



CHAPTER 2

Installation of Cisco MDS SAN-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.

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 2-12](#)
- [Where Do You Go Next?, page 2-13](#)
- [About Cisco Fabric Manager, page 2-13](#)
- [Installing the Management Software, page 2-18](#)
- [Upgrading the Management Software, page 2-36](#)
- [Upgrading Fabric Manager Server and Fabric Manager Standalone Version Using the Fabric Manager Update Installer, page 2-37](#)
- [Integrating Cisco Fabric Manager with Other Management Tools, page 2-38](#)
- [Running Fabric Manager Behind a Firewall, page 2-38](#)
- [Uninstalling the Management Software, page 2-40](#)

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.

Before you can configure a switch, follow these steps:

-
- Step 1** Verify the following physical connections for the new Cisco MDS 9000 Family switch:

Send documentation comments to mdsfeedback-doc@cisco.com

- 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 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.

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:

Send documentation comments to mdsfeedback-doc@cisco.com

- 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 [“Role-Based Authorization”](#) section on page 39-1).

You must explicitly configure a strong 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 strong password (see the [“User Accounts”](#) section on page 39-10). If you configure and subsequently forget this new password, you have the option to recover this password (see the [“Recovering the Administrator Password”](#) section on page 39-19).

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 [Figure 2-1](#) and [Chapter 43, “Configuring IP Services”](#)).

Send documentation comments to mdsfeedback-doc@cisco.com

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 the new password for the administrator is a requirement and cannot be skipped.



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

Enter the password for admin: **2004asdf*1kj18**

Send documentation comments to mdsfeedback-doc@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 on page 39-10](#).

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 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.

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 [“Role-Based Authorization” section on page 39-1](#) for information on default roles and permissions.

**Note**

User login IDs must contain non-numeric characters.

a. Enter the user login ID.

Enter the user login ID: *user_name*

b. Enter the user password.

Enter the password for user_name: *user-password*

Step 6 Enter **yes** (yes is the default) to create an SNMPv3 account.

Configure SNMPv3 Management parameters (yes/no) [y]: **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-only SNMP community string (yes/no) [n]: **yes**

a. Enter the SNMP community string.

Send documentation comments to mdsfeedback-doc@cisco.com

SNMP community string: *snmp_community*

Step 8 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 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 IP address: *ip_address*

b. Enter the mgmt0 subnet mask.

Mgmt0 IP 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.

IP 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** (yes is the default) to enable IP routing capabilities.

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

c. Enter **yes** (yes is the default) to configure a static route (recommended).

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

Send documentation comments to mdsfeedback-doc@cisco.com

- d. Enter **yes** (yes is the default) to configure the default network (recommended).

Configure the default network: (yes/no) [y]: **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** (yes is the default) to configure the DNS IP address.

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

Enter the DNS IP address.

DNS IP 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** (yes is the default) to enable Telnet service.

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

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

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

- Step 14** Enter the SSH key type (see the “[Generating the SSH Server Key Pair](#)” section on page 39-16) that you would like to generate.

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

- 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 **on** (off is the default) to configure the PortChannel auto-create state.

Configure default port-channel auto-create state (on/off) [off]: **on**

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

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

Send documentation comments to mdsfeedback-doc@cisco.com

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 “[Zone Set Distribution](#)” section on page 30-25).

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

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 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
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 (see [Chapter 15, “Software Images”](#)).

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 [Chapter 1, “Configuring and Managing VSANs”](#)).

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

**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 on page 39-10.

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**

b. Enter **no** (no is the default) to configure the read-only SNMP community string.

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

c. Enter the SNMP community string.

SNMP community string: *snmp_community*

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*

Send documentation comments to mdsfeedback-doc@cisco.com

- 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.
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 “[Generating the SSH Server Key Pair](#)” section on page 39-16) 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.

Send documentation comments to mdsfeedback-doc@cisco.com

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 **off** (off is the default) to configure the PortChannel auto-create state.

