



Device Fault Manager Frequently Asked Questions

- General Questions, page F-2
- DFM Domain Manager and Broker, page F-3
- Adding and Managing Devices, page F-4
- SNMP Traps, page F-9
- Polling, page F-10
- Device Discovery (Probing) and Inventory Collection, page F-11
- Faults and Alarms, page F-15
- Polling and Threshold Groups, page F-16
- Working with Interfaces, page F-19
- Adapters: Overview, page F-22
- Understanding and Modifying What DFM Console and Window Displays, page F-37
- Basic Installation Questions, page F-42
- Process Management, page F-44

General Questions

[What does DFM do?, page F-2](#)

[What is DFM not meant to be used for?, page F-2](#)

[Does DFM maintain a history of faults?, page F-2](#)

What does DFM do?

- Identifies possible problems on Cisco devices by monitoring events sent by the device ([traps](#)) and querying the device for health (SNMP)
- Interoperates with other fault management systems
- Is ready to use out of the box, with preset threshold and polling parameters

What is DFM not meant to be used for?

- MIB browsing/compiling
- Trap viewing/listening (however, DFM does listen for and process certain [SNMP traps](#))
- Server/desktop fault analysis, or network-wide/multivendor fault analysis
- Alerting users to device configuration changes

Does DFM maintain a history of faults?

DFM can maintain a history of faults if you download and install the Fault History dropin at <http://www.cisco.com/cgi-bin/tablebuild.pl/cw-fault-history>. You can also use the [File Notifier Adapter](#) to log all faults, and then, for example, write your own scripts for processing the fault file.

How often is new device support released?

DFM Incremental Device Support (IDU) packages are normally released every three months. These packages provide support for new devices, in between major DFM releases. (These packages normally also contain bug fixes.) You can download an IDU by logging into Cisco.com and pointing your browser to: <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>.

DFM Domain Manager and Broker

[What is the DFM broker?, page F-3](#)

[What is the DFM domain manager?, page F-3](#)

[Can I change the name of the domain name to something besides DFM?, page F-3](#)

[Can I define additional domains on the same system?, page F-3](#)

What is the DFM broker?

The DFM broker (called DfmBroker) is a process running DFM software that facilitates communication between a domain manager (DfmServer) and its clients (consoles and [adapters](#)). The broker maintains information about the domain manager: its name (DfmServer), the hostname on which the DfmServer is running, and the TCP port where the DfmServer listens for client connections. The broker periodically connects to DfmServer to monitor its status.

What is the DFM domain manager?

The DFM domain manager (called DfmServer) is a process running DFM software that monitors network elements, analyzes the causes of failures, and diagnoses the effects of the failures on related elements. The domain manager consists of the following:

- DFM *analysis model*, which describes the elements DFM can manage, the faults managed elements can generate, and the symptoms caused by generated faults.
- DFM *inventory*, an in-memory repository of elements managed by DFM.
- DFM *adapters*, applications that perform special communications functions, such as updating inventory information, forwarding [SNMP traps](#) to another network management system (NMS), and receiving and forwarding fault information (a file, an email address, another NMS) to other recipients.

Can I change the name of the domain name to something besides DFM?

No.

Can I define additional domains on the same system?

No. Only one copy of DFM can be installed on a machine. This is the only supported configuration for more than one domain on the same machine.

Adding and Managing Devices

- How do I add devices to DFM (so DFM can manage them)?, page F-4
- What is the difference between managed and unmanaged?, page F-5
- Are devices automatically managed when I add them to DFM?, page F-5
- Can I delete or unmanage multiple devices at one time?, page F-5
- Which devices can DFM manage?, page F-5
- How many devices can DFM manage?, page F-5
- How do I unmanage an element?, page F-6
- How do I add devices that have intelligent modules (such as a switch with an RSM or MSFC)?, page F-6
- What do I have to do if I change a managed device's community string?, page F-6
- What do I have to do if I change a managed device's IP address?, page F-6
- What determines whether or not a device element is managed?, page F-7
- How do I unmanage an element, or change an unmanaged element to managed?, page F-7
- How do I determine which ports and interfaces are managed or unmanaged?, page F-7
- What are the default managed/unmanaged ports/interfaces?, page F-7
- How do I change DFM's default behavior for determining whether or not to manage a device?, page F-8

How do I add devices to DFM (so DFM can manage them)?

You can add devices to DFM in these ways:

- Use a seed file to add a list of devices you want DFM to manage. A seed file is a two-column file listing devices by name/IP address and read-only community string.
 - For instructions on preparing a seed file, see the appropriate installation guide.
 - Be sure the default read community string matches that of your network.

The seed file must be on the same host as the [domain manager](#). Once you have prepared your seed file, add the devices by selecting **Inventory > Import from Seed File** from the Administration Console. Be sure to select **Inventory > Reconfigure** and **Inventory > Save Inventory** when you are done.

- Use the Add Agent command to add one device. Select **Inventory > Add Agent** from the Administration Console. Be sure to select **Inventory > Reconfigure** and **Inventory > Save Inventory** when you are done.
- Use the [RME Adapter](#) to automatically synchronize a local or remote Resource Manager Essentials (Essentials) inventory with the DFM [inventory](#). When devices are added to Essentials, they are automatically [probed](#) by DFM. (However, when devices are removed from Essentials, you must manually remove them from DFM.) The CiscoWorks process that performs this synchronization is called DfmChangeProbe.

What is the difference between managed and unmanaged?

Managed means that the element is monitored by the DfmServer. Unmanaged means that the element has been [probed](#) and element information is in the DFM [inventory](#), but the DfmServer is not currently monitoring the element.

Are devices automatically managed when I add them to DFM?

Yes. DFM will attempt to manage any device it discovers during [inventory collection](#). When a device is added, DFM [probes](#) it for configuration information, and adds that information to the DFM [inventory](#). What goes into the inventory depends on the device MIBs, and to what extent [DFM supports the MIB](#) (or MIBs).

