-31](#)
  - viewing information [7-30](#)
  - viewing ISL information [7-36](#)
  - viewing module details [7-34](#)
  - viewing zone information [7-38](#)
- Inventory tab
  - description [7-29](#)
- IP-ACLs
  - wizard [5-40](#)
  - See also IPv4-ACLs; IPv6-ACLs
- IP addresses
  - management interfaces [2-3](#)
- IPFC
  - errors caused by configuration [13-8](#)

- in-band access [2-13](#)
- in-band management [2-18](#)
- IP routing
  - enabling [2-7, 2-11](#)
- IPS modules
  - core dumps [B-2](#)
- IPv4-ACLs
  - FabricWare support [D-2](#)
- IPv4 default gateways
  - configuring [2-10](#)
- iSCSI
  - Fabric Manager Client support [5-2](#)
  - wizard [5-40](#)
- ISLs
  - graph past 24 hours performance [7-27](#)
  - performance statistics [8-1](#)
  - statistics [11-3](#)
  - viewing detailed inventory information [7-36](#)
  - viewing performance information [7-17](#)
- IVR
  - Fabric Manager Client support [5-2](#)
  - FICON support [B-2](#)
  - service groups [B-2](#)
  - wizard [5-40](#)

---

## J

- Java
  - execution failures [13-6](#)
- java.lang.ArrayIndexOutOfBoundsException  
errorArrayIndexOutOfBoundsException error [13-7](#)
- Java RMI
  - ports used [2-42](#)
- Java Runtime Environment. See JRE
- Java Web Start
  - checking installation [13-3](#)
  - clearing the cache [13-6](#)
  - Fabric Manager support [2-19](#)
  - hangs on the download dialog [13-5](#)

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

not detected [13-4](#)

running from command line [13-5](#)

setting up on \*.jnlp files [13-5](#)

## JNLP

verifying settings [13-3](#)

## JRE

Fabric Manager requirements [7-4](#)

---

## K

### kernel core dumps

configuring [B-3](#)

### kickstart images

description [12-2](#)

KICKSTART variable [12-1](#)

selecting for supervisor modules [12-2](#)

### Konqueror

configuring for Java Web Start [13-5](#)

---

## L

### licenses

backing up files [B-1](#)

Fabric Manager [13-24](#)

moving between switches [B-1](#)

One-Click License Install failed [13-9](#)

unsupported features [B-1](#)

viewing switch information [7-33](#)

wizard [5-40](#)

linkFailCreditLossB2B tooltip [13-17](#)

linkFailCreditLoss tooltip [13-17](#)

linkFailDebounceTimeout tooltip [13-17](#)

linkFailLineCardPortShutdown tooltip [13-17](#)

linkFailLinkReset tooltip [13-17](#)

linkFailLIPF8Rcvd tooltip [13-17](#)

linkFailLIPRcvdB2B tooltip [13-17](#)

linkFailLossOfSignal tooltip [13-17](#)

linkFailLossOfSync tooltip [13-17](#)

linkFailLRRcvdB2B tooltip [13-17](#)

linkFailNOSRcvd tooltip [13-17](#)

linkFailOLSRcvd tooltip [13-17](#)

linkFailOPNyRETB2B tooltip [13-17](#)

linkFailOPNyTMOB2B tooltip [13-17](#)

linkFailPortInitFail tooltip [13-17](#)

linkFailPortUnusable tooltip [13-17](#)

linkFailRxQOverflow tooltip [13-17](#)

linkFailTooManyINTR tooltip [13-17](#)

### link failures

reason codes [C-1](#)

linkFailure tooltip [13-17](#)

### Linux [2-35](#)

Fabric Manager support [2-19](#)

installing Fabric Manager Web Services [7-4](#)

install scripts [2-35](#)

### logins

failure recovery [13-6](#)

### logs

increasing log window size [13-10](#)

viewing information [7-66](#)

viewing using Device Manager [10-4](#)

viewing using Fabric Manager Web Server [10-4](#)

loopbackDiagFailure tooltip [13-17](#)

loopbackIsolation tooltip [13-17](#)

### loopback tests

configuring frequency [B-3](#)

### loops

monitoring [B-3](#)

---

## M

### management

role-based [5-40](#)

### management access

configuring in-band [2-9 to 2-12](#)

configuring out-of-band [2-5 to 2-9](#)

description [2-13](#)

in-band [2-4](#)

