



Installation and Configuration

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.

This chapter contains the following sections:

- [About Cisco Fabric Manager, page 1-1](#)
- [Installing the Management Software, page 1-6](#)
- [Upgrading the Management Software, page 1-9](#)
- [Downgrading the Management Software, page 1-9](#)
- [Launching the Management Software, page 1-10](#)
- [Integrating Cisco Fabric Manager with Other Management Tools, page 1-11](#)
- [Running Fabric Manager Behind a Firewall, page 1-12](#)
- [Uninstalling the Management Software, page 1-13](#)

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 Configuration Guide* or the *Cisco MDS 9020 Switch Configuration Guide and Command Reference Guide*. For details on managing switches running Cisco FabricWare, see the [“Managing Cisco FabricWare with Fabric Manager” section on page C-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 Services

Send documentation comments to mdsfeedback-doc@cisco.com.

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. See [Chapter 2, “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. See [Chapter 3, “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:

- external and internal loopback test
- flash files
- create cli user
- security - iscsi users
- quiese pc
- 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 8080, you need to modify your workstation settings.

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 localhost under the Exceptions section.

Send documentation comments to mdsfeedback-doc@cisco.com.

Step 5 Click OK to save your changes.

See the “[Running Fabric Manager Behind a Firewall](#)” section on page 1-12.

Device Manager

The Device Manager presents 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 4, “Device Manager.”](#)

Performance Manager

Performance Manager provides 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. See [Chapter 33, “Performance Monitoring.”](#)

Fabric Manager Web Services

The Fabric Manager Web Services 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 Services, see [Chapter 5, “Fabric Manager Web Services.”](#)

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 1-1](#) lists the management protocols that Fabric Manager supports to access, monitor, and configure the Cisco MDS 9000 Family of switches .

Table 1-1 ***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.

Send documentation comments to mdsfeedback-doc@cisco.com.

Table 1-1 Supported Management Protocols (continued)

Management Protocol	Purpose
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.
XML/CIM over HTTP/HTTPS	Includes CIM server support for designing storage area network management applications to run on Cisco SAN-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:

Send documentation comments to mdsfeedback-doc@cisco.com.

- 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.

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.

Send documentation comments to mdsfeedback-doc@cisco.com.

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/Downgrade - The installer detects your current version of Fabric Manager and Device Manager, and it provides the option to upgrade or downgrade. 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 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.



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 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 username and password for all the switches in the fabric

Cisco MDS SAN-OS Release 2.1(1a) or later supports AAA authentication using RADIUS, TACACS+ or local SNMP users.

The Cisco Fabric Manager software executable files reside on each supervisor module of each Cisco MDS 9000 Family switch running Cisco MDS SAN-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 pm Cisco.com at the following website:

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

The Cisco Fabric Manager management software has been tested with the following software:

- Operating Systems
 - Windows 2000, 2003, XP

Send documentation comments to mdsfeedback-doc@cisco.com.

- Solaris 2.8
- Redhat Linux 7.2
- Java
 - Sun JRE and JDK 1.4.0, 1.4.1, 1.4.2, and 1.5.0

**Note**

Fabric Manager Release 2.1(2a) or later support JRE and JDK 1.5.0. Earlier Fabric Manager releases should use JRE and JDK 1.4.2.

- Java Web Start 1.2 and 1.0.1
- Browsers
 - Internet Explorer 5.5 or later
 - Netscape 6 or later
 - Mozilla 1.0 or later

Installation Procedure

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

To install Fabric Manager from the CD-ROM, navigate to the Fabric Manager installation notes and follow the directions.

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 your workstation, follow these steps:

Step 1 Optionally, enter the IP address or host name of the supervisor module running Cisco MDS SAN-OS in the Address or Location field of your browser.

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 not, a link is provided to the appropriate Sun Microsystems web page so you can install it. Fabric Manager looks for version 1.4(x) during installation.

The supervisor module HTTP server displays the installation window.

Step 2 Click the link to the Sun Java Virtual Machine software (if required) and 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**

In some cases, license validation from Cisco partners requires Java version 1.4.2_04 or later. If you cannot install licenses from a Cisco partner, check to make sure your Java version is at least 1.4.2_04.

Send documentation comments to mdsfeedback-doc@cisco.com.

**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.

- Step 3** Click on the desired installation link (**Fabric Manager**, **Device Manager**, or **Fabric Manager Web Services and Performance Manager**).

**Note**

If Performance Manager generates errors on installation make sure that Fabric Manager and Performance Manager are installed in the same directory.

- Step 4** Select an installation folder for Fabric Manager on your workstation, as shown in [Figure 1-1](#). The default location is C:\Program Files\Cisco Systems\MDS 9000 for Windows. 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.