Can I delete or unmanage multiple devices at one time?

Yes, if you have installed the latest DFM IDU available from <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>.

Which devices can DFM manage?

DFM can manage all devices listed on the supported devices list (see http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/ms/index.htm). Downloadable incremental device support (IDU) packages are available from <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>.

How many devices can DFM manage?

Standalone DFM can manage up to 1,000 devices and 30,000 ports (of which 15%, or 4,500, are managed ports). If DFM is installed with the LAN Management Solution (LMS) bundle, the bundle limit is 500 devices and the same number of ports (see

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/lms/index.htm). You may occasionally want to [verify how many ports are currently managed](#).

How do I unmanage an element?

From the Administration Console, select the element and right-click **Unmanage**. To unmanage a port or interface, select the element from the device's ComposedOf topology list, and right-click **Unmanage**. Be sure to select **Inventory > Reconfigure** and **Inventory > Save Inventory** when you are done. You can also unmanage all elements in a group (including a group of ports or interfaces) if you have installed the latest DFM IDU from <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>.

How do I add devices that have intelligent modules (such as a switch with an RSM or MSFC)?

Add the device before adding the module. Make sure that the community strings on the device and module are the same.

What do I have to do if I change a managed device's community string?

Change the device's community string in DFM by selecting **Inventory > Add Agent** from the Administration Console. Be sure you select **Inventory > Reconfigure** and **Inventory > Save Inventory** when you are done.

What do I have to do if I change a managed device's IP address?

Do the following from the Administration Console:

1. Delete the device from the DFM inventory (select the device and right-click **Delete**).
2. Select **Inventory > Reconfigure** and **Inventory > Save Inventory** to save your changes to the inventory (which allow you to re-add the device).
3. Add the device to the DFM inventory using **Inventory > Add Agent**. (If your device is a switch that has intelligent modules, make sure the community strings for the switch and modules are the same.)
4. Select **Inventory > Reconfigure** and **Inventory > Save Inventory**.

What determines whether or not a device element is managed?

It depends on the settings in the [polling and threshold groups](#) the element belongs to. Of course, the device must also be supported by DFM (see http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dev_sup/index.htm).

How do I unmanage an element, or change an unmanaged element to managed?

Users normally unmanage device elements they are not interested in. They also do so temporarily when they know there is an element problem and do not want to receive frequent notifications about it. Managing and unmanaging are performed from the Administration Console:

- To unmanage an element, select the element and right-click **Unmanage**.
- To manage an unmanaged element:
 - a. Select the element and right-click **Manage**.
 - b. Select the element and right-click **Rediscover** to probe the element.
 - c. Select **Inventory > Reconfigure**.
 - d. Select **Inventory > Save Inventory**.

How do I determine which ports and interfaces are managed or unmanaged?

Use the `sm_adapter` command in conjunction with the `getNetworkAdapters.asl` script as described in (see “[Listing Managed Ports and Interfaces](#)” section on page 6-14).

What are the default managed/unmanaged ports/interfaces?

- Ports (switches): By default, DFM manages trunk ports but does not manage *access ports*. DFM considers a port to be a trunk port if it connects to a Cisco network device running Cisco Discovery Protocol (CDP). In other words, a trunk port connects to a router, or to a switch that is managed by the same DFM server. DFM does not manage access ports by default (an access port is a switch port that is connected to a host or device not managed by DFM; that is, an end-station port).
- Interfaces (routers): By default, DFM manages all interfaces listed in the `ifTable`.

How do I change DFM's default behavior for determining whether or not to manage a device?

To change this behavior, [create a new polling and threshold group](#) for the elements you want to be managed by default.

SNMP Traps

[Does DFM report all SNMP traps?, page F-9](#)

[How does DFM handle SNMP traps?, page F-9](#)

[What version of SNMP traps does DFM support?, page F-9](#)

[How do I configure DFM to receive traps?, page F-10](#)

[How do I configure DFM to forward traps?, page F-10](#)

Does DFM report all SNMP traps?

No, because DFM is not a trap viewer. However, certain traps are processed (see [Appendix B, “MIBs Polled and SNMP Traps Processed or Passed-Through by DFM”](#)).

How does DFM handle SNMP traps?

For certain SNMP traps, DFM will either:

- Process the SNMP traps, or
- Treat the SNMP traps as pass-through traps and display them on the Monitoring Console.

See [Appendix B, “MIBs Polled and SNMP Traps Processed or Passed-Through by DFM”](#) for more information.

What version of SNMP traps does DFM support?

DFM 1.0 and 1.1 pollers support V1 SNMP traps for polling, receiving and forwarding. The DFM 1.1 poller can support V2 traps if you download and install the new Incremental Device Update (IDU) packages, available from Cisco.com at <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>. Received V2 traps are forwarded as V1 traps.

DFM 1.2 and DFM 1.2 Updated for Common Services Version 2.2 support V1 and V2 traps for polling and receiving. Received V2 traps are forwarded as V1 traps.

How do I configure DFM to receive traps?

DFM is already configured to receive SNMP traps, but you can specify a different listening port with the [SNMP Trap Adapter](#).

How do I configure DFM to forward traps?

Use the [SNMP Trap Adapter](#).

Polling

[What is polling?](#), page F-10

[Does DFM use only SNMP for polling?](#), page F-10

[What MIB objects does DFM poll?](#), page F-11

[By default, how often is polling done?](#), page F-11

[Can I use DFM to browse MIBs?](#), page F-11

[Do I need to download any MIBs from Cisco.com to use DFM with another NMS \(such as HP OpenView\)?](#), page F-11

[Where is the DFM-MIB?](#), page F-11

What is polling?

Polling is the process of requesting and receiving information from a particular device MIB (such as the CISCO-ENVMON MIB for voltage/temperature faults), or a particular MIB object. Polling does not reveal configuration changes, such as the addition of new interfaces. What is polled is determined by the [polling and threshold groups](#) to which a device element belongs.

Does DFM use only SNMP for polling?

