



Getting Started

This section provides a minimum number of steps for setting up DFM and viewing diagnostic results. It is intended to help you to start using DFM immediately.

Configuration Roadmap

Table 4-1 lists the basic tasks for setting up DFM.

Table 4-1 Configuration Roadmap

Task	Steps	References
Add devices to DFM managed inventory.	1. Add devices and credentials to Common Services Device and Credentials Repository (DCR).	<ul style="list-style-type: none"> Managing Device Credentials, page 4-3 Importing Devices to the Device and Credentials Repository, page 4-6
	2. Verify that devices were discovered (and troubleshoot problems, if necessary).	<ul style="list-style-type: none"> Verifying Devices Added to DFM, page 4-7 Troubleshooting Device Discovery, page 4-9
Configure Trap Receiving	<p>3. Determine which of the following approaches to SNMP trap receiving to take and perform the appropriate steps:</p> <ul style="list-style-type: none"> Send SNMP traps directly to DFM: <ol style="list-style-type: none"> Update DFM trap receiving port if necessary. Enable devices to send traps to DFM. Integrate DFM SNMP trap receiving with other NMSs or trap daemons. 	<ul style="list-style-type: none"> Updating the SNMP Trap Receiving Port, page 4-11 Enabling Devices to Send Traps to DFM, page 4-11 Integrating DFM Trap Receiving with NMSs or Trap Daemons, page 4-12
(Optional) Configure DFM Trap Forwarding	4. Configure DFM to forward traps.	Configuring SNMP Trap Forwarding, page 4-14

After you complete the tasks in [Table 4-1](#):

- You can monitor the network using the Alerts and Activities display (see [Viewing Alerts, page 4-14](#)).
- You can use DFM and continue to configure it (see [What Next?, page 4-15](#)).

Using the CiscoWorks Home Page

The CiscoWorks home page is the launch point for CiscoWorks applications and the window from which you log out of CiscoWorks applications. The CiscoWorks home page includes launch points for:

- Common Services—Services for CiscoWorks applications to perform tasks such as configuring the server, selecting a login module, and creating a device credentials database.
- Device Center—A center where you can examine and act on a selected device; provides a summary and links to tools you can use, reports you can run, and tasks you can perform on the device.
- Locally installed CiscoWorks applications—By default, the locally installed Device Fault Manager appears on the CiscoWorks home page.

If you would like to launch additional applications directly from the CiscoWorks home page, you can do so by registering the applications with the local CiscoWorks home page.

**Note**

For more information about how DFM integrates with Common Services, Device Center, and the CiscoWorks home page, see *User Guide for Device Fault Manager 2.0.6*.

Registering Applications with the CiscoWorks Home Page

Registering applications with the CiscoWorks home page enables you, for example, to launch remote CiscoWorks applications from the local CiscoWorks home page:

- On a standalone DFM, you can register a remote Resource Manager Essentials (RME) to the CiscoWorks home page.
- On a remote RME, you can register a standalone DFM to the CiscoWorks home page. (Do this while logged into the local CiscoWorks home page for the remote RME.)
- On a local DFM, if you have an additional DFM server, you can also register it to the CiscoWorks home page.

**Note**

For a CiscoWorks application to register with the CiscoWorks home page, it must run on CiscoWorks Common Services 3.0.

For information about registering a DFM server to the CiscoWorks home page, see *User Guide for Device Fault Manager 2.0.6*. For complete information about Common Services, see *User Guide for CiscoWorks Common Services 3.0.6*.

Understanding and Configuring Security

DFM supports the following security-related mechanisms:

- SNMPv3 protocol (Authentication/No-Privacy option)—DFM supports the authentication/no-privacy option between the server and the device.
- Security on the CiscoWorks server—You can configure the following aspects of security for the server on which DFM resides:
 - **Secure Socket Layer (SSL)**—DFM can use SSL protocol between the server and the browser. You can enable and disable SSL for the server. If you enable SSL, you should set up a self-signed security certificate to enable SSL communication. For more information, see *User Guide for Device Fault Manager 2.0.6*.
 - **Local security or Cisco Secure ACS**—Access to tasks within DFM is controlled either by local security, provided by Common Services, or by Cisco Security ACS. Local security is enabled on the server by default. DFM supports integration with Cisco Secure ACS. You use Common Services to select the type of security you want.