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- out-of-band [2-4](#)
- management interfaces
  - IP addresses [2-3](#)
- management protocols
  - supported (table) [2-16](#)
- map preferences
  - Automatically Save Layout default [5-35](#)
  - Detach Overview Window default [5-35](#)
  - Display End Device Labels default [5-34](#)
  - Display End Devices default [5-34](#)
  - Display Unselected VSAN Members default [5-34](#)
  - Expand Loops default [5-34](#)
  - Expand Multiple Links default [5-34](#)
  - Layout New Devices Automatically default [5-35](#)
  - Open New Device Manager Each Time default [5-34](#)
  - Override Preferences for Non-default Layout default [5-35](#)
  - Select Switch or Link from Table default [5-35](#)
  - Use Quick Layout when Switch has >=30 End Devices default [5-35](#)
- maps
  - black squares [13-14](#)
  - brown squares [13-14](#)
  - clearing license orange X [13-24](#)
  - clearing topologies [13-21](#)
  - color definitions [13-13](#)
  - default preferences [5-34](#)
  - freezing the layout look [13-13](#)
  - green squares with mode [13-14](#)
  - grouping end devices [5-37](#)
  - highlighting [5-29](#)
  - icon descriptions [5-27](#)
  - light gray squares [13-14](#)
  - module warnings [13-13](#)
  - no squares [13-14](#)
  - orange crosses [13-14](#)
  - orange squares with mode [13-14](#)
  - purging down elements [5-30](#)
  - red crosses [13-14](#)
  - red line through switches [13-13](#)
  - red squares [13-14](#)
  - refreshing [5-30](#)
  - saving [5-30](#)
  - shows two switches when only one [13-13](#)
  - tab descriptions [5-29](#)
  - upgrade software without losing map settings [13-19](#)
  - viewing large [5-29](#)
  - Visio diagrams [5-30](#)
- maps module failuresmaps
  - fan failuresmaps
    - power supply failures [13-13](#)
- McAfee Internet Suite 6.0 Professional
  - Device Manager installation failures [13-7](#)
  - Fabric Manager installation failures [13-7](#)
- messages
  - selecting severity level [7-54](#)
- mgmt0
  - out-of-band management [2-18](#)
- mgmt0 interfaces
  - configuring out-of-band access [2-6](#)
  - out-of-band access [2-13](#)
- modems
  - configuring settings [B-1](#)
- module configurations
  - preserving [B-2](#)
  - purging [B-2](#)
- modules
  - connecting to [B-2](#)
  - replacing [12-18](#)
- module tests
  - configuring [B-3](#)
- Mozilla
  - configuring for Java Web Start [13-5](#)
- multiple fabrics [10-3](#)
  - managing [13-24](#)

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

---

## N

### network administrator roles

FabricWare [D-2](#)

### network monitoring

device discovery [10-1](#)

mapping topologies [10-2](#)

### network operator roles

FabricWare [D-2](#)

### NICs

manually specifying for Device Manager [13-21](#)

manually specifying for Fabric Manager Client [13-21](#)

manually specifying for Fabric Manager Server [13-20](#)

### nondisruptive upgrades

methods [12-5](#)

### nonParticipating tooltip [13-17](#)

### notifications

adding forwards [7-53](#)

conditions for sending [7-63](#)

removing forwards [7-54](#)

### NPIV

configuring [B-2](#)

N-Port identifier virtualization. See NPIV

### NPV

wizard [5-40](#)

### ntop freeware

batch files [9-5](#)

modifying launch scripts [9-5](#)

### NTP servers

configuring [2-8](#)

---

## O

### offline tooltip [13-17](#)

### OHMS

configuring [B-3](#)

### ohmsExtLBTest tooltip [13-17](#)

Online Health Management System. See OHMS

### Opera

configuring for Java Web Start [13-5](#)

other tooltip [13-17](#)

### out-of-band access

mgmt0 interfaces [2-13](#)

### out-of-band management

configuring [2-5, 2-10](#)

Ethernet connection [2-18](#)

---

## P

### PAA-2s

Cisco Traffic Analyzer [9-3](#)

description [9-2](#)

### PAAs

compared with PAA-2s [9-3](#)

### parentDown tooltip [13-18](#)

### passwords

administrator [2-3](#)

assigning using Fabric Manager [5-40](#)

recovering [7-49](#)

setting administrator default [2-9](#)

### pcAnyWhere

replacing with DirectX [13-6](#)

stopping [13-6](#)