No. DFM collects fault and performance information using SNMP, but device connectivity is monitored using ICMP (ping). If a device does not respond to an ICMP poll, it is placed on a “do not poll” list and is not polled by SNMP. In addition, the polling interval for ICMP is always set to be 60 seconds less than the polling interval for SNMP, to ensure that SNMP has the most current and correct data. (You can disable ICMP polling without disabling SNMP polling if you have downloaded and installed the latest patch/IDU from the DFM download site: <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>.)

What MIB objects does DFM poll?

The MIBs that DFM polls are listed in the “[MIBs Polled by DFM](#)” section on [page B-1](#).

By default, how often is polling done?

Polling is done every four minutes. An explanation of how the polling interval is calculated is provided in the “[Polling](#)” section on [page 4-2](#).

Can I use DFM to browse MIBs?

No. DFM is not a MIB browser.

Do I need to download any MIBs from Cisco.com to use DFM with another NMS (such as HP OpenView)?

No.

Where is the DFM-MIB?

Because it is not a CISCO MIB, the DFM-MIB is not available on any download site, although the contents are publicized in [Appendix C, “SNMP Trap Notifier MIB.”](#)

Device Discovery (Probing) and Inventory Collection

[What is probing?, page F-12](#)

[Will DFM detect changes I make to my devices/network configuration?, page F-12](#)

[Can I view the inventory file of managed devices?, page F-12](#)

[How often is the DFM inventory saved?, page F-12](#)

[Does DFM automatically discover new devices in the network?, page F-12](#)

[Does DFM automatically rediscover existing devices in the network?, page F-13](#)

[What is the difference between discovery, rediscovery, and inventory collection?, page F-13](#)

[Can I change the inventory collection schedule?, page F-13](#)

[What is the difference between using the Rediscovery Schedule and the Automatic Inventory Collection checkbox?, page F-13](#)

[How do I disable the Automatic Inventory Collection checkbox?, page F-13](#)

[Can I perform immediate manual discover/rediscovery?](#), page F-14

[What is device certification?](#), page F-14

[Do I have to wait for another DFM release for new device support?](#), page F-14

What is probing?

Probing is done during [rediscovery](#): it is the process of requesting and receiving device configuration information by performing a complete device MIB walk (which is how DFM discovers which MIBs a device supports). This is done when a new device is [added](#) to the [DFM inventory](#) (and the device is discovered), when [inventory collection](#) is done and devices are rediscovered, or when you perform a manual rediscovery of a device element. The device configuration DFM receives during a probe is saved to the DFM inventory.

Will DFM detect changes I make to my devices/network configuration?

Yes, but only when [inventory collection](#) is done and the device is rediscovered. You can rediscover a device manually by selecting the device and right-clicking **Rediscover**. (Be sure to select **Inventory > Reconfigure** and **Inventory > Save Inventory** after a manual rediscovery.)

Can I view the inventory file of managed devices?

No. The DFM inventory is a runtime, in-memory inventory, and is not viewable. There is a permanent inventory that is saved to disk, but it is not viewable. All changes you make are stored in the runtime inventory when you select **Inventory > Reconfigure**, but changes are saved to the permanent inventory only when [inventory collection](#) is done or when you select **Inventory > Save Inventory**. (Remember that, in addition to device information, the DFM inventory contains information on the relationships among device objects, polling and threshold groups and their settings, and so forth.)

How often is the DFM inventory saved?

The inventory is saved every six hours (but [inventory collection](#) is done once a week).

Does DFM automatically discover new devices in the network?

No; devices must be added using one of the [supported methods](#).

Does DFM automatically rediscover existing devices in the network?

Yes. By default, this is **scheduled** to be done once a week (on Sunday at midnight), and is called *inventory collection*. Devices are rediscovered for configuration information, and based on that collection, DFM updates the DFM **inventory**.

What is the difference between discovery, rediscovery, and inventory collection?

These concepts are basically the same. *Inventory collection* occurs when DFM **probes** the **inventory** to *discover* new devices, or to *rediscover* currently managed devices. DFM updates the inventory based on the results of inventory collection. A complete inventory collection is performed, by default, once a week (on Sunday at midnight).

Can I change the inventory collection schedule?

Yes, by using the Rediscovery Schedule. Select **Device Fault Manager > Administration > Device Discovery > Rediscovery Schedule**, click **Help**, and follow the instructions.

What is the difference between using the Rediscovery Schedule and the Automatic Inventory Collection checkbox?

The Automatic Inventory Collection checkbox (which is displayed when you select the DFM domain in the topology window) runs on a relative time basis. In other words, it runs relative to the last collection. The Rediscovery Schedule, on the other hand, allows you to specify a date, time, and period for collection. Because the Rediscovery Schedule function is consistent with how other CiscoWorks functions work, we recommend that you use the Rediscovery Schedule and disable the Automatic Inventory Collection checkbox.

How do I disable the Automatic Inventory Collection checkbox?

From the Administration Console:

1. Select the DFM domain in the topology window.
2. Deselect the Automatic Inventory Collection checkbox.
3. Click **Apply**, and select **Inventory > Reconfigure**.
4. Select **Inventory > Save Inventory**.

Can I perform immediate manual discover/rediscovery?

Yes, you can [probe](#) in one of three different ways, all from the Administration Console:

- To probe only a selected device, select **Inventory > Rediscover**.
- To probe everything in the update pending list, select **Inventory > Inventory Collection Pending**.
- To probe the entire inventory, select **Inventory > Inventory Collect All**.

What is device certification?

Device certification describes the level at which DFM supports a device. The higher the level, the more information DFM can provide about the device. You can check a device's certification level by selecting the device, right-clicking **Browse**, and checking the value of the Certification attribute in the Attributes tab. There are five levels of DFM device certification:

- Validated—DFM has been field-tested with this device. (This is the highest level of certification.)
- Certified—DFM uses information public MIBs to perform discovery on this device.
- Template—DFM has no information on MIBs supported by this device.
- Undiscovered—DFM has not fully discovered the device due to an [inventory collection error](#) (see the “[DFM Inventory Collection Errors](#)” section on [page 7-9](#)).
- Unsupported—DFM does not support this device.