Note

For more information, see *User Guide for Device Fault Manager 2.0.6*.

Managing Device Credentials

DCR is a common repository of devices and their credentials for use by individual applications. DFM takes its device list and credentials from DCR. DCR enables DFM to synchronize with or select from a device list that is shared by other CiscoWorks applications that are installed locally. You will use DCR to:

- Add a single device or import devices in bulk to the repository.
- Exclude devices from being imported to the repository.
- Delete devices from the repository.

To perform these tasks, see *User Guide for CiscoWorks Common Services 3.0.6*. For scenarios for DFM, see [Performing Device Management, page 4-6](#).

Using the LMS Setup Center

The LMS Setup Center displays your DFM system configuration and allows you to make modifications to the configuration. The Setup Center link is enabled only if the LMS license is detected on the system.

After installation, you can configure the necessary server settings in a single session using the Setup Center. The Setup Center displays the current value of a system or server setting and provides an Edit link to configure the settings.

The configurations are grouped into the following categories: [System Settings](#), [Security Settings](#), [Data Collection Settings](#), and [Data Purge Settings](#).



Note

Refer to the *User Guide for Device Fault Manager (Software Release 2.0.6)* and *User Guide for CiscoWorks Common Services 3.0.5* for more information about the system configuration settings.

System Settings

The System Settings window contains information about the following:

Field	Description	Clicking the Edit icon next to the value takes you to the ...
CiscoWorks Homepage Server Name	The display name of the CiscoWorks Server in the home page.	Common Services Homepage Settings page.
SMTP Server	The SMTP Gateway Server for sending emails out of the server.	Common Services System Preferences page.
CiscoWorks Email ID	The sender's address in all emails originating from the system.	Common Services System Preferences page.
Backup Schedule	The schedule for backup of data and configuration.	Common Services Backup Job page.
License Status	The validity of the CiscoWorks license. The evaluation license expires 90 days after it has been installed.	Common Services License Information page.
DFM Default SMTP Server	This SMTP server is used by default when you add or edit subscriptions for email notifications or send email notifications from the Alerts and Activities display.	DFM Default SMTP Server page.
DFM Notification Service	Use the Notification Services page to customize event names and manage DFM notifications.	DFM Notification Services page.
DFM SNMP Configuration	The SNMP timeout and retries are global SNMP settings in DFM. If an SNMP query does not respond in time, DFM will time out. It will then retry contacting the device for as many times as displayed.	DFM SNMP Configuration page.

The System Settings window has a **Refresh** button at the upper-right corner. To see your changes, refresh the page.

Security Settings

The Security Settings window contains information about the following:

Field	Description	Clicking the Edit icon next to the value takes you to the ...
Server Certificate	Common Services uses self-signed security certificates, which can be used to enable SSL connections between the client browser and the management server.	Common Services Certificate Setup page.
Browser-Server Security Mode	To make sure all communication from the browser to the server is secure, select HTTPS.	Common Services Browser-Server Security Mode Setup page.

Field	Description	Clicking the Edit icon next to the value takes you to the ...
System Identity User	This is used as the default identity for the system while communicating with peer CiscoWorks servers.	Common Services System Identity Setup page.
Authentication Mode	Common Services provides several pluggable authentication modules to authenticate the user to the applications.	Common Services AAA Mode Setup page.
Authorization Mode	The authorization mode used by the applications.	Common Services AAA Mode Setup page.
Number of Users	The number of local users in a system.	Common Services Local User Setup page.
Internet Proxy Setup	The proxy server details for connection to external networks.	Common Services Proxy Server Setup page.
RCP Username	This is used as a trusted username for RCP communications between the server and the network devices.	Common Services System Preferences page.
Single Sign-On Mode	SSO is used to navigate to multiple servers without having to authenticate to each one of them.	Common Services Single Sign-On Setup page.

The Security Settings window has a **Refresh** button at the upper-right corner. To see your changes, refresh the page.

