

This section introduces the basic concepts, methodology, and general troubleshooting guidelines for problems that may occur when configuring the Fabric Manager and using the Cisco MDS 9000 Family of multilayer directors and fabric switches.

Contents

- [1 Troubleshooting Fabric Manager](#)
- [2 Overview](#)
- [3 Guidelines](#)
- [4 Initial Troubleshooting Checklist](#)
 - ◆ [4.1 Common Troubleshooting Tools in Fabric Manager](#)
- [5 Troubleshooting Fabric Manager Issues](#)
 - ◆ [5.1 Cannot Log Into Fabric Manager](#)
 - ◆ [5.2 Cannot Upgrade Fabric Manager](#)
 - ◆ [5.3 Map Shows Two Switches Where Only One Switch Exists](#)
 - ◆ [5.4 Old Devices Appear on the Map](#)
 - ◆ [5.5 Red Line Through the Switch](#)
 - ◆ [5.6 Dotted Orange Line Through the Switch](#)
 - ◆ [5.7 Fabric Manager Not Receiving Traps](#)
- [6 Tips for Using Fabric Manager](#)
 - ◆ [6.1 Setting the Map Layout So It Stays After Restarting the Fabric Manager](#)
 - ◆ [6.2 Fabric Manager Upgrade Without Losing Map Settings](#)
 - ◆ [6.3 Restrictions When Using Fabric Manager Across FCIP](#)
 - ◆ [6.4 Running Cisco Fabric Manager with Network Multiple Interfaces](#)
 - ◆ [6.5 Specifying an Interface for Fabric Manager Server](#)
 - ◆ [6.6 Specifying an Interface for Fabric Manager Client or Device Manager](#)
 - ◆ [6.7 Configuring a Proxy Server](#)
 - ◆ [6.8 Clearing Topology Maps](#)
 - ◆ [6.9 Using Fabric Manager in a Mixed Software Environment](#)
- [7 Troubleshooting Fabric Manager Web Client](#)
 - ◆ [7.1 Cannot Download Fabric Manager Web Client](#)
 - ◆ [7.2 Allowing Network-Open Users to Download Fabric Manager Web Client](#)
 - ◆ [7.3 Clearing Java Cache](#)
 - ◆ [7.4 Cannot Access Fabric Manager Web Client](#)
 - ◆ [7.5 Verifying the TCP Port for Fabric Manager Web Client](#)
 - ◆ [7.6 Cannot Launch Fabric Manager Web Client](#)
 - ◆ [7.7 Enabling the Java Runtime Console](#)
 - ◆ [7.8 Allowing the Java Web Start ActiveX Control to Run](#)
 - ◆ [7.9 Trusting the Remote Fabric Manager Web Site](#)
 - ◆ [7.10 Clearing Java Web Start Cache](#)
 - ◆ [7.11 Cannot Log Into Fabric Manager Web Client](#)
 - ◆ [7.12 Recovering a Web Client Password](#)
 - ◆ [7.13 Setting Fabric Manager Authentication Method](#)
- [8 Troubleshooting Performance Manager](#)
 - ◆ [8.1 Performance Manager Generates Java Error](#)
 - ◆ [8.2 Performance Manager Not Working](#)
- [9 Troubleshooting Device Manager](#)
 - ◆ [9.1 Wrong Version of Device Manager is Launched](#)

- [10 Location of Log Files](#)

Troubleshooting Fabric Manager

This section contains some common issues you may experience while using Cisco Fabric Manager, and provides solutions.

This section contains the following sections:

- Overview
- Guidelines
- Initial Troubleshooting Checklist
- Troubleshooting Fabric Manager Issues
- Tips for Using Fabric Manager
- Troubleshooting Fabric Manager Web Client
- Troubleshooting Performance Manager
- Troubleshooting Device Manager

Overview

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

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 tools leverage unique MDS 9000 switch capabilities including Fibre Channel ping and traceroute.