Devices must be either Validated or Certified to be considered supported by DFM. Note that the Undiscovered level indicates an inventory collection error, not a lack of device support.

For more information on device certification levels, see the “[System Information Probe](#)” section on [page 7-2](#).

Do I have to wait for another DFM release for new device support?

No. Between major releases, support for certain Cisco devices can be downloaded. These Incremental Device Update (IDU) packages are available to all users from Cisco.com at <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>.

Faults and Alarms

[What is a fault, and how does DFM classify faults?, page F-15](#)

[What is the difference between the DFM terms fault and alarm?, page F-15](#)

[What are the most common faults and exceptions diagnosed by DFM?, page F-15](#)

[What determines how DFM performs polling and generates alarms for devices?, page F-16](#)

What is a fault, and how does DFM classify faults?

DFM considers an event to be a fault when it surpasses a threshold for acceptable behavior. When this happens, DFM generates a fault notification (or alarm), which is displayed in the Monitoring and Administration Consoles. DFM displays two kinds of fault notifications:

- *Symptomatic notifications*, which identify a single fault (symptom).
- *Compound notifications*, which identify one or more related symptoms. In DFM terminology, a compound notification is a roll-up of related symptoms.

Compounds are sometimes called *aggregates* (in the adapter configuration files), or simply *exceptions* (from the naming standard for compounds—`OperationalException`, `PerformanceException`, and so forth).

What is the difference between the DFM terms fault and alarm?

A *fault* is an event in which DFM determines a device is operating outside acceptable behavior—for example, a port is down that should be up, or a threshold has been exceeded that should not be exceeded. An *alarm* is a notification created by DFM to inform the user about the fault. DFM gathers information about the device and the fault, and then issues the alarm.

What are the most common faults and exceptions diagnosed by DFM?

The following are examples of the what DFM commonly looks for on different types of elements:

- Chassis—Backplane utilization
- Fan—Fan state not normal
- Memory—Excessive fragmentation, buffer miss rate, buffer utilization, free memory

- Network adapters—Backup activated error rates (at system and VLAN level), broadcast rates, collision rates, discard rates, flapping, maximum uptime, queue drop rates, utilization
- Power supplies—Voltage out of range
- Processors—Utilization
- SNMP agent—Unresponsive
- System—Excessive restarts
- Temperature—Temperature out of range

For more details on faults reported by DFM, see [Chapter 3, “Faults and Exceptions Diagnosed by DFM.”](#)

What determines how DFM performs polling and generates alarms for devices?

This is determined by the [polling and threshold groups](#) to which a device and its elements belong.

Polling and Threshold Groups

[What determines the defaults for DFM polling and alarm generation?, page F-16](#)

[When a device is added to DFM, how does DFM determine which polling and threshold group the device should belong to?, page F-17](#)

[What are classes and instances?, page F-17](#)

[What are the default polling and threshold groups?, page F-17](#)

[Can an element belong to more than one polling group or threshold group?, page F-17](#)

[Can I create new groups?, page F-18](#)

[How do I disable polling for a device or specific elements in a device?, page F-18](#)

[How do I disable only certain types of polling?, page F-18](#)

[How do I change polling for unwanted faults/exceptions?, page F-19](#)

[How do I change thresholds for unwanted faults/exceptions?, page F-19](#)

What determines the defaults for DFM polling and alarm generation?

This is determined by the *polling group* and *threshold group* to which a device and its elements belong. When a device is [added](#) to DFM and has been [discovered](#), the elements of the device become members of two groups—a polling group and a threshold group. These groups determine management policies for the device. The

polling group determines which device elements are [polled](#) and how often; the threshold group determines at which point DFM should generate alarm. There are different polling groups and threshold groups, and you can create groups.

When a device is added to DFM, how does DFM determine which polling and threshold group the device should belong to?

The device is assigned to polling and threshold groups depending on the group matching criteria as described in the [“Default Polling and Threshold Groups” section on page 8-5](#).

What are classes and instances?

A class is a group of objects that are structurally and operationally related, such as switches or routers. An object or element that belongs to a class is called an instance of that class; for example, a specific Cisco Catalyst 550 device is an instance of the Switch class. The most commonly used DFM classes are described in [Appendix E, “Valid Classes, Instances, and Events.”](#)

The terms *object* and *instance* are also used interchangeably, although an element normally specifies something physical (such as a power supply), while an object can specify something logical (such as a VLAN).

What are the default polling and threshold groups?

The following are the default groups:

- Default polling groups: Switches, Routers, Hubs and Bridges, Uncertified Systems, and Other Systems. For more information on the default polling groups, see the [“Default Polling Groups” section on page 8-5](#).
- Default threshold groups: Interface, Access Ports, Trunk Ports, System Resource. (By default, access ports are not managed, so that group will be empty.) If you have downloaded and installed Patch/IDU 1.2.9 or later, there are three additional threshold groups: System Elements, Unmanaged Ports/Interfaces, and Unmanaged systems (go to <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>.) For more information on the default threshold groups, see the [“Default Threshold Groups” section on page 8-7](#).

Can an element belong to more than one polling group or threshold group?

Yes. If an element belongs to more than one group, DFM will use the settings of the group with the highest priority (see the [“Method for Setting Priorities” section on page 8-17](#)).

Can I create new groups?

Yes. The following are examples of why you might want to do this:

- To [poll](#) certain routers more frequently
- To change DFM default behavior regarding unmanaged elements (so they are managed by default)
- To set port flapping thresholds on specific router interfaces

For information on how to create groups, see the [“Creating New Groups” section on page 8-22](#). If you want to create a group that is a subset of an existing group—such as a group of routers—select the existing group, and then select **Group > New Group**. You can then adjust the settings as desired. Be sure to select **Apply**, **Inventory > Reconfigure** and **Inventory > Save Inventory** when you are done.