### peerFCIPPortClosedConnection tooltip [13-18](#)

### peerFCIPPortResetConnection tooltip [13-18](#)

### performance

configuring collections [7-60](#)

customizing reports [7-39](#)

custom monitoring [7-27](#)

data [8-3](#)

event triggers [8-2](#)

graphs [11-7](#)

historical monitoring [11-4](#)

host-optimized port groups [11-7](#)

ISL statistics (procedure) [11-3](#)

monitoring [8-1](#)

monitoring in Device Manager (procedure) [11-2](#)

per-port monitoring (procedure) [11-2](#)

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- real-time monitoring [11-1](#)
- summary reports [11-7](#)
- tables [11-7](#)
- using thresholds [8-2](#)
- viewing future predictions [7-26](#)
- viewing summaries [7-14](#)
- performance collections
  - adding [7-60](#)
  - configuring thresholds [7-63](#)
  - removing [7-61](#)
- Performance Manager
  - architecture [8-1](#)
  - authentication [4-4](#)
  - configuring data collection [8-3](#)
  - configuring flows [8-3](#)
  - configuring with Traffic Analyzer [11-10](#)
  - creating a flow [11-4](#)
  - creating collections [11-4](#)
  - data collection [8-2](#)
  - data interpolation [8-2](#)
  - description [2-15](#)
  - exporting as CSV [11-9](#)
  - reports [11-7](#)
  - shows as disabled service [13-6](#)
  - using thresholds [8-2](#)
  - verifying collections [3-6](#)
  - viewing reports [11-7](#)
  - wizard for configuring [11-5](#)
- Performance Manager reports
  - exporting as XML [11-9](#)
  - generating top 10 [11-8](#)
  - viewing events [11-8](#)
  - viewing graphs [11-7](#)
  - viewing host-optimized port group performance [11-7](#)
  - viewing summary reports [11-7](#)
  - viewing tables [11-7](#)
- Performance tab
  - description [7-13](#)
- polling periods
  - changing [3-10](#)
- Port Analyzer Adapters 2. See PAA-2s
- portBindFailure tooltip [13-18](#)
- portBlocked tooltip [13-18](#)
- portChannelMembersDown tooltip [13-18](#)
- PortChannels
  - configuring using Device Manager [6-7](#)
  - creation dialog box too small [13-8](#)
  - down states [C-2](#)
  - incompatible modes [C-2](#)
  - incompatible remote switch [C-2](#)
  - incompatible speeds [C-2](#)
  - wizard [5-40](#)
- portFabricBindFailure tooltip [13-18](#)
- portGracefulShutdown tooltip [13-18](#)
- port groups
  - host-optimized performance [11-7](#)
- ports
  - disabling using Device Manager [6-7](#)
  - enabling using Device Manager [6-7](#)
- Port Security
  - wizard [5-40](#)
- portVsanMismatchIsolation tooltip [13-18](#)
- preferences
  - Confirm Deletion default [5-34](#)
  - default [5-33](#)
  - Device Manager [6-8](#)
  - Export Tables with Format default [5-34](#)
  - Fabric Manager Clients [5-33](#)
  - Show CFS Warnings default [5-34](#)
  - Show Device Name by default [5-33](#)
  - Show End Device Using default [5-34](#)
  - Show Shortened iSCSI Names default [5-34](#)
  - Show Timestamps as Date/Time default [5-34](#)
  - Show WorldWideName (WWN) Vendor default [5-34](#)
  - Telnet Path default [5-34](#)
  - Use Secure Shell instead of Telnet default [5-34](#)

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

---

## Q

### QoS

wizard [5-40](#)

---

## R

### RADIUS

FabricWare support [D-2](#)

rcfInProgres tooltip [13-18](#)

### reason codes

description (table) [C-1](#)

### recovery

passwords [7-49](#)

### Red Hat Linux

Fabric Manager Server [3-1](#)

### remote AAA server

delayed authentication [4-2](#)

### remote file systems

accessing [B-2](#)

### remote SPAN

configuring [B-2](#)

### resources

management [2-17](#)

### role-based management

controlling access [5-40](#)

### roles

adding web services roles [7-58](#)

privileges [5-40](#)

removing web services roles [7-59](#)

### round-trip response time

monitoring [9-3](#)

### RRD

configuring database [7-64](#)

### RSPAN

configuring [B-2](#)

---

## S

### SAN extension tuner

configuring [B-2](#)

SAN operating system. See Cisco MDS SAN-OS

schedulers. See command schedulers

### SCP

support [2-16](#)

### scripts

FMServer.sh [2-35](#)

### SCSI

monitoring frame counts [9-3](#)

monitoring I/Os per second [9-3](#)

monitoring read throughput [9-3](#)

monitoring traffic throughput [9-3](#)