Data Collection Settings

The Data Collection Settings window contains information about the following:

Field	Description	Clicking the Edit icon next to the value takes you to the ...
DCR Mode	Whether DCR is operating in Standalone, Master, or Slave mode.	Common Services Mode Settings page.
DFM Rediscovery Schedule	Gives you the schedule when DFM probes devices to discover their configurations and verify their manageable elements in the inventory.	DFM Rediscovery Schedule page.
DFM SNMP Trap Forwarding	Whether SNMP Trap Forwarding is configured. SNMP Trap Forwarding is the method through which DFM forwards SNMP traps from devices in the DFM inventory.	DFM SNMP Trap Forwarding page.
DFM Polling and Threshold	Gives you the number of timeouts and retries while DFM polls devices.	DFM Polling and Thresholds page.

The Date Collection Settings window has a **Refresh** button at the upper-right corner. To see your changes, refresh the page.

Data Purge Settings

The Data Purge Settings window contains information about the following:

Field	Description	Clicking the Edit icon next to the value takes you to the ...
DFM Daily Purge Schedule	DFM Fault History data remains in the DFM database for 31 days. Purging occurs every day in order to maintain only 31 days of data. You can see the time set for daily purging. By default, purging begins at 00:00.	DFM Daily Purging Schedule page.

The Data Purge Settings window has a **Refresh** button at the upper-right corner. To see your changes, refresh the page.

Performing Device Management

There are two distinct sets of device management tasks:

- Maintaining a device list and credentials—You must use Common Services Device and Credentials Repository to perform the associated tasks for all CiscoWorks applications.
- Adding devices to DFM, discovering them, and maintaining a managed inventory of devices—You must use DFM to perform these tasks. By default, DFM automatically synchronizes its device inventory with the devices in DCR. Alternatively, you can configure DFM to manage devices only after you select them from DCR.

Importing Devices to the Device and Credentials Repository

You can import devices to DCR from an NMS or from a file. The file format is documented in *User Guide for Common Services 3.0.6*.

Adding Devices to DFM



Note

Devices must exist in DCR before you can add them to DFM.

- Step 1** On the DFM home page, select **Device Management > Device Selector**.
- Step 2** To manually select devices to add to DFM:
- Deselect the Synchronize with Device Credentials Repository check box. (By default, the check box is selected.)
 - After new devices have been added to DCR, click **Ctrl** and select devices from the Devices not in Device Fault Manager list.
 - Click the **> Add >>** button.
 - Click **OK**.

- Step 3** To automatically add devices to DFM:
- Select the Synchronize with Device Credentials Repository check box.
 - Click **OK**.
-

For more information, see *User Guide for Device Fault Manager 2.0.6*.

Verifying Devices Added to DFM

You can verify that your devices have been added to DFM by checking the following:

- A brief summary—See [Viewing the Device Summary, page 4-7](#).
- Details for devices in a particular device state—See [Viewing Device Details, page 4-7](#).
- Discovery status of all devices—See [Viewing Discovery Status, page 4-8](#).

If you find that problems have occurred during device discovery, see [Troubleshooting Device Discovery, page 4-9](#).

Viewing the Device Summary

-
- Step 1** On the DFM home page, select **Device Management > Device Summary**. The Device Summary page opens.
-

The device summary displays the number of devices in each of the following device states:

- Known**—The device has been successfully imported and is fully managed by DFM.
- Learning**—DFM is discovering the device. This is the beginning state, when the device is first added or is being rediscovered.
- Questioned**—DFM cannot manage the device. See [Troubleshooting Device Discovery, page 4-9](#).
- Pending**—The device is being deleted. DFM is waiting for confirmation from all of its data collectors before purging the device and its details.
- Unknown**—DFM does not support the device.

For a list of devices in a particular device state, see [Viewing Device Details, page 4-7](#). For a list of all devices, see [Viewing Discovery Status, page 4-8](#).

Viewing Device Details

-
- Step 1** On the DFM home page, select **Device Management > Device Details**. The Device Report page opens. In the Device Selector pane, a device group for each current device state is displayed.
- Step 2** Select a device group or devices from a group and click **View**. The Device Details report opens in a new window and displays the following information.

Column	Description
Device Name	IP address or DNS name for the device. Clicking this link launches the Detailed Device View, which lists the device components and their managed state (from here you can also change the managed state).
IP Address	IP address for the device.
Status	The device state: Known, Learning, Questioned, Pending, or Unknown. For device state definitions, see Viewing the Device Summary, page 4-7 . If devices are not in the Known state, see Troubleshooting Device Discovery, page 4-9 .
Device Type	The device type; for example, Content Networking, Routers, Switches and Hubs, and so on. For more information, see <i>User Guide for Device Fault Manager 2.0.6</i> .
First Added	Date and time the device was first added to DFM.
Last Discovered	Date and time of most recent discovery.