How do I disable polling for a device or specific elements in a device?

You should [unmanage](#) the device if you want to disable [polling](#) for all elements in a device, or if you want to disable polling for a group of devices. To disable polling for only certain elements in a device (such as ports), select the specific element and right-click **Unmanage**. (Be sure to select **Inventory > Reconfigure** and **Inventory > Save Inventory** when you are done.)

How do I disable only certain types of polling?

Disable the AnalysisMode setting for that type of [polling](#). For example, to poll ports and interfaces for performance but not for connectivity, do the following:

1. From the Polling and Thresholds Console, select the Polling tab and locate the polling group you want to reconfigure.
2. Under Settings, select the type of polling you want to disable (for example, Connectivity Polling—Ports and Interfaces).
3. In the right window, set AnalysisMode to Disable.
4. Click **Apply**.
5. Select **Group > Reconfigure**.
6. To permanently save your changes, from the Administration Console, select **Inventory > Save Inventory**.

How do I change polling for unwanted faults/exceptions?

From the Polling and Thresholds Console, select the Polling tab. Select the polling type on the left, and adjust the threshold on the right. Be sure to do the following to save your settings:

1. Click **Apply**.
2. Select **Group > Reconfigure**.
3. From the Administration console, select **Inventory > Save Inventory**.

How do I change thresholds for unwanted faults/exceptions?

From the Polling and Thresholds Console, select the Thresholds tab. Select the setting on the left, and adjust the threshold on the right. Be sure to do the following to save your settings:

1. Click **Apply**.
2. Select **Group > Reconfigure**.
3. From the Administration Console, select **Inventory > Save Inventory**.

Working with Interfaces

[How does DFM determine an interface mode?, page F-19](#)

[How do I change an interface mode?, page F-20](#)

[If I reload a device, will DFM automatically recognize the device's ifIndex change?, page F-20](#)

[How does DFM handle port/interface duplexity?, page F-20](#)

[How do I disable management for virtual interfaces?, page F-21](#)

How does DFM determine an interface mode?

DFM classifies most interfaces as NORMAL, with the following exceptions:

- PPP, SLIP—Dial-on-Demand
- BRI, ISDN—Backup

(ISDN interfaces are modeled differently if you have installed the latest DFM IDU available from <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>.)

How do I change an interface mode?

Although it appears as if you can edit the group attribute fields using the Administration Console, such changes do not affect the settings. You must use the Polling and Thresholds Console and create a new group to change the interface mode. The following tells you how to change PPP interfaces from the default mode (Dial-on-Demand) to NORMAL:

1. From the Polling and Thresholds Console, in the Thresholds tab, create a new interface group called PPP.
2. Add the following Matching Criteria: TYPE=PPP, MODE=NORMAL
3. Increase the Priority of this new Multilink PPP Group to a higher level than the default group (Dial-on-Demand).
4. Click **Apply**.
5. Click **Reconfigure**.
6. Verify the members of the new PPP group.
7. From the Administration Console, select **Inventory > Save Inventory**.

If I reload a device, will DFM automatically recognize the device's ifIndex change?

No, not until [inventory collection](#) is done. You should manually [rediscover](#) the device from the Administration Console:

1. Select the device and right-click **Rediscover**.
2. Select **Inventory > Reconfigure**.
3. Select **Inventory > Save Inventory**.

How does DFM handle port/interface duplexity?

DFM determines duplexity in different ways, depending upon which version of DFM you are running. For details see [“Understanding the High Utilization Fault” section on page 3-12](#). If you know that the value is incorrect, you can change it manually (see the [“Wildcard Patterns” section on page 8-24](#)).

How do I disable management for virtual interfaces?

If you have downloaded and installed DFM 1.2 Patch/IDU 1.2.9 (or later) you can perform bulk manage and unmanage operations on selected groups of ports or interfaces.

1. From the Polling and Thresholds Console, in the Thresholds tab, select the port or interface group you wish to unmanage.
2. Right-click **Unmanage**.
3. Select **Reconfigure** from the Group menu.
4. Select **Save Inventory** from the Inventory menu to update the DFM inventory.

If you have not downloaded and installed the latest patch/IDU, to disable analysis for interfaces (or ports), assign the interfaces to a new group that has no settings:

1. From the Administration Console, select **Edit > Polling and Thresholds**.
2. In the Thresholds tab, expand the topology tree until you have expanded Interface Groups.
3. Select Interface Groups and right-click **New Group**.
4. Enter a new name for the group (for example, “Virtual Interfaces”) and an optional description. The new group is displayed under Interface Groups.
5. Select the new group and the Matching Criteria tab.
6. Set the matching criteria:
 - a. Select DeviceID and/or Description from the Disabled Criteria list.
 - b. Click **Enable**.
 - c. Double-click the Value column to change the value used in matching criteria (this example is for virtual interfaces):
For DeviceID, use “*VL*”
For Description, use “*VLAN*”
 - d. Click **Register** and **Apply**.
7. Under the Priorities tab, select the new group you created.
8. Using the arrow button, move the new group to the top of the list (to make it highest priority).
9. Click **Apply**.

10. Select the DFM domain and **Group > Reconfigure**.
11. From the Administration Console, select the DFM domain and **Inventory > Save Inventory**.

Adapters: Overview

[What are DFM adapters?](#), page F-22

[What are the basics of adapter configuration?](#), page F-23

[How do I set up notification adapters to monitor only selected faults?](#), page F-24

[What are the names of the CiscoWorks adapter processes?](#), page F-25

[File Notifier Adapter](#), page F-25

[Mail Notifier Adapter](#), page F-27

[Trap Notifier Adapter](#), page F-29

[HPOV-NetView Adapter](#), page F-31

[SNMP Trap Adapter](#), page F-33

[RME Adapter](#), page F-36

What are DFM adapters?