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

Guidelines

Consider the following guidelines when using Fabric Manager:

- Use SNMPv3 with authentication and privacy enabled for encrypted network management traffic.
- If you are running SAN-OS 3.1(3) or earlier, use the Accelerate Discovery check box when starting Fabric Manager.
- Log into Fabric Manager with a user that has network-admin or network-operator privileges to have a full view of your fabric.
- Do not use one-time passwords with Fabric Manager.

Initial Troubleshooting Checklist

Begin troubleshooting Fabric Manager issues by checking the following issues first:

Checklist	Checkoff
Verify licensing requirements. See <i>Cisco MDS 9000 Family Fabric Manager Configuration Guide</i> .	
Verify that you have a compatible version of Java installed. Refer to the release notes for the software version you installed to obtain the correct Java version.	
Verify that the necessary ports are open in your firewall if Fabric Manager Server is installed behind a firewall. Refer to the <i>Cisco MDS 9000 Family Fabric Manager Configuration Guide</i> for details on running Fabric Manager behind a firewall.	
Verify that you have installed the same version of Fabric Manager Client, Fabric Manager Server, and Fabric Manager Web Client.	
Open a browser window and put in your switch address in as the URL. Check the issues presented in the FAQ link.	


Common Troubleshooting Tools in Fabric Manager

Choose **Admin** on Fabric Manager or Fabric Manager Web Client to access Fabric Manager Server configuration options. See also the "Troubleshooting a Nondisruptive Upgrade on a Fabric Switch" section.

Troubleshooting Fabric Manager Issues

This section covers the following topics:

- Cannot Log Into Fabric Manager
- Cannot Upgrade Fabric Manager
- The Map Shows Two Switches Where Only One Switch Exists
- Old Devices Appear on the Map
- Red Line Through the Switch
- Dotted Orange Line Through the Switch
- Fabric Manager Not Receiving Traps


 **Note:** Do not use one-time passwords with Fabric Manager or Device Manager.

Cannot Log Into Fabric Manager

Fabric Manager uses the SNMP user name and password combination to communicate with the switch. The SNMP user name is automatically synchronized with the CLI user names configured. If you use the administrator password recovery procedure, you must manually reset the administrative password on the switch to resynchronize the SNMP and CLI user name and password. See the "Recovering the Administrator Password" section.

Cannot Upgrade Fabric Manager

If you attempt to upgrade Fabric Manager by pointing your web browser at a switch running Cisco SAN-OS 3.0(1) through SAN-OS 3.1(3), you may encounter an issue where the upgrade does not complete. You should open the Java Web Start application on your desktop and disable HTTP proxy. If you are using Microsoft Windows, open Java Web Start and choose **File > Preferences** to access the HTTP proxy settings.

 **Note:** Starting with SAN-OS 3.2(1), Fabric Manager is installed or upgraded from a CD-ROM or from Cisco.com.

Map Shows Two Switches Where Only One Switch Exists

If two switches show on your map, but you only have one switch, it may be that you have two switches in a non contiguous VSAN with the same domain ID. The Fabric Manager uses the VSAN ID and domain ID to look up a switch, which can cause the fabric discovery to assign links incorrectly between these errant switches.

The workaround is to verify that all switches use unique domain IDs within the same VSAN in a physically connected fabric. (The fabric configuration checker will do this task.)

Old Devices Appear on the Map

If you are running a SAN-OS 3.1(3) or earlier version, and old devices appear on your fabric map, you might have made changes to the fabric topology, such as changing a switch IP address or removing a device, but launched Fabric Manager with the Accelerate Discovery check box checked.

The workaround is to log out, and then log back in without checking the Accelerate Discovery check box.

Red Line Through the Switch

If a red line shows through your switch, the Fabric Manager sees something wrong with the switch. Check the **Switch->Inventory** report. A module, fan, or power supply has failed or is offline and plugged in.