Viewing Discovery Status

The discovery status page displays all devices in a tabular format along with their processing and discovery state.

- Step 1** On the DFM home page, select **Device Management > Discovery Status**. The Discovery Status page opens.

The View Discovery Status table displays the following information:

Column	Description
Device Name	IP address or DNS name for the device.
Status	Device state—Known, Learning, Questioned, Pending, or Unknown. For device state definitions, see Viewing the Device Summary, page 4-7 . If devices are not in the Known state, see Troubleshooting Device Discovery, page 4-9 .
DFM Processing	Processing status—One of the following: <ul style="list-style-type: none"> Active—DFM is managing the device. Suspended—DFM is not managing the device. N/A—DFM cannot manage the device; the device state is Questioned.
Last Discovered	Date and time of most recent discovery.

- Step 2** To view the status of device discovery, select Device Fault Manager > **Device Management > View Discovery Status**.

Troubleshooting Device Discovery

To troubleshoot device discovery, try the following:

- If a device is not responding, confirm all device credentials and readd the device. See [Changing Device Credentials, page 4-9](#).
- Increase SNMP timeout settings if device rediscovery times out for several devices. See [Modifying SNMP Timeout and Retries, page 4-9](#).
- View device error information on the Edit Device Configuration page. See [Rediscovering a Device, page 4-9](#).
- Verify that the device is operational during the import and that it supports MIB II.
- Check the reason for devices in the Questioned state. See [Understanding Device Discovery Messages, page 4-10](#).

After troubleshooting your problem, check the device status. See [Viewing Discovery Status, page 4-10](#).

Changing Device Credentials

You change device credentials using Common Services DCR.

Modifying SNMP Timeout and Retries

If an SNMP query does not respond in time, DFM times out. DFM retries contacting the device for as many times as you indicate. The timeout period is doubled for every subsequent retry.

For example, if the timeout value is 4 seconds and the retries value is 3 seconds, DFM waits 4 seconds before the first retry, 8 seconds before the second retry, and 16 seconds before the third retry.

The SNMP timeout and retry values are global settings. Change these values as follows:

-
- Step 1** Select **Device Management > SNMP Config**. The SNMP Configuration page appears.
 - Step 2** Select a new SNMP Timeout setting. The default is 4 seconds.
 - Step 3** Select a new Number of Retries setting. The default is 3 retries.
 - Step 4** Click **Apply**. Click **Yes** to confirm.
-

Rediscovering a Device

You can rediscover devices or device groups using the Rediscover/Delete Devices page. When rediscovery takes place, any new device configuration settings overwrite the previous settings.

-
- Step 1** Select **Device Management > Rediscover/Delete**. The Rediscover/Delete Devices page appears.
 - Step 2** Select the devices or group(s) you want to rediscover.
 - Step 3** Click **Rediscover**.

Rediscovery is started. To view rediscovery status, select **Device Management > View Discovery Status**.

Viewing Discovery Status

To view the discovery status of a device, select **Device Management > View Discovery**.

Understanding Device Discovery Messages

[Table 4-2](#) lists messages that might be shown for devices in the Questioned state.

Table 4-2 Import Error Messages

Message	Meaning	Action
SNMP Timeout	The device is in the Questioned state because the SNMP read-only community string for the device is incorrect.	See Changing Device Credentials, page 4-9 to enter the correct read community string for the device.
Others: Missing IP Address or Data Collector Timeout	The device is in the Questioned state because of some other reason. It could be that DNS resolution for the device failed or the data collector timed out.	<p>Click the device on the Rediscover/Delete Devices page. The error message displays the exact problem.</p> <ul style="list-style-type: none"> • If the IP address is missing: <ul style="list-style-type: none"> – Readd the device with the correct IP address. or – Make sure that DFM can resolve the device name: try adding the domain name as part of the device name. • If the data collector times out, restart the daemon manager to get all data collectors in sync.