Configure default port-channel auto-create state (on/off) [off]: **off**

- Step 18** 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 19** Enter **no** (no is the default) to disable a full zone set distribution (see the “[Zone Set Distribution](#)” section on page 30-25).

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 20** 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 21** Enter **yes** (yes is default) to use and save this configuration.

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

Send documentation comments to mdsfeedback-doc@cisco.com



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 (see [Chapter 15, “Software Images”](#)).

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.
```

Accessing the Switch

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.

Send documentation comments to mdsfeedback-doc@cisco.com

Figure 2-2 **Switch Access Options**

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.

To use the CLI, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

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 CLI 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 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

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto: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. 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:

- External and internal loopback test
- Flash files
- 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 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.

Send documentation comments to mdsfeedback-doc@cisco.com

- 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 2-38.

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 6, “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 60, “Performance Monitoring.”](#)

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 Server.”](#)

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.

Send documentation comments to mdsfeedback-doc@cisco.com

Table 2-1 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 - 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.



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 user name 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 on Cisco.com at the following website:

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

Send documentation comments to mdsfeedback-doc@cisco.com

Supported Software



Note

For the latest information on supported software, refer to the *Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 3.2(1)*.

Cisco Fabric Manager has been tested with the following software:

- Operating Systems
 - Windows 2000 SP4, 2003 SP2, XP SP2
 - Red Hat Enterprise Linux AS Release 4
 - Solaris (SPARC) 8, 9 and 10
 - VMWare Server 1.0, VMWare ESX Server 3.5

Table 2-2 VMWare Server

Base Operating System	Virtual Operating System
Windows 2000 SP4	Windows XP SP2
Windows 2000 SP4	Windows 2000 SP4

- Java
 - Sun JRE and JDK 1.5(x) is supported
 - Java Web Start 1.2, 1.0.1 and 1.5
- Browsers
 - Internet Explorer 6.x and 7.0



Note

Internet Explorer 7.0 is not supported on Windows 2000 SP4.

- Firefox 1.5 and 2.0
- 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 4)
 - PostgreSQL 8.1 (Solaris 8, 9 and 10)
- Security
 - Cisco ACS 3.1 and 4.0
 - PIX Firewall
 - IP Tables
 - SSH v2
 - Global Enforce SNMP Privacy Encryption
 - HTTPS

Send documentation comments to mdsfeedback-doc@cisco.com

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.

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 2-20.



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 2-24. 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 2-20.

Installing the Database

Before you install Fabric Manager, you must install a database. As of Cisco SAN-OS Release 3.1(2b), you can use Oracle Database 10g Express. Your other choice is PostgreSQL. Its a best practice to backup all the rrd file in \$INSTALL/pm/db before upgrade.



Note

Its a best practice to backup all the rrd file in \$INSTALL/pm/db before upgrade.

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.

Send documentation comments to mdsfeedback-doc@cisco.com**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 change the default Oracle admin port and to create a database account.

```
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 only supported on Microsoft Windows. It is not supported on UNIX systems.

**Note**

For information about backing up the Oracle database, click the following link:

http://download.oracle.com/docs/cd/B25329_01/doc/admin.102/b25107/backrest.htm#i1004902 or use the exp/imp utility at 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. Click the following link: <http://www.postgresql.org/docs/8.1/static/app-pgdump.html>.

Send documentation comments to mdsfeedback-doc@cisco.com

Installing PostgreSQL



Note

If you choose to install PostgreSQL, you must make sure that the Secondary Logon Service is running and you must also disable any security software you are running, as PostgreSQL may not install certain folders or users.

To install the PostgreSQL database on Windows, follow the instructions in the “[Installing Fabric Manager](#)” section on page 2-24.

Before installing PostgreSQL on Solaris 8, you might have to complete the following steps in order for PostgreSQL to install correctly:

Step 1 Set the load library path.

```
crle -c /var/ld/ld.config -l
/lib:/usr/lib:/usr/local/lib:{pg_install_dir}/usr/local/pgsql/lib:{pg_install_dir}/usr/
local/lib
```

Step 2 Set the following two properties in /etc/system.

```
set semsys:seminfo_semmni=512
set semsys:seminfo_semms=512
```

Step 3 Once you complete Step 2, reboot your Solaris workstation after you sync.