Dotted Orange Line Through the Switch

If a dotted orange line shows through your switch, this indicates a minor status warning for that switch. Usually it means an issue with one of the modules. The tooltip should display exactly what is wrong. Hold the mouse over the switch to see the tooltip.

Fabric Manager Not Receiving Traps

You can set SNMP traps to test a Call Home application without risking adverse impact to your production SAN. Traps for temperature, fans, and power supply monitoring are then received by Fabric Manager.

If Fabric Manager is not receiving traps, verify that your switch is sending traps by using the following CLI commands:

- **test pfm snmp test-trap fan** - To generate a test SNMP trap for fan.
- **test pfm snmp test-trap powersupply** - To generate a test SNMP trap for power supply.
- **test pfm snmp test-trap temp_sensor** - To generate a test SNMP trap for temperature.

Tips for Using Fabric Manager

This section covers the following topics:

- Setting the Map Layout So It Stays After Restarting the Fabric Manager
- Fabric Manager Upgrade Without Losing Map Settings

- Restrictions When Using Fabric Manager Across FCIP
- Running Cisco Fabric Manager with Network Multiple Interfaces
- Configuring a Proxy Server
- Clearing Topology Maps
- Using Fabric Manager in a Mixed Software Environment

Setting the Map Layout So It Stays After Restarting the Fabric Manager

If you have configured the map layout and would like to "freeze" the map so that the objects stay as they are even after you stop Fabric Manager and restart it again, do the following:

1. Right-click a blank space in the map. You see a pop-up menu.
2. Select **Layout -> Fix All Nodes** from the menu.

Fabric Manager Upgrade Without Losing Map Settings

When you upgrade from one version of Fabric Manager to another, there is a way to prevent the loss of map settings (enclosure names, placement on the map, etc.)

The MDS 9000/db directory and subfolders contain files for all the discovered fabrics (*.dat) and maps (*.map). These are upgradable between versions. If you need to clear the fabric cache, you should first export the enclosures to a file to avoid losing them. Everything else aside from enclosures and map coordinates are stored on the switch. The preferences, last opened, and site_ouis.txt format does not change from release to release.

Restrictions When Using Fabric Manager Across FCIP

Fabric Manager will work without any restrictions across an FCIP tunnel as long as the tunnel is up. However, Fabric Manager cannot automatically discover a Cisco SN5428 mgmt 0 IP address in the fabric. For that switch, Fabric Manager displays a red slash through an FCIP device because of a timeout error. It still sees all targets, initiators, and ISLs attached to a Cisco SN5428 (or any other switch) as long as they appear in the name server or FSPF.

To work around this, you can manually enter the IP address in the Switches table, and click **Apply**. If the community string is correct, the red slash goes away. Even if the community string is incorrect, double-clicking the Cisco SN5428 launches the web tool.

Running Cisco Fabric Manager with Network Multiple Interfaces

If your PC has multiple network interfaces (NICs), the Cisco Fabric Manager applications detect these interfaces automatically (ignoring loopback interfaces). Fabric Manager client and Device Manager detect all interfaces on your PC each time you launch them, and allow you to select one. Fabric Manager Server detects on initial install, and allows you to select one. You are not prompted again to choose an interface with these two applications.

There may be circumstances where you will want to change the interface you are using. For example:

- If you add an interface after you have installed Fabric Manager Server
- If you decide to use a different interface than the one you initially selected
- If for any reason one of the Cisco Fabric Manager applications did not detect multiple interfaces

See the following sections, depending on which application you want to recognize the interface.