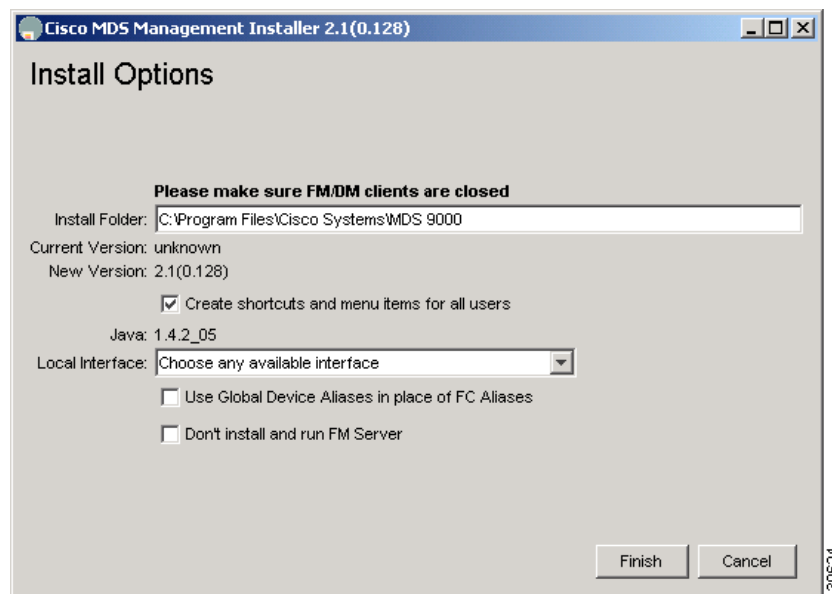
- Step 5** Check the **Use Global Aliases in place of FC Aliases** if you want to use global device aliases or replace existing per VSAN FC aliases with global device aliases.

**Tip**

After installation, you can choose to use global aliases by setting **fabric.globalAlias** to true in the server.properties file. In Fabric Manager Release 2.1(2) or later, you can select **Server > Admin** and check the **Device Alias** check box to use global aliases, or you can uncheck **Device Alias** to use FC aliases.

- Step 6** Check the **don't install and run FM Server** if you are installing just the Fabric Manager client on a remote workstation.

Figure 1-1 *Install Options*



Send documentation comments to mdsfeedback-doc@cisco.com.

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. Three services are started: Fabric Manager Server, Database, and Web Server. The Performance Manager server is installed but the service is not started at install time, as certain setup steps must be completed first.

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, FMPersist.sh, PMCollector.sh and FMWebClient.sh. All server-side data and Performance Manager data are stored under the install directory.

Fabric Manager client cannot run without the server component, Fabric Manager Server. The server component is downloaded and installed when you download and install Fabric Manager or Device 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.

Upgrading the Management Software

If you log into a switch running Cisco MDS SAN-OS with Fabric Manager or 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 1-6](#). You can also upgrade the software at any time by entering the IP address or host name of the supervisor module with the later version of software in the Address (Location) field of your browser.

Downgrading the Management Software

You can manage switches on your fabric with a later version of Fabric Manager than the version of Cisco MDS SAN-OS or Cisco FabricWare on the switches, but you cannot manage all features on switches with a later version of the switch software.

Downgrading to Release 2.x or Later

To downgrade from any Cisco MDS SAN-OS or Cisco FabricWare Release 2.x or later to an earlier version of Release 2.x, follow these steps:

-
- | | |
|---------------|--|
| Step 1 | Close all instances of Fabric Manager Client or Device Manager on your workstation. |
| Step 2 | Enter the IP address or host name of the supervisor module with the lower version of software in the Address or Location field of your browser and follow the installation steps. See the “Installing the Management Software” section on page 1-6 . |
-

Downgrading to Cisco MDS SAN-OS Release 1.3(x) or Earlier

To downgrade the management software from any Cisco MDS SAN-OS or Cisco FabricWare Release 2.x or later to Release 1.3(x) or earlier, follow these steps:

Send documentation comments to mdsfeedback-doc@cisco.com.

-
- Step 1** Close all instances of Fabric Manager Client or Device Manager on your workstation.
 - Step 2** Choose **Start > Programs > Cisco MDS 9000 > Uninstall** to uninstall Fabric Manager on Windows. Type `/usr/local/cisco_mds9000/uninstall.sh` or `$HOME/cisco_mds9000/uninstall.sh` to uninstall Fabric Manager on UNIX, depending on where Fabric Manager was installed.
 - Step 3** Enter the IP address or host name of the supervisor module with the lower version in the Address or Location field of your browser.
 - Step 4** Click on the desired installation link (**Fabric Manager**, **Device Manager**, or **Fabric Manager Web Services and Performance Manager**).
 - Step 5** Select an installation folder for Fabric Manager on your workstation.
-

Unless you specify a different directory on a Windows PC, the version 1.3(x) software is installed in the default location of `.\Documents and Settings\USER_ID\cisco_mds9000`. A Cisco MDS program group is created under **Start > Programs**. 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.

Launching the Management Software

To launch the Fabric Manager (Fabric View) or Device Manager (Device View and Summary View), follow these steps:

-
- Step 1** Double-click the **Fabric Manager** icon or the **Device Manager** icon on your desktop or select the option from the Windows Start menu.