Configuring SNMP Trap Receiving and Forwarding

DFM can receive traps on any available port and forward them to other NMSs (specified by IP addresses and ports). This capability enables DFM to easily work with other trap processing applications. However, you must enable SNMP on your devices and configure SNMP to send traps either directly to DFM or to one of the following:

- An NMS
- A trap daemon

To send traps directly to DFM, perform the tasks in [Enabling Devices to Send Traps to DFM, page 4-11](#). To integrate SNMP trap receiving with an NMS or a trap daemon, follow the instructions in [Integrating DFM Trap Receiving with NMSs or Trap Daemons, page 4-12](#).

Updating the SNMP Trap Receiving Port

By default, DFM receives SNMP traps on port 162 (or, if port 162 is occupied, port 9000). If you need to change the port, you can do so.

-
- Step 1** On the Configuration tab of the DFM home page, select **Other Configurations > SNMP Trap Receiving**.
 - Step 2** Enter the port number in the Receiving Port entry box.
 - Step 3** Click **Apply**.
-

For a list of ports that DFM uses, see [Verifying TCP and UDP Ports that DFM Uses, page 2-1](#).

Enabling Devices to Send Traps to DFM

Because DFM uses SNMP MIB variables and traps to determine device health, you must configure devices to provide this information. For any Cisco devices that you want DFM to monitor, SNMP must be enabled and the device must be configured to send SNMP traps to the DFM server.

Make sure your devices are enabled to send traps to DFM by using the command line or GUI interface appropriate for your device:

- [Enabling Cisco IOS-Based Devices to Send Traps to DFM, page 4-11](#)
- [Enabling Catalyst Devices to Send SNMP Traps to DFM, page 4-12](#)

Enabling Cisco IOS-Based Devices to Send Traps to DFM

For devices running Cisco IOS software, provide the following commands:

```
(config)# snmp-server [community string] ro
(config)# snmp-server enable traps
(config)# snmp-server host [a.b.c.d] traps [community string]
```

where *[community string]* indicates an SNMP read-only community string and *[a.b.c.d]* indicates the SNMP trap receiving host (the DFM server).

For more information, see the appropriate command reference guide.

-
- Step 1** Log in to Cisco.com.
 - Step 2** Select **Products & Solutions > Cisco IOS Software**.
 - Step 3** Select the Cisco IOS Software release version used by your Cisco IOS-based devices.
 - Step 4** Select **Technical Documentation** and select the appropriate command reference guide.
-

Enabling Catalyst Devices to Send SNMP Traps to DFM

For devices running Catalyst software, provide the following commands:

```
(enable)# set snmp community read-only [community string]
(enable)# set snmp trap enable all
(enable)# set snmp trap [a.b.c.d] [community string]
```

Where *[community string]* indicates an SNMP read-only community string and *[a.b.c.d]* indicates the SNMP trap receiving host (the DFM server).

For more information, see the appropriate command reference guide.

-
- Step 1** Log in to Cisco.com.
- Step 2** Select **Products & Solutions > Switches**.
- Step 3** Select the appropriate Cisco Catalyst series switch.
- Step 4** Select **Technical Documentation** and select the appropriate command reference guide.
-

Integrating DFM Trap Receiving with NMSs or Trap Daemons

You might need to complete one or more of the following steps to integrate trap receiving with other trap daemons:

- Add the host where DFM is running to the list of trap destinations in your network devices. See [Enabling Devices to Send Traps to DFM, page 4-11](#). Specify port 162 as the destination trap port. (If another NMS is already listening for traps on the standard UDP trap port (162), use port 9000, which DFM will use by default.)
- If your network devices are already sending traps to another management application, configure that application to forward traps to DFM. See appropriate documentation for the management application.

The following sections describe different scenarios for SNMP trap receiving and lists the advantages of each.

Scenarios—DFM Receives SNMP Traps and Forwards Them to an NMS

Table 4-3 lists configurations in which DFM receives SNMP traps and forwards them to an NMS.