- Specifying an Interface for Fabric Manager Server
- Specifying an Interface for Fabric Manager Client or Device Manager

Specifying an Interface for Fabric Manager Server

To specify an interface for Fabric Manager Server, follow these steps:

1. Go to the MDS 9000 folder.
 2. Edit the server.properties file with a text editor.
 3. Scroll until you find the line snmp.localaddress.
 4. If the line is commented, remove the comment character.
 5. Set this value to the IP address or interface name of the NIC you want to use.
 6. Save the file.
 7. Stop and restart Fabric Manager Server.
-

Specifying an Interface for Fabric Manager Client or Device Manager

To specify an interface for the Fabric Manager Client or Device Manager, follow these steps:

1. Go to the MDS 9000/bin folder.
 2. Edit the DeviceManager.bat file or the FabricManager.bat file.
 3. Scroll to the line that begins with set JVMARGS=.
 4. Add the parameter -Device Managerds.nmsaddress=ADDRESS, where ADDRESS is the IP address or interface name of the NIC you want to use.
 5. Save the file and relaunch Fabric Manager Client or Device Manager.
-

Configuring a Proxy Server

If your network uses a proxy server for HTTP requests, make sure the Java Web Start Application Manager is properly configured with the IP address of your proxy server.

To configure a proxy server in the Java Web Start Application Manager, follow these steps:

1. Double-click the Java Web Start application manager icon on your Windows desktop, or choose **Program Files > Java Web Start**.
2. Select **File > Preferences** from the Java WebStart Application Manager.
3. Click the **Manual** radio button and enter the IP address of the proxy server in the HTTP Proxy field.

4. Enter the HTTP port number used by your proxy service in the HTTP Port field.
5. Click **OK**.

Clearing Topology Maps

If you have a switch that you have removed from the fabric, there will be a red X through the switch's icon. You can clear this information from the Fabric Manager client, or from the Fabric Manager server (which will clear the information for all clients) without having to reboot the switch.


To clear information from topology maps, follow these steps:

1. Click on the **Refresh Map** icon in the Fabric pane.

◇ This clears the information from the client.

2. From the Server menu, click **Purge Down Elements**.

◇ This clears the information from the server.

 **Note:** Any devices not currently accessible (may be offline) are purged.

Using Fabric Manager in a Mixed Software Environment


You can use Fabric Manager version 2.x to manage a mixed fabric of Cisco MDS 9000 Family switches. Certain 2.x feature tabs will be disabled for any switches running a software version that does not support those features.

Troubleshooting Fabric Manager Web Client

Using Fabric Manager Web Client, you can monitor MDS switch events, performance, and inventory, and perform minor administrative tasks. Fabric Manager Web Client provides summary and drill-down performance reports. These reports are only available if you create a collection using Performance Manager and start the collector.

This section includes the following topics:

- Cannot Access Fabric Manager Web Client
- Cannot Launch Fabric Manager Web Client
- Cannot Log Into Fabric Manager Web Client

 **Note:** You must log in with a network-access role to access the Admin tab in Fabric Manager Web Client.

Cannot Download Fabric Manager Web Client

Symptom Cannot download Fabric Manager Web Client.

Table 26-1 Cannot Access Fabric Manager Web Client

Symptom	Possible Cause	Solution
---------	----------------	----------

Cannot download Fabric Manager Web Client.	To download Fabric Manager Web Client, you must have network-admin role.	A network-admin can allow a network-oper to download the client. See the "Allowing network-open Users to Download Fabric Manager Web Client" section.
	Java cache may contain damaged or incorrect files.	Empty Java cache and restart the download. See the "Clearing Java Cache" section.

Allowing Network-Open Users to Download Fabric Manager Web Client

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

A network-admin can modify the server.properties file to allow users with network-open role to download the Fabric Manager Web Client by following these steps:

-
1. Open the server.properties file in the Fabric Manager installation directory. On a Windows platform, this file is in C:\Program Files\Cisco Systems\MDS 9000 by default.
 2. Set web.allowDownload4All=true. By default, this property is not set.
 3. Save and exit the file.
 4. Restart Fabric Manager.

Clearing Java Cache

If you encounter problems downloading Fabric Manager Web Client, the Java cache may contain damaged files or old versions of software. To correct this problem, clear Java cache.