Step 4 Launch the installer script.

```
./install.sh {pg_install_dir}
```



Note

If you monitor a large fabric on the solaris, then manually copy \$INSTALLDIR/conf/postgresql_sol_big.conf to \$INSTALLDIR/db/data/postgresql.conf, and restart the Postgres server with the new configuration.



Note

Before starting the installation, ensure that you have logged in as a Superuser.

To install the PostgreSQL database on Solaris, follow these steps:

Step 1 To install PostgreSQL, run the following commands:

```
cd /tmp/pginstall
./install.sh
```

Step 2 When you install PostgreSQL, all the libraries in /usr/local/lib and pgsq are stored in /usr/local/bin. There might be conflicting libraries or dependencies that can cause an incorrect or incomplete PostgreSQL installation. For more information, go to <http://www.postgresql.org>.

Step 3 When the installation is finished, you must create a database user to login to the database. To create a database user, run the following command:

```
createuser -s -d -r -l -P -U postgres admin
```

Step 4 Enter the database User in the **DB User** field.

Step 5 Enter database password for new role in the **DB Password** field.

Step 6 Repeat the password in the **Confirm DB Password** field.

Send documentation comments to mdsfeedback-doc@cisco.com

**Note**

The installer does not permit any password less than six characters. Choose a strong password that includes both uppercase and lowercase letters, special characters, and numbers. For example, **testABC#136**.

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 8, ensure that the UDP buffer size is at least 64k.

```
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.

To install the PostgreSQL database on Linux, follow these steps:

Step 1 To install PostgreSQL, run the following commands:

```
cd /tmp/pginstall
./install.sh
```

Step 2 When you install PostgreSQL, all the libraries and binaries are stored in **/usr/lib** and **/usr/bin**, respectively. There might be conflicting libraries or dependencies that can cause an incorrect or incomplete PostgreSQL installation. For more information, go to <http://www.postgresql.org>.

Step 3 When the installation is finished, you must create a database user to login to the databases. To create a database user, run the following command:

```
createuser -s -d -r -l -P -U postgres admin
```

Step 4 Enter a **password** for the new role.

Step 5 Re-enter the **password**.

The database user ID must be provided in the Fabric Manager Installer.

Step 6 To stop and start the postmaster (PostgreSQL Database Server), run the following command:

```
/etc/init.d/postgresql [stop|start]
```

Database Backup and Restore-Postgres

The Fabric Manager uses Postgres Database as the default database. The Fabric Manager backup utility uses Postgres `pg_dump` utility, to dump all database content to an ASCII dump file. Restore utility uses `psql` to re-create data using the dump file.

Send documentation comments to mdsfeedback-doc@cisco.com

<http://www.postgresql.org/docs/current/interactive/app-pgdump.html>

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

Backup

To perform a backup of the FM database, follow these command 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

Restore

To restore FM database, you must have a good backup file, and stop FMServer before restoration. Run restore, follow these commands on Linux Solaris. (assume INSTALLDIR is the top directory of Fabric Manager installation).

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

Importing PM Statistics Data to Fabric Manager

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

-
- Step 1** Stop the Fabric Manger Server.
 - Step 2** Copy the "**existing**" rrd file (from prior installation) to \$INSTALLDIR/pm/db.
 - Step 3** Run the "\$INSTALLDIR/bin/pm.bat s".
 - Step 4** Restart the Fabric Manager Sever.
 - Step 5** Add fabric to PM collection using WebClient.

The PM historic statistics shall be available on WebClient after an hour run.

Installing Fabric Manager

As of Cisco SAN-OS Release 3.2(1), 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.

Send documentation comments to mdsfeedback-doc@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** Install the database that is to be used with Fabric Manager by following the instructions in the “[Installing the Database](#)” section on page 2-20.
- Step 3** Copy the Fabric Manager jar file m9000-fm-3.2.0.136.jar from the CD-ROM to a folder on the Solaris workstation.
- Step 4** Launch the installer using the following command:
- ```
java -Xms512m-Xmx512m -jar m9000-fm-3.2.0.136 -jar
```
- Step 5** 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.

---

**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 vitally important if the default PostgreSQL is used with Fabric Manager, as this database requires the local console for all installations and upgrades.

---

To install 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 to the management software setup wizard message in the Cisco Fabric Manager Installer window shown in [Figure 2-3](#).

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

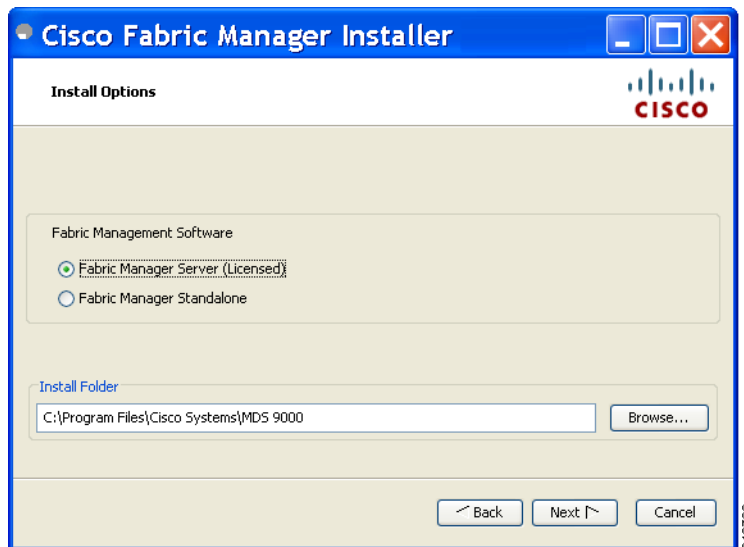