Adapters are applications that run as separate processes connecting the DfmServer to its environment. Adapters allow DFM to communicate and exchange information with other applications. DFM adapters can be classified as follows:

- *Notification adapters*, which forward event information to designated recipients:
 - A file ([File Notifier Adapter](#))
 - An email address ([Mail Notifier Adapter](#))
 - Another NMS ([Trap Notifier Adapter](#))
- *Event adapters*, which forward traps from another NMS to DFM. The [HPOV-NetView Adapter](#) performs this function for HP OpenView and NetView.

- *Special adapters*, which perform special functions:
 - *SNMP Trap Adapter*, which receives and/or forwards pass-through and certain processed SNMP traps.
 - *RME Adapter*, which synchronizes the DFM [inventory](#) with the list of devices in the Resource Manager Essentials inventory.

What are the basics of adapter configuration?

The following are adapter starting points:

- You do not have to do anything to start these adapters; they start automatically when installed:
 - The [RME Adapter](#) starts automatically if Resource Manager Essentials (Essentials) is installed on the same machine as the adapter. Even if Essentials is installed after the adapter, the adapter detects the installation and starts automatically (unless it is manually disabled).
 - The [HPOV-NetView Adapter](#) starts automatically if HP OpenView or NetView is installed on the same machine. If HP OpenView or NetView is installed after the adapter, the adapter detects the installation and starts automatically.
 - The [SNMP Trap Adapter](#) (for trap receiving).
- You must manually start this adapter, but you do not need to configure it unless you want to use a listening port other than 162:
 - [File Notifier Adapter](#)
- You must configure and manually start these adapters:
 - [Mail Notifier Adapter](#)
 - [Trap Notifier Adapter](#)
 - [SNMP Trap Adapter](#) (for forwarding)
- If the CiscoWorks daemon manager goes down, adapters requiring manual starts will not be restarted. You can use the command line to modify this behavior and register these adapters for automatic restart.

How do I set up notification adapters to monitor only selected faults?

You must manually edit the adapter configuration file, and then restart the appropriate [CiscoWorks adapter process](#).

You can do one of the following:

- Specify an existing subscription profile (*filename*) by using this code fragment:

```
SubscribesTo =
{
    GA_ProfileSubscription::Descriptive-Text
    {
        profileName = "filename"
    }
}
```

See the [“Specifying a Notification Adapter Subscription Profile” section on page 10-11](#) for subscriptions examples.

- Specify the classes, instances, and events you want the notification adapter to track by using this code fragment (do not use a comma after the final fragment):

```
GA_ChoiceSubscription::Descriptive-Text
{
    # Subscribe to events whose class, instance, and event
    # names match the given pattern.
    className = "class"
    instanceName = ".*"
    eventName = "event"
    aggregates = {TRUE|FALSE}
    symptoms = {TRUE|FALSE}
},
GA_ChoiceSubscription::Descriptive-Text
{
    # Subscribe to events whose class, instance, and event
    # names match the given pattern.
    className = "class"
    instanceName = ".*"
    eventName = "event"
    aggregates = {TRUE|FALSE}
    symptoms = {TRUE|FALSE}
}
```

Note that you cannot use include or exclude patterns, and you can use the wildcard pattern only for instanceName (see the [“Examples of Subscription Choices” section on page 10-14](#) for subscriptions examples).

What are the names of the CiscoWorks adapter processes?

The following adapters are CiscoWorks processes:

- File Notifier Adapter: DfmFileNotifier
- Mail Notifier Adapter: DfmMailNotifier
- Trap Notifier Adapter: DfmTrapNotifier
- RME Adapter: DfmChangeProbe
- SNMP Trap Adapter: part of DfmServer process

The HPOV-NetView Adapter does not have a corresponding CiscoWorks process.

File Notifier Adapter

[What does the File Notifier Adapter do?, page F-25](#)

[Can I modify the content of the information saved by the File Notifier Adapter?, page F-25](#)

[Where is the File Notifier Adapter configuration file located?, page F-26](#)

[Where is the File Notifier Adapter log file?, page F-26](#)

[Where is the log of alarms stored by the File Notifier Adapter?, page F-26](#)

[What do I have to do to get the File Notifier Adapter running?, page F-26](#)

[How do I specify which alarms I want logged by the File Notifier Adapter?, page F-26](#)

[What do I have to do if I make a manual change to the File Notifier Adapter configuration file?, page F-26](#)

[How do I disable the File Notifier Adapter?, page F-26](#)

What does the File Notifier Adapter do?

The File Notifier Adapter creates an alarm log of all notifications processed by DFM, and stores the notifications in a file. A file is the only valid recipient for this adapter, and you cannot change the location of the alarm log file (NMSROOT/objects/smarts/logs/DFM-alarms.log).

Can I modify the content of the information saved by the File Notifier Adapter?

You can modify the types of faults that are logged, but you cannot change the format of the file. The following is an example of the file contents:

```
02-Feb-2001 11:58:38 NOTIFY Switch::172.16.0.0::DiscoveryError 100% An error was encountered during the last discovery probe of this System.
```

```
02-Feb-2001 12:00:19 CLEAR Switch::172.16.0.0::DiscoveryError An error
was encountered during the last discovery probe of this System.
```

```
02-Feb-2001 12:03:14 NOTIFY Switch::172.16.0.0::PowerSupplyException
100% System is experiencing power supply problems.
```

Where is the File Notifier Adapter configuration file located?

The File Notifier Adapter configuration file is at *NMSROOT/objects/smarts/conf/notifier/filelog_notify.conf*.

Where is the File Notifier Adapter log file?

The File Notifier Adapter log file is at *NMSROOT/objects/smarts/logs/sm_file_notifier.log*.

Where is the log of alarms stored by the File Notifier Adapter?

The File Notifier Adapter alarm log file is at *NMSROOT/objects/smarts/logs/DFM-alarms.log*.

What do I have to do to get the File Notifier Adapter running?

Select **Device Fault Manager > Administration > Fault Notification > File Notifier**, click **Help**, and follow the instructions.