-
1. Navigate to **Control Panel > Java**, and double-click Java to open the Java Control Panel.
 2. Click **View** under **Temporary Internet Files** region to open the Java Cache Viewer.
 3. Show application and applets, by selecting the appropriate item from the Show drop-down list.
 4. Select the appropriate applications and applets and click the **delete** icon, or right-click and choose **Remove Application** from the shortcut menu.
 5. Click **Close**.

Cannot Access Fabric Manager Web Client

Symptom Cannot access Fabric Manager Web Client.

Table 26-2 Cannot Access Fabric Manager Web Client

Symptom	Possible Cause	Solution
Cannot access Fabric Manager Web Client.	Using wrong TCP port.	Verify TCP port where Fabric Manager Web Client was installed. See the "Verifying TCP port for Fabric Manager Web Client" section.
	TCP port blocked by firewall.	Open TCP port in your firewall. For more information on running Fabric Manager behind a firewall, see the <i>Cisco MDS 9000 Family Fabric Manager Configuration Guide</i> .

Verifying the TCP Port for Fabric Manager Web Client

To verify the TCP port used by Fabric Manager Web Client, view `\tomcat\conf\server.xml` from the directory where you installed Fabric Manager Web Client. You see the following lines after some copyright information:

```
<Connector className="org.apache.catalina.connector.http.HttpConnector"
    port="80" minProcessors="5" maxProcessors="75"
    enableLookups="false" redirectPort="8443"
    acceptCount="10" debug="0" connectionTimeout="60000"/>
<!-- Define an SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector className="org.apache.catalina.connector.http.HttpConnector"
    port="8443" minProcessors="5" maxProcessors="75"
    enableLookups="true"
    acceptCount="10" debug="0" scheme="https" secure="true">
    <Factory className="org.apache.catalina.net.SSLServerSocketFactory"
        clientAuth="false" protocol="TLS"/>
</Connector>
-->
```

Look for the Connector setting that is not commented out (that is, not preceded by `<!--`), and search for the port setting. This is the TCP port number used by Fabric Manager Web Client. You can edit this file if you need to change the TCP port number in use or if you need to use SSL.

Cannot Launch Fabric Manager Web Client

Symptom Cannot successfully launch Fabric Manager Web Client.

Table 26-3 Cannot Launch Fabric Manager Web Client

Symptom	Possible Cause	Solution
Java Web Start not detected error message displays.	Appropriate version of Java may not be installed.	Install the appropriate version of the Java Runtime Environment. Cisco recommends Java version 1.5 or above, which includes Java Web Start. Refer to the installation instructions in the <i>Cisco MDS 9000 Family Fabric Manager Configuration Guide</i> , or the <i>Release Notes</i> for your specific Fabric Manager release.
	The Java Runtime console may be	Enable the Java Runtime console. See the "Enabling the Java Runtime Console" section.

	disabled.	
	Internet Explorer 7 blocks the Java Web Start ActiveX control.	Allow the browser to run the Java Web Start ActiveX control. See the "Allowing the Java Web Start ActiveX Control to Run" section.
Cannot connect to a remote Fabric Manager server.	Internet Explorer 7 may block the pop-ups that are required to complete the connection.	Add the web site to your trusted sites list, and allow it to open pop-ups, including script-generated input dialog boxes. See the "Trusting the Remote Fabric Manager Web Site" section.
Launch fails, or wrong version appears.	Java Web Start cache contains multiple versions of Fabric Manager software.	Clear the Java Web Start cache. See Clearing Java Web Start Cache.

Enabling the Java Runtime Console

If you are running the Microsoft Internet Explorer 7 browser, the Java Runtime console may be disabled by default.

To enable the Java Runtime console, follow these steps:

-
1. Choose **Tools > Manage Add-ons > Enable or Disable Add-ons**.

◇ You see the Manage Add-ons dialog box.

2. Select the Java Runtime Console and then click the **Enable** radio button in the Settings area.

3. Click **OK**.
-

Allowing the Java Web Start ActiveX Control to Run

If you are using Internet Explorer 7, you might be prompted to take action to allow the Java Web Start ActiveX control to run.