**Figure 2-3 Welcome to the Management Software Setup Wizard**



**Step 5** Click **Next** to begin the installation.

**Step 6** Check the **I accept the terms of the License Agreement** check box and click **Next**. You see the Install Options dialog box shown in [Figure 2-4](#).

**Figure 2-4 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.

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

**Note**

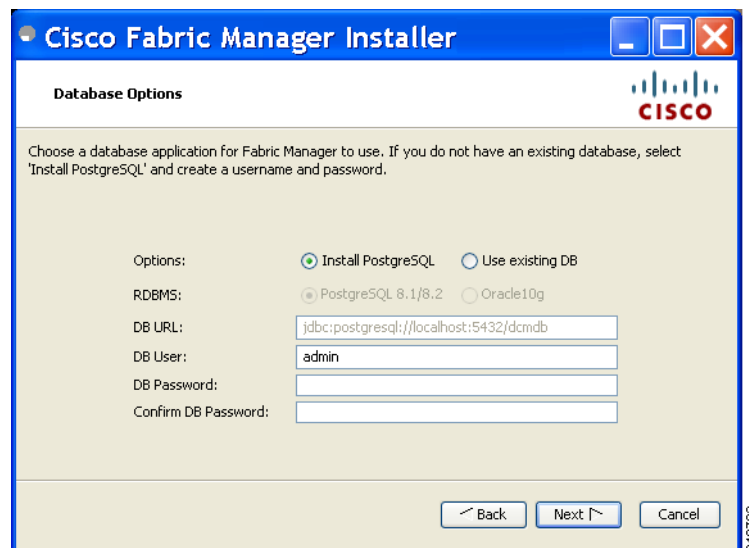
Fabric Manager Standalone is a single application containing Fabric Manager Client and a local version of Fabric Manager Server bundled together. Fabric Manager Standalone allows you to discover and monitor the immediate fabric.

**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 2-5](#).

**Figure 2-5 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, as 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 2-6](#).

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

**Figure 2-6** User Options Dialog Box

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

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

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

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



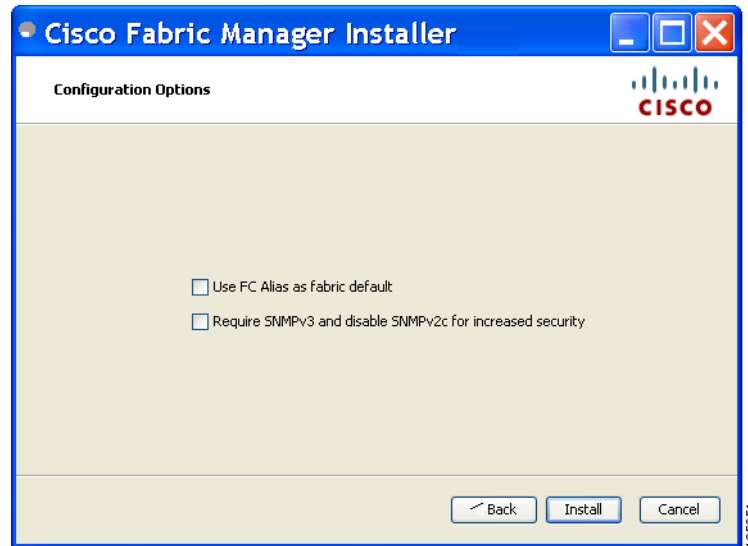
**Note** When the MDS radio button is selected, the FM authentication uses the user database in the switch for authentication.

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

You see the Configuration Options dialog box for Fabric Manager Standalone shown in [Figure 2-8](#).

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

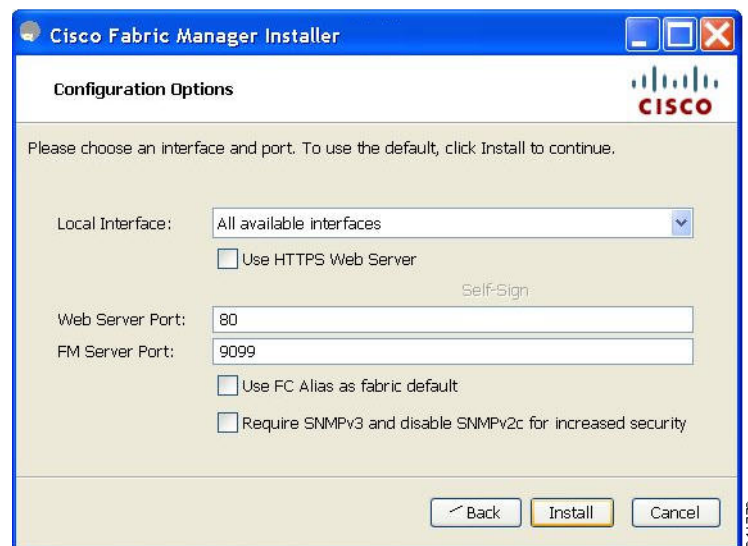
**Figure 2-8 Configuration Options Dialog Box for Fabric Manager Standalone**



- 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 2-9](#).

**Figure 2-9 Configuration Options Dialog Box for Fabric Manager Server**



- Step 17** Select the local interface, web server port or fm server port and check the FC Alias and SNMPv3 check boxes as desired and 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 2-10](#)



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

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

**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.

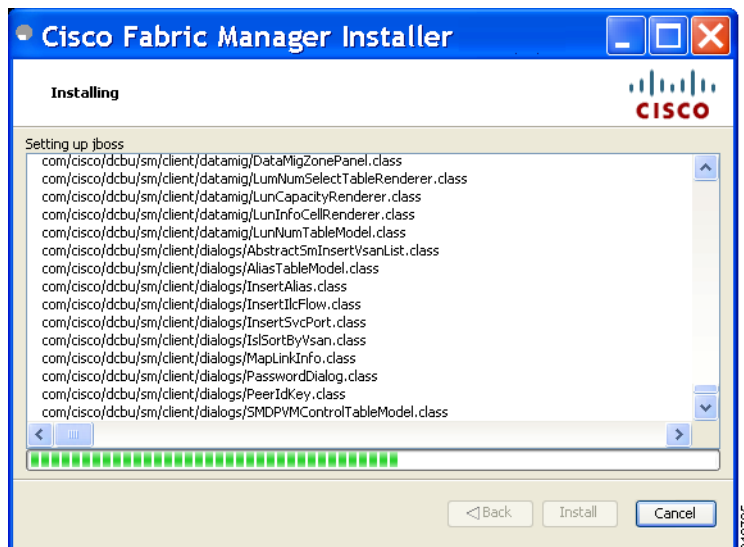
**Note**

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 which are all located in the \$INSTALL/conf directory. Change **server.bindaddr**s 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.

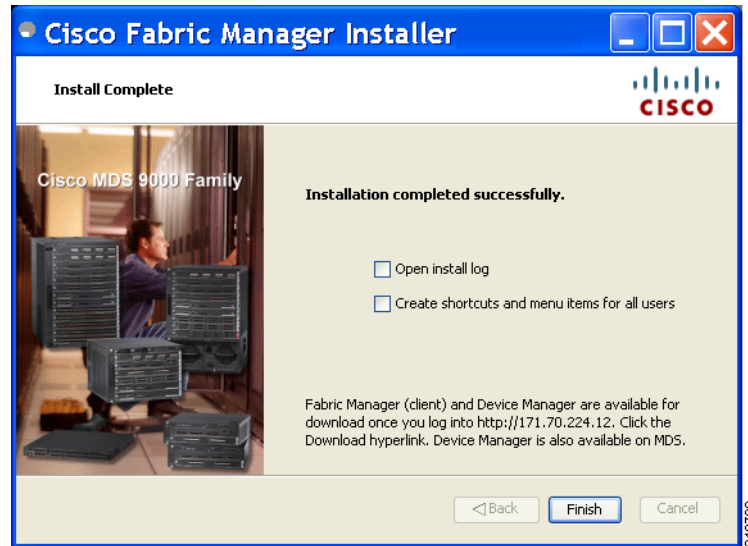
**Figure 2-10 Progress of Installation**



Once the installation is finished, you see an installation completed message in the Cisco Fabric Manager Installer window shown in [Figure 2-11](#).

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