Table 4-3 Configuring DFM to Receive SNMP Traps and Forward Them

With DFM installed on...	You can configure DFM to...		Advantages
	Receive traps on this port and...	Forward traps to an NMS on this port	
A host with an NMS	162 (standard listening port and DFM default)	9000 (nonstandard listening port) Note You must configure the NMS to listen on this port.	<ul style="list-style-type: none"> DFM provides a reliable trap reception and forwarding mechanism. Devices do not need to be reconfigured to send traps to another host or port. DFM and the NMS run on the same host.
	9000	162	<ul style="list-style-type: none"> DFM provides a reliable trap reception and forwarding mechanism. No reconfiguration of the NMS is required; it continues to listen for traps on default port 162. DFM and the NMS run on the same host.
A host and an NMS installed on a remote host	162	162 (on the remote host)	<ul style="list-style-type: none"> DFM provides a reliable trap reception and forwarding mechanism. NMS continues to receive traps on port 162. Network devices continue to send traps to port 162.

Scenarios—An NMS Receives SNMP Traps and Forwards Them to DFM

Table 4-4 lists configurations in which an NMS receives SNMP traps and forwards the traps to DFM. In these configurations, the HPOV-NetView adapters forward SNMP traps to DFM; the adapters must be installed properly. For more information, see [Installing and Upgrading HPOV-NetView Adapters, page 2-13](#).

Table 4-4 Configuring DFM to Receive SNMP Traps Forwarded by an NMS

With DFM installed on...	And the NMS receiving traps on this port ...	Configure DFM to receive traps (forwarded from the NMS) on this port...	Advantages
A host with an NMS	162 (standard listening port)	9000 (nonstandard listening port; DFM will use this port automatically if port 162 is occupied)	<ul style="list-style-type: none"> No reconfiguration of the NMS is required. No reconfiguration of network devices is required. DFM and the NMS run on the same host. DFM does not receive traps dropped by the NMS.
A host and an NMS installed on a remote host	162 (on the remote host) Note You must install the HPOV-NetView adapters on the remote host.	162	<ul style="list-style-type: none"> No reconfiguration of the NMS is required. No reconfiguration of network devices is required. DFM does not receive traps dropped by the NMS.

Configuring SNMP Trap Forwarding

By default, DFM does not forward unprocessed SNMP traps. However, you can configure it to do so.

-
- Step 1** On the Configuration tab of the DFM home page, select **Other Configurations > SNMP Trap Forwarding**.
- Step 2** For each host, enter:
- An IP address or DNS name for the hostname.
 - A port number on which the host can receive traps.
- Step 3** Click the **Apply** button.
-

Viewing Alerts

To start the Alerts and Activities display, from the DFM home page, select **Alerts and Activities**.

Starting DFM

To start DFM, log into the CiscoWorks home page. In the Device Fault Manager pane, click the Device Fault Manager link. A Device Fault Manager window—the DFM home page—opens, focused on the Alerts and Activities tab. After you open the DFM home page, you can access all DFM applications from it.


Note

Clicking any of the following links on the CiscoWorks home page causes the DFM home page to shift focus from the Alerts and Activities tab to the correspondingly named tab:

- Device Management
- Notification Services
- Fault History
- Configuration

Clicking the Alerts and Activities link opens a separate Device Fault Manager window with an Alerts and Activities display, a real-time monitor for displaying the operational health of your network.


Note

You must add devices to DFM before the Alerts and Activities display can show results.

What Next?

After you complete the tasks in this chapter, DFM will be ready to monitor and analyze events and provide notification of alerts on the Alerts and Activities display.

[Table 4-5](#) summarizes how to continue setting up DFM.

Table 4-5 **Setting Up DFM**

Task	Description
Configure views for the Alerts and Activities display	View groups control which groups of devices are the focus of the Alerts and Activities display. DFM provides two default view groups. You can add additional view groups.
Configure notifications	In addition to learning about alerts by monitoring the Alerts and Activities display, you can subscribe users to receive email and hosts to receive DFM-generated SNMP traps in response to alerts.
Configure polling parameters and thresholds	DFM provides default values for polling parameters and threshold values. However, you can update the values as needed for your network. You should plan to apply the changes when activity on the DFM server is low.

Table 4-5 **Setting Up DFM (continued)**

Task	Description
Configure purging	By default, DFM purges the database daily at midnight. You can modify the schedule.
Configure rediscovery	DFM provides a single default schedule for rediscovery. You can use that schedule, or suspend it and create additional rediscovery schedules.

To use DFM more fully, you might want to perform additional configuration tasks. See the online help or *User Guide for Device Fault Manager 2.0.6* for information on using and configuring DFM.