When you launch the Fabric Manager Web Client, a message appears on the browser information bar, indicating that the web site wants to run the Java Web Start ActiveX Control from Sun Microsystems.

To allow the web site to run the Java Web Start ActiveX control and launch the Fabric Manager Web Client, follow these steps:

-
1. Click the **here** link on the Internet Explorer information bar.
 2. Select **Run ActiveX Control** from the choices shown.
-

Trusting the Remote Fabric Manager Web Site

If you are launching the Fabric Manager Web Client and connecting to a remote Fabric Manager Server using Internet Explorer 7, pop-up dialog boxes might be disabled by default.

To allow the script-generated input dialog boxes required to connect to the Fabric Manager Server to appear, follow these steps:


1. In the Internet Explorer 7 browser, choose **Tools > Internet Options**.

◇ You see the Internet Options dialog box.

2. Click the **Security** tab, and then click the **Trusted sites** zone.

3. Click **Sites**. You see the Trusted Sites dialog box.

4. Enter the URL of the specific site that you want to trust in the Add this site to the zone field. If you are already viewing the web site that you want to trust, the URL will be shown automatically.

 **Note:** If the web site is not encrypted with SSL, uncheck the **Require server verification (https:) for all sites in this zone** check box.

5. Click **Add**. The URL or IP address appears in the Websites list.

6. Click **OK**, and then click **OK** on the **Security** tab to exit.

Clearing Java Web Start Cache

To clear the Java Web Start cache, follow these steps:

1. Start the Java Web Start Application Manager (**javaws.exe** or **javaws**).

2. Go to **File > Preferences > Advanced** and clear the applications folder or cache. You can manually delete the .javaws or cache directory. On Windows, this directory is under Documents and Settings, and on UNIX, this directory is under \$HOME.

Cannot Log Into Fabric Manager Web Client

Symptom Cannot log into Fabric Manager Web Client.

Table 26-4 Cannot Access Fabric Manager Web Client

Symptom	Possible Cause	Solution
Cannot log into Fabric Manager Web Client.	Forgot password.	Reset the administrative password. See the "Recovering a Web Client Password" section.
	Access set for RADIUS or TACACS but server is not responding.	Set for local authentication. See the "Setting Fabric Manager Authentication Method" section. After you verify the RADIUS or TACACS server, you can set the

		authentication method to use RADIUS or TACACS .
	No valid ID message displayed. Fabric Manager Server has not discovered the fabric.	Open Fabric Manager and rediscover the fabric.

Recovering a Web Client Password

Fabric Manager Web Client user passwords are encrypted and stored locally on the workstation where you installed the Web Client. If you forget a password, you can make a new network-admin user locally on the workstation where you installed the Web Client and then log in and delete the old user account under the Admin tab.

To create a user on the workstation where you installed the Web Client and deleted the old user, follow these steps:

1. Go to the Web Client installation directory and **cd** to the bin directory.
2. Enter the following line to create a user:

```
addUser <userName> <password>
```

3. Stop Fabric Manager Web Client if it is running. If you installed this on Windows, you can stop the service using Windows Services under Administrative Tools.
4. Launch **Fabric Manager Web Client**.
5. Click **Admin > Configure > Web Users > Local Database**.

◇ You see the list of users in the local database.

6. Select the user that you want to delete and click **Delete** to remove the old user.

Setting Fabric Manager Authentication Method

To set the authentication method used by Fabric Manager (including the Web Client), follow these steps:

1. Go to the Fabric Manager installation directory and open cisco_mds9000\AAA.properties in an edit program (for example, Notepad on Microsoft Windows).
2. Set authentication.mode=local.
3. Restart Fabric Manager.

Troubleshooting Performance Manager

Performance Manager gathers network device statistics historically and provides this information graphically using a web browser. It presents recent statistics in detail and older statistics in summary. Performance Manager also integrates with external tools such as Cisco Traffic Analyzer.