**Figure 2-11 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 in Cisco SAN-OS Release 3.2\(1\) and Later”](#) section on page 5-2 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. Three services are started: Fabric Manager Server, Database, and Web Server. The Performance Manager server is installed but the service is not started upon installation, 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, All 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.

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

## Creating Startup Files in Solaris

The Postgre SQL and Fabric Manager does not automatically start-up in Solaris after the installation. The init files should be created in /etc/init.d, and the following commands should be included in the files.

### To start Postgre SQL and FM:

- \$INSTALL/db/bin/DB start
- \$INSTALL/bin/FMServer.sh start

### To stop Postgre SQL and FM:

- \$INSTALL/db/bin/DB stop
- \$INSTALL/bin/FMServer.sh stop

## Installing Device Manager

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

- 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 2-12](#).

**Figure 2-12** 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 2-13](#).



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

**Figure 2-13** Welcome to the Management Software Setup Wizard Window



**Step 3** Click **Next** to begin the Installation.

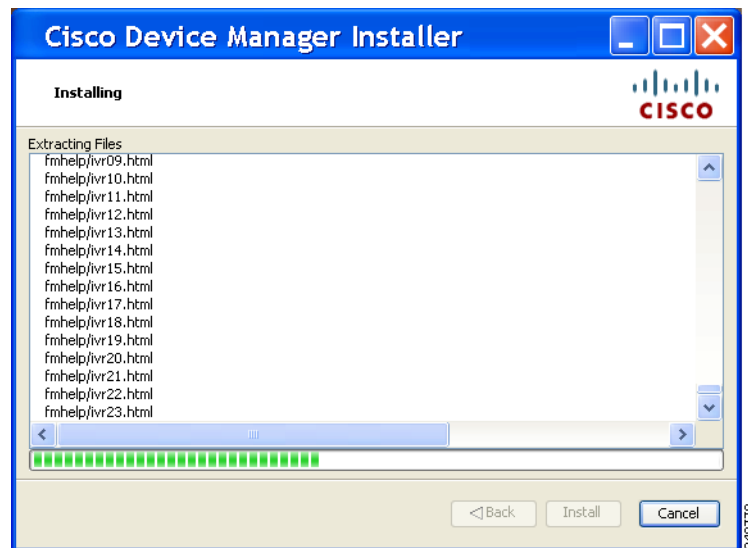
**Step 4** Check the **I accept the terms of the License Agreement** check box and click **Next**.

**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**.

You see the installation progress in the Cisco Device Manager Installer window shown in [Figure 2-14](#).

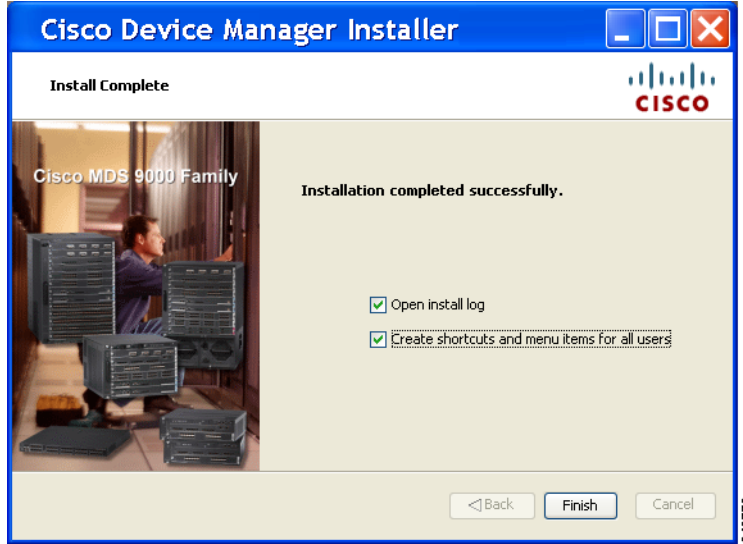
**Figure 2-14** Progress of Installation



Once the installation is finished, you see an installation completed message in the Cisco Device Manager Installer window shown in [Figure 2-15](#).

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

**Figure 2-15** 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. Also, the shortcut is not offered when you lauche Fabric Manager from the FM download page.

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

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

Double click Java.

The Java Control Panel displays as shown in the [Figure 2-16](#)

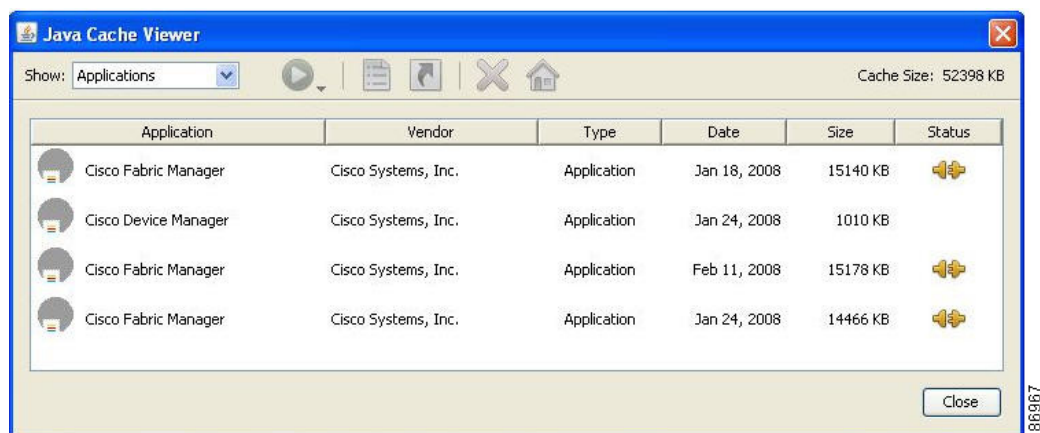
**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

**Figure 2-16** Java Control Panel Dialog Box



- Step 2** Click **View** under **Temporary Internet Files** region, as shown in [Figure 2-17](#). The **Java Cache Viewer** dialog box displays..