### SCSI sessions

monitoring status [9-3](#)

### SD ports

Cisco Traffic Analyzer [9-4](#)

### serial console ports

accessing switches [2-13](#)

### services

restarting [7-50](#)

starting [7-50](#)

stopping [7-50](#)

### services modules

replacing [12-18](#)

### setup command

using [2-12](#)

### SFPs

not present reason codes [C-1](#)

### SFTP

support [2-16](#)

### shell scripts

\$HOME/.cisco\_mds9000/bin directory [13-4](#)

DeviceManager.sh [13-4](#)

FabricManager.sh [13-4](#)

for uninstalling Fabric Manager [2-45](#)

### shortcuts

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- not visible on desktops [13-4](#)
- SNMP
  - enabling access [2-7](#)
  - port used [2-42](#)
  - proxy services [2-14](#)
- SNMP\_TRAP
  - port used [2-42](#)
- SNMP community strings
  - configuring [2-10](#)
- SNMP preferences
  - Enable Audible Alert when Event Received default [5-34](#)
  - Retry request 1 time(s) after 5 sec timeout default [5-34](#)
  - Trace SNMP packets in Log default [5-34](#)
- SNMPv1
  - FabricWare support [D-2](#)
  - support [2-16](#)
- SNMPv2
  - FabricWare support [D-2](#)
- SNMPv2c
  - support [2-16](#)
- SNMPv3
  - support [2-16](#)
- software images
  - default settings [12-18](#)
  - selecting for supervisor modules [12-2](#)
  - space requirements [12-4](#)
  - upgrade prerequisites [12-3 to ??](#)
  - upgrading SAN-OS images [12-1](#)
  - variables [12-1](#)
- software installation
  - Software Installation Wizard [12-8](#)
- software upgrades
  - disruptive [12-5](#)
  - mechanisms [12-5](#)
  - Software Installation Wizard [12-8](#)
- Solaris [2-35](#)
  - Fabric Manager Server [3-1](#)
  - installing Fabric Manager Web Services [7-4](#)
  - install scripts [2-35](#)
- SPAN
  - configuring on switch ports [9-4](#)
  - monitoring traffic [9-1](#)
- SPAN ports
  - viewing detailed traffic information [7-25](#)
- srcPortNotBound tooltip [13-18](#)
- SSH
  - enabling [2-8, 2-11](#)
  - FabricWare support [D-2](#)
  - port used [2-42](#)
  - support [2-16](#)
- SSI boot images
  - configuring [B-2](#)
- SSL certificates
  - using with Fabric Manager Web Services [7-5](#)
- SSMs
  - managing [B-2](#)
- standby supervisor modules
  - boot alert [12-17](#)
  - boot variable version [12-16](#)
  - copying image to [B-2](#)
  - managing bootflash: [12-17](#)
- startup configuration files
  - unlocking [B-2](#)
- static routes
  - configuring [2-7](#)
- statistics
  - SCSI I/O [9-3](#)
- storage devices
  - performance statistics [8-1](#)
- storage traffic
  - viewing performance information [7-23](#)
- subnet masks
  - configuring switches [2-3](#)
  - initial configuration [2-7, 2-11](#)
- summary reports
  - description [7-1](#)

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Sun JRE

Fabric Manager support [2-19](#)

## Supervisor-1 modules

migrating from Supervisor-2 modules (note) [12-16](#)

selecting software images [12-2](#)

## Supervisor-2 modules

Generation 1 chassis [12-17](#)

migrating from Supervisor-1 modules [12-16 to ??](#)

select software images [12-2](#)

## supervisor modules

managing standby bootflash: [12-17](#)

migrating to Supervisor-2 modules [12-16 to ??](#)

replacing [12-16, 12-18](#)

standby boot alert [12-17](#)

standby supervisor boot variable version [12-16](#)

upgrading a dual supervisor switch [B-1](#)

viewing using Device Manager [6-7](#)

suspendedByMode tooltip [13-18](#)

suspendedBySpeed tooltip [13-18](#)

suspendedByWWN tooltip [13-18](#)

swFailure tooltip [13-18](#)

## switches

accessing [2-13](#)

initial setup [2-2](#)

starting [2-1](#)

starting up [B-1](#)

upgrading with dual supervisors [B-1](#)

viewing license information [7-33](#)

## switching modules

replacing [12-18](#)

viewing using Device Manager [6-7](#)