The Performance Manager has three operational stages:

- Definition--The Flow Wizard sets up flows in the switches.
- Collection--Reads the configuration from the database, the flow configuration from the switches, and collects the desired information.
- Presentation--Generates web pages to present the collected data.

Performance Manager uses a round-robin database to hold the statistical data collected from the fabric. This data is stored based on the configured parameters in the collection configuration file. At each polling interval, Performance Manager gathers the relevant statistics and stores them in the round-robin database. This database is a fixed size and will not grow beyond its preset limits.

Performance Manager creates a series of archived data to hold summarized information present in the real-time round-robin database. This archived data is used to generate daily, weekly, monthly, and yearly consolidated reports. In this way, Performance Manager maintains significant historical data without the cost of an ever-increasing database size.

This section contains the following topics:

- Performance Manager Generates Java Error
- Performance Manager Not Working

Performance Manager Generates Java Error

Symptom Performance Manager generates JAVA error.

Table 26-5 Performance Manager Generates JAVA Error

Symptom	Possible Cause	Solution
Performance Manager generates JAVA error.	Incompatible JAVA version.	Upgrade to JAVA JRE and JDK version 1.5.0.

Performance Manager Not Working

Symptom Performance Manager not working.

Table 26-6 Performance Manager Not Working

Symptom	Possible Cause	Solution
Performance Manager not working.	No collection created.	Create a collection using Fabric Manager. Performance Manager reports are available after the first set of statistics are gathered based on a collection.

Troubleshooting Device Manager

While Fabric Manager provides real-time views of your network fabric, Device Manager provides a real-time graphic representation of a Cisco MDS 9000 Family switch chassis, including the installed switching modules, the supervisor modules, the status of each port within each module, the power supplies, and the fan assemblies.

Device Manager allows you to troubleshoot device-specific configuration issues by providing detailed information for verification. It also allows you to perform switch-level configurations, including:

- Configure zones for multiple VSANs
- Manage ports, PortChannels, and trunking
- Manage SNMPv3 and CLI security access to switches
- Manage alarms, events, and notifications
- Save and copy configuration files and software images
- View hardware configurations, chassis, modules, port status, and statistics

Device Manager uses the SNMP user name/password combination to communicate with the switch. The SNMP user name is automatically synchronized with the CLI user names configured. If you use the administrator password recovery procedure, you must manually reset the administrative password on the switch to resynchronize the SNMP and CLI user name and password. See the "Recovering the Administrator Password" section.

Wrong Version of Device Manager is Launched

Symptom When launching Device Manager from the Fabric Manager Web Client, the wrong version is opened.

Table 26-7 Wrong version of Device Manager is opened

Symptom	Possible Cause	Solution
Wrong version of Device Manager is opened.	Java Web Start cache contains multiple versions of Device Manager software.	Clear the Java Web Start cache. See "Clearing Java Web Start Cache".

Location of Log Files

You can also refer to the relevant log files to know more about troubleshooting fabric manager. The relevant log files and their locations are listed below.

The log files on server side are located at *\$INSTALLDIR/dcm/fm/logs*:

- Web Server Log: *fm_web.log*
- Web Report Log: *fm_webreport.log*
- Server SNMP Log: *fms_snmp.log*
- Server SNMP Trap Log: *fms_snmp_trap.log*
- Web Service Log: *fms_ws.log*
- FM Server Log: *fmserver.log*

Cisco_MDS_SanOS_Troubleshooting_Guide_--_Troubleshooting_Fabric_Manager

- Performance Manager Log: *pm.log*
- SME Log: *sme.log*

The log files on the client side are located at *\$HOME/.cisco_mds9000/logs*:

- Event Related Log: *fm_event.log*
- Client Log: *fm.log*
- Client SNMP Log: *fm_snmp.log*
- Client Topology Log: *fm_map.log*

Back to Main Page: [Cisco MDS SAN-OS Troubleshooting Guide](#)