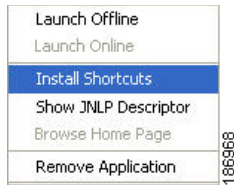
**Figure 2-17** Java Cache Viewer Dialog Box



- Step 3** To recreate the shortcut, right-click on the application, and select **Install Shortcuts** from the shortcut menu, as shown in [Figure 2-18](#)

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

**Figure 2-18**      **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 mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)




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

As of Release 3.3.1a, the Cisco MDS 9000 Fabric Manager Update Installer can be used to:

- Upgrade Fabric Manager Server
- Upgrade Fabric Manager Standalone

The Fabric Manager Update Installer is smaller in size than the larger Fabric Manager installer which makes it easier to download. It 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 2-3](#) shows the recommended Fabric Manager upgrade paths.

**Table 2-3** Fabric Manager Upgrade Path using `java -Xmx512m -jar jar_file_name`

| 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 light installer <code>{java -Xmx512m -jar jar_file_name}</code> and then follow the steps to upgrade Fabric Manager.</li> </ol> <p> <b>Note</b> Change the server port to 9099 if you are not upgrading from Release 3.2(2c) in Step 2.</p> |
| 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 light installer <code>{java -Xmx512m -jar jar_file_name}</code> and then follow the steps to upgrade Fabric Manager.</li> </ol> <p> <b>Note</b> Change the server port to 9099 if you are not upgrading from Release 3.2(2c) in Step 1.</p>                               |
| 3.2(x)              | 3.3(1a) or above | <ol style="list-style-type: none"> <li>1. Upgrade to 3.3(x) or above by launching the light installer <code>{java -Xmx512m -jar jar_file_name}</code> and then follow the steps to upgrade Fabric Manager.</li> </ol> <p> <b>Note</b> Change the server port to 9099 if you are not upgrading from Release 3.2(2c).</p>                                                                       |

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

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

## 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 68, “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 require the PAA to transport MDS SPAN traffic to a Windows PC or workstation.

## 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 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 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.

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

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 <code>server.properties</code> .                                                                                                                  |