## switch management

architecture [2-17](#)

in-band [2-18](#)

out-of-band [2-18](#)

## switch port interfaces

configuring default [2-11](#)

## switch ports

configuring trunk modes [2-11](#)

## syslog

port used [2-42](#)

viewing information [7-11](#)

viewing registration information [7-52](#)

viewing with Events tab [7-9](#)

## system health

initiating [B-3](#)

## system images

description [12-2](#)

selecting for supervisor modules [12-2](#)

SYSTEM variable [12-1](#)

## system messages

viewing [7-11](#)

viewing using Device Manager [10-4](#)

viewing using Fabric Manager Web Server [10-4](#)

viewing with Events tab [7-9](#)

---

## T

## tables

filtering [7-3](#)

navigating [7-3](#)

searching for information [7-3](#)

## Telnet

enabling [2-8, 2-11](#)

port used [2-42](#)

support [2-16](#)

## templates

creating for custom reports [7-39](#)

modifying custom report templates [7-46](#)

## terminals

configuring settings [B-1](#)

## TFTP

port used [2-42](#)

support [2-16](#)

## thresholds

baselines for performance [8-2](#)

## time delays

setting [B-2](#)



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

tooManyInvalidFLOGIs tooltip [13-18](#)

topologies

clearing maps [13-21](#)

mapping [10-2](#)

topology map

mapping multiple fabrics [10-3](#)

topology maps

custom [10-2](#)

description [10-2](#)

enclosures [10-3](#)

saving custom layouts (procedure) [10-2](#)

tovMismatch tooltip [13-18](#)

traffic

managing using Cisco Traffic Analyzer [9-2](#)

monitoring using Cisco Traffic Analyzer [9-2](#)

Traffic Analyzer. See Cisco Traffic Analyzer

traps

viewing registration information [7-52](#)

troubleshooting

Fabric Manager tools [5-41](#)

trunking

configuring using Device Manager [6-7](#)

trunkNotFullyActive tooltip [13-18](#)

## U

UDP traffic

blocking [2-14](#)

UNIX

install scripts [2-35](#)

launching Fabric Manager Web Services [7-7](#)

UNIX issues

parent menus disappear [13-12](#)

too many open files error [13-12](#)

web browser cannot find web server [13-12](#)

upgradeInProgress tooltip [13-18](#)

upgrades. See disruptive upgrades; nondisruptive upgrades; software upgrades

upgrading

switches [B-1](#)

user accounts

creating additional at setup [2-5](#)

User-based roles

FabricWare support [D-2](#)

users

adding [7-57](#)

default [2-3](#)

removing [7-58](#)

## V

Visio diagrams

saving maps as [5-30](#)

vsanInactive tooltip [13-18](#)

vsanMismatchIsolation tooltip [13-18](#)

VSANs

flow statistics [8-6](#)

mismatches [C-2](#)

wizard [5-40](#)

## W

Windows

Fabric Manager Server [3-1](#)

Fabric Manager support [2-19](#)

installing Fabric Manager Web Services [7-4](#)

Windows issues

blue screen [13-11](#)

Device Manager window content disappears [13-11](#)

Fabric Manager window content disappears [13-11](#)

icons disappear from desktop [13-11](#)

printing causes an application crash [13-11](#)

SCP/SFTP failures [13-12](#)

text fields are too small [13-11](#)

Windows XP hangs [13-11](#)

Windows workstations

modifying [2-15](#)

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## wizards

- DPVM Wizard [5-40](#)
- FCIP Wizard [5-40](#)
- FCoE Wizard [5-40](#)
- IP ACL Wizard [5-40](#)
- iSCSI Wizard [5-40](#)
- IVR Zone Wizard [5-40](#)
- License Install Wizard [5-40](#)
- NPV Wizard [5-40](#)
- PortChannel Wizard [5-40](#)
- Port Security Wizard [5-40](#)
- QoS Wizard [5-40](#)
- Software Install Wizard [5-40](#)
- VSAN Wizard [5-40](#)
- Zone Edit Tool Wizard [5-40](#)

## WWNs

- suspended connection [C-2](#)

---

## X

## XML

- support [2-17](#)

---

## Z

- zoneMergeFailureIsolation tooltip [13-18](#)

## zone policies

- configuring [2-11](#)

- zoneRemoteNoRespIsolation tooltip [13-18](#)

## zones

- displayed as bold [13-9](#)
- troubleshooting tools [5-41](#)
- viewing inventory information [7-38](#)
- wizard [5-40](#)

## zoning

- FabricWare support [D-1](#)