To log only certain alarms, you must [edit the configuration file](#). If the CiscoWorks daemon manager goes down, the adapter will not be restarted when DFM comes up. If you want it to automatically restart, you must register the adapter as described in the “[Registering and Unregistering the DFM Processes Using pdcmd](#)” section on page 11-15.

How do I specify which alarms I want logged by the File Notifier Adapter?

You must manually [edit the configuration file](#) to subscribe to specific events.

What do I have to do if I make a manual change to the File Notifier Adapter configuration file?

You must restart the DfmFileNotifier process for your changes to take effect.

How do I disable the File Notifier Adapter?

Select **Device Fault Manager > Administration > Fault Notification > File Notifier**, click **Help**, and follow the instructions.

If you have configured the adapter to restart upon CiscoWorks restart and you want to disable automatic restart of the adapter, see the [“Registering and Unregistering the DFM Processes Using pdcmd”](#) section on page 11-15.

Mail Notifier Adapter

[What does the Mail Notifier Adapter do?](#), page F-27

[Do I have to have an SMTP server to use the Mail Notifier Adapter?](#), page F-27

[Where is the Mail Notifier Adapter configuration file?](#), page F-27

[Where is the Mail Notifier Adapter log file?](#), page F-28

[What do I have to do to get the Mail Notifier Adapter running?](#), page F-28

[Can I use the Mail Notifier Adapter to send a page when a certain fault occurs?](#), page F-28

[Can I modify the content of the email sent by the Mail Notifier Adapter?](#), page F-28

[Can I configure the Mail Notifier Adapter to send notifications to different recipients depending on the fault type?](#), page F-28

[What is the difference between using the Mail Notifier Adapter and Edit > Recipients in the Monitoring Console?](#), page F-28

[Can I configure the adapter to send email only when certain alarms are generated?](#), page F-28

[What do I have to do if I make a manual change to the Mail Notifier Adapter configuration file?](#), page F-29

[How do I disable the Mail Notifier Adapter?](#), page F-29

What does the Mail Notifier Adapter do?

The Mail Notifier Adapter sends email to an email address when DFM generates certain notifications.

Do I have to have an SMTP server to use the Mail Notifier Adapter?

Yes.

Where is the Mail Notifier Adapter configuration file?

The Mail Notifier Adapter configuration file is at *NMSROOT/objects/smarts/conf/notifier/mail_notify.conf*.

Where is the Mail Notifier Adapter log file?

The Mail Notifier Adapter log file is at *NMSROOT/objects/smarts/logs/sm_mail_notifier.log*.

What do I have to do to get the Mail Notifier Adapter running?

Select **Device Fault Manager > Administration > Fault Notification > Mail Notifier**, click **Help**, and follow the instructions.

To log only certain alarms, you must [edit the configuration file](#). If the CiscoWorks daemon manager goes down, the adapter will not be restarted when DFM comes up. If you want it to automatically restart, you must register the adapter as described in the [“Registering and Unregistering the DFM Processes Using pdcmd”](#) section on page 11-15.

Can I use the Mail Notifier Adapter to send a page when a certain fault occurs?

Yes, if the email address you provide is a paging gateway.

Can I modify the content of the email sent by the Mail Notifier Adapter?

You can modify the types of faults that are logged, but you cannot modify the content of the email. The following is an example of an email sent by the Mail Notifier Adapter:

```
InCharge Domain: DFM Router 10.3.28.1 OperationalException - This system or the components of this system are not functioning properly
```

Can I configure the Mail Notifier Adapter to send notifications to different recipients depending on the fault type?

No. You can send notifications to different recipients, but all recipients will receive the same information.

What is the difference between using the Mail Notifier Adapter and Edit > Recipients in the Monitoring Console?

The Edit > Recipients function is not supported. Use **Device Fault Manager > Administration > Fault Notification > Mail Notifier**.

Can I configure the adapter to send email only when certain alarms are generated?

Yes. You must manually [edit the configuration file](#) to subscribe to specific events.

What do I have to do if I make a manual change to the Mail Notifier Adapter configuration file?

You must restart the DfmMailNotifier process for your changes to take effect.

How do I disable the Mail Notifier Adapter?

Select **Device Fault Manager > Administration > Fault Notification > Mail Notifier**, click **Help**, and follow the instructions.

If you have configured the adapter to restart upon CiscoWorks restart and you want to disable automatic restart of the adapter, see the [“Registering and Unregistering the DFM Processes Using pdcmd”](#) section on page 11-15.

Trap Notifier Adapter

[What does the Trap Notifier Adapter do?](#), page F-29

[Where is the Trap Notifier Adapter configuration file?](#), page F-30

[Where is the Trap Notifier Adapter log file?](#), page F-30

[Can I forward traps to multiple NMSs using the Trap Notifier Adapter?](#), page F-30

[Can I configure the Trap Notifier Adapter to send notifications only when certain alarms are generated?](#), page F-30

[Can I configure the Trap Notifier Adapter to send notifications to different NMSs, depending on the fault type?](#), page F-30

[Can I configure the Trap Notifier Adapter to use a different community string for outgoing traps?](#), page F-30

[What do I have to do to get the Trap Notifier Adapter running?](#), page F-31

[What do I have to do if I make a manual change to the Trap Notifier Adapter configuration file?](#), page F-31

[How do I disable the Trap Notifier Adapter?](#), page F-31

What does the Trap Notifier Adapter do?

The Trap Notifier Adapter converts DFM alarms displayed on the Monitoring Console into [SNMP traps](#), and forwards these traps to an NMS, normally for additional processing or display. The converted alarms can also be forwarded to another domain manager. DFM has its own MIB for generating the SNMP traps; you do not have to download the MIB to use it. (Although the MIB is not on a download site, you can view its contents in [Appendix C, “SNMP Trap Notifier MIB.”](#))

Where is the Trap Notifier Adapter configuration file?

The Trap Notifier Adapter configuration file is at *NMSROOT/objects/smarts/conf/notifier/trap_notify.conf*.