| 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 <code>-Dsnmp.localport</code> option.                                                                                                              |
| 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 <code>server.properties</code> .                                                                                                                  |

| Port(s) Used/Type | Service Descriptor                                      | Service Name                          | Attribute Name                  |
|-------------------|---------------------------------------------------------|---------------------------------------|---------------------------------|
| 1098 (TCP)        | conf/jboss-service.xml                                  | jboss:service=Naming                  | RmiPort                         |
| 9099 (TCP)        | conf/jboss-service.xml                                  | jboss:service=Naming                  | Port ( FM changed 1099 to 9099) |
| 4444 (TCP)        | conf/jboss-service.xml                                  | jboss:service=invoker,type=jrmp       | RMIObjectPort                   |
| 4445 (TCP)        | conf/jboss-service.xml                                  | jboss:service=invoker,type=pool<br>ed | ServerBindPort                  |
| 8009 (TCP)        | deploy/jbossweb-tomcat41.sar/META-INF/jboss-service.xml | jboss.web:service=WebServer?          | port on AJP Connector           |
| 8083 (TCP)        | conf/jboss-service.xml                                  | jboss:service=WebService              | Port                            |

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

|               |                                           |                                             |                    |
|---------------|-------------------------------------------|---------------------------------------------|--------------------|
| 8092<br>(TCP) | deploy/jms/oil2-service.xml               | jboss.mq:service=InvocationLayer?,type=OIL2 | ServerBindPort     |
| 8093<br>(TCP) | deploy/jms/ui12-service.xml               | jboss.mq:service=InvocationLayer?,type=UIL2 | ServerBindPort     |
| 3873<br>(TCP) | Service end point for EJB3 aspect service | JBoss EJB3 Aspect Service Deployer          | JBoss EJB3 Invoker |

## 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. 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** 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.

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.