If you started Fabric Manager, the Fabric Manager server loads. You see a log-in screen for Fabric Manager or Device Manager. (You briefly see a command-line window).
 - Step 2** Click **Options** to expand the login screen if necessary to select the seed switch and SNMP configuration.
 - Step 3** Enter the IP address or device name in the Device Name(s) field, or select an IP address from the list of previously accessed devices from the drop-down menu to the right of the Device Name(s) field.
 - Step 4** Leave the **SNMPv3** check box checked to select SNMP version 3. Otherwise, uncheck the check box to use SNMP version 2.



Note The default authentication digest used for storing user names and passwords is MD5. In case you selected SHA instead, the relative check box in the Fabric Manager initial login screen should be checked.

- Step 5** Enter a **User Name** and **Password**.
- Step 6** If the SNMPv3 Privacy option is enabled, enter the **Privacy Password** used for encrypting management traffic.

The Privacy option causes all management traffic to be encrypted while, with SNMPv3, user names and passwords are always encrypted.

Send documentation comments to mdsfeedback-doc@cisco.com.

**Note**

You can create users with management traffic encryption (so a Privacy password is required) or no management traffic encryption (no Privacy password is required). Requiring a Privacy password, and making it different from the authentication password, ensures stronger security but may cause AAA problems.

- Step 7** 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. See the [“Fabric Manager Server Proxy Services” section on page 1-2](#).

**Note**

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 8** Optionally, select the **Local Interface** for Fabric Manager client. In Fabric Manager Release 2.1(2) or later, Fabric Manager automatically detect the correct interface to use.

- Step 9** Click **Open**.

You see either the Fabric Manager or the Device Manager.

**Note**

When logging into Fabric Manager or Device Manager, the local SNMP database is checked first. If no username entry is found, the AAA database is checked.

**Note**

If you have an incomplete view of your fabric, rediscover the fabric with a user that has a network administrator or network operator role.

Integrating Cisco Fabric Manager with Other Management Tools

You can use Fabric Manager, Device Manager, and Performance Manager with other management tools. Here is a brief description of these tools. For more information on these tools and how they work together with the Cisco Fabric Manager management applications, see [Chapter 35, “Troubleshooting Your Fabric,”](#)

- 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 required the PAA to transport MDS SPAN traffic to a Windows PC or workstation.

Send documentation comments to mdsfeedback-doc@cisco.com.

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.

By default, Fabric Manager client component and Device Manager use the first available UDP port for receiving SNMP responses. The UDP SNMP Trap local ports are (1162 for Fabric Manager, and 1163 or 1164 for Device Manager). Fabric Manager Client also opens TCP RMI port 9099. If Device Manager is opened from the Fabric Manager client, it listens on the first available UDP port for Fabric Manager requests.

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:

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

- On a UNIX desktop, uncomment the following:

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



Note

UDP port 161 on the firewall must be open for incoming traffic. If the firewall blocks outgoing responses from snmp, then you can control which local ports DM or FM should open.

The Fabric Manager Server proxy services feature, available in Cisco MDS SAN-OS Release 2.1(1a) or later, uses a configurable TCP port (9189 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:

- java.rmi.registry.port = 9099
- java.rmi.server.remoteObjectPort = 9199

As long as these two ports are opened, the Fabric Manager client can connect to the server. There may be other TCP ports connected to Fabric Manager Client, but they are initiated by the server, which is behind the firewall.

Below is a list of all ports used by the Fabric Manager applications:

Common to all applications

- SSH 22 (TCP)
- TELNET 23 (TCP)
- HTTP 80 (TCP)
- TFTP 69 (UDP)
- SYSLOG 514 (UDP)

Fabric Manager Server and Performance Manager

- SNMP_TRAP 2162 (UDP)
- SNMP picks a random free local port (UDP) - (can be changed in server.properties)
- Java RMI 9099, 9199 to 9299 (TCP)

Fabric Manager Client

Send documentation comments to mdsfeedback-doc@cisco.com.

- Java RMI 9099, 9199 to 9299 (TCP)
- SNMP picks a random free local port. (UDP) or 9189 (TCP) if SNMP proxy is enabled (can be changed in server.properties)

Device Manager

- SNMP_TRAP 1163 to 1170 (UDP) (picks one available in this range)
- SNMP picks a random free local port (UDP) or 9189 (TCP) if SNMP Proxy is enabled (can be changed in server.properties)

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.
- 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 For older installations, delete the .cisco_mds9000 folder. You will have to 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.



Note You cannot downgrade from Fabric Manager Release 2.x to Fabric Manager Release 1.3(x). If you want to run Fabric Manager Release 1.3(x) on a PC that is running Fabric Manager Release 2.x, you must first uninstall Release 2.x and then install Release 1.3. Fabric Manager will not work if you have Release 2.x and Release 1.3 installed on the same PC.

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.
-

Send documentation comments to mdsfeedback-doc@cisco.com.