Where is the Trap Notifier Adapter log file?

The Trap Notifier Adapter log file is at *NMSROOT/objects/smarts/log/sm_trap_notifier.log*.

Can I forward traps to multiple NMSs using the Trap Notifier Adapter?

Yes, but you will have to manually edit the configuration file and restart the CiscoWorks DfmTrapNotifier process. The following excerpt from the configuration file shows the portion of the file that you must edit:

#For case of three recipients:

```
ProvidesAdditionalParams =
Trap_AdapterParams::trap_Notifier-Parameters
{
    recipients = {{"host_name1", 162, "1"},
                  {"host_name2", port_num2, "1"},
                  {"host_name3", port_num3, "1"} }
}
```

Can I configure the Trap Notifier Adapter to send notifications only when certain alarms are generated?

Yes. You must manually [edit the configuration file](#) to subscribe to specific events.

Can I configure the Trap Notifier Adapter to send notifications to different NMSs, depending on the fault type?

No. You can send traps to different NMSs, but all NMSs will receive the same information.

Can I configure the Trap Notifier Adapter to use a different community string for outgoing traps?

You can do this if you have downloaded and installed DFM 1.2 Patch/IDU 1.2.8 or later (from <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>). For more information, refer to “Using the Command Line to Configure the Trap Notifier Adapter” section on page 10-23.

What do I have to do to get the Trap Notifier Adapter running?

Select **Device Fault Manager > Administration > Fault Notification > Trap Notifier**, click **Help**, and follow the instructions.

To log only certain alarms, you must [edit the configuration file](#). If the CiscoWorks daemon manager goes down, the adapter will not be restarted when DFM comes up. If you want it to automatically restart, you must register the adapter as described in the [“Registering and Unregistering the DFM Processes Using pdcmd”](#) section on page 11-15.)

What do I have to do if I make a manual change to the Trap Notifier Adapter configuration file?

You must restart the DfmTrapNotifier process for your changes to take effect.

How do I disable the Trap Notifier Adapter?

Select **Device Fault Manager > Administration > Fault Notification > Trap Notifier**, click **Help**, and follow the instructions.

If you have configured the adapter to restart upon CiscoWorks restart and you want to disable automatic restart of the adapter, see the [“Registering and Unregistering the DFM Processes Using pdcmd”](#) section on page 11-15.)

HPOV-NetView Adapter

[What does the HPOV-NetView Adapter do?, page F-32](#)

[Can the HPOV-NetView Adapter work on a remote HP OpenView or NetView host that is not running CiscoWorks?, page F-32](#)

[If traps are forwarded to HP OpenView or NetView, how are the messages formatted?, page F-32](#)

[What versions of HP OpenView and NetView will work with the HPOV-NetView Adapter?, page F-32](#)

[What do I have to do to get the HPOV-NetView Adapter running?, page F-32](#)

[Under what circumstances would I make a manual change to the HPOV-NetView Adapter configuration file?, page F-32](#)

[Where is the HPOV-NetView Adapter configuration file?, page F-33](#)

[Where is the HPOV-NetView Adapter log file?, page F-33](#)

What does the HPOV-NetView Adapter do?

The HPOV-NetView Adapter forwards traps from a local or remote HP OpenView or NetView NMS to DFM, enabling DFM to receive traps from devices managed by HP OpenView and NetView.

Can the HPOV-NetView Adapter work on a remote HP OpenView or NetView host that is not running CiscoWorks?

Yes. A special installation script is provided with DFM to do this, as described in the appropriate installation guides.

If traps are forwarded to HP OpenView or NetView, how are the messages formatted?

The format is specified in the DFM MIB, as described in [Appendix C, “SNMP Trap Notifier MIB.”](#)

What versions of HP OpenView and NetView will work with the HPOV-NetView Adapter?

The DFM 1.2 and DFM 1.2 Updated for Common Services Version 2.2 HPOV-NetView Adapters work with:

- HP OpenView 6.2
- NetView:
 - 6.01 (DFM 1.2, and DFM Updated for Common Services Version 2.2)
 - 7.1 (DFM 1.2 Updated for Common Services Version 2.2)

What do I have to do to get the HPOV-NetView Adapter running?

If HP OpenView or NetView is installed on the same machine as DFM, you do not have to do anything. The adapter starts running as soon as it detects HP OpenView or NetView. When CiscoWorks starts, the adapter will automatically start. If HP OpenView or NetView is on a remote machine, you must install the remote HPOV-NetView Adapter on the remote machine, as described in the installation guides.

Under what circumstances would I make a manual change to the HPOV-NetView Adapter configuration file?

You should never change this configuration file.

Where is the HPOV-NetView Adapter configuration file?

The HPOV-NetView Adapter configuration file is at one or both of the following locations, depending on whether you are using HP OpenView or NetView:

- HP OpenView: *NMSROOT/objects/smarts/conf/OV/server.conf*
- NetView: *NMSROOT/objects/smarts/conf/NV/server.conf*

Where is the HPOV-NetView Adapter log file?

The HPOV-NetView Adapter log file is located at one or both of the following locations, depending on whether you are using HP OpenView or NetView:

- HP OpenView: *NMSROOT/objects/smarts/logs/sm_ov_fwd.log*
- NetView: *NMSROOT/objects/smarts/logs/sm_nv_fwd.log*

SNMP Trap Adapter

[What does the SNMP Trap Adapter do?, page F-33](#)

[What is the difference between the SNMP Trap Adapter and the Trap Notifier Adapter?, page F-34](#)

[Where is the SNMP Trap Adapter configuration file?, page F-34](#)

[Where is the SNMP Trap Adapter log file?, page F-34](#)

[What do I have to do to get the SNMP Trap Adapter running?, page F-34](#)

[What if another NMS is already using the trap listening port?, page F-35](#)

[Can I configure the SNMP Trap Adapter to use a different community string for forwarding destinations?, page F-35](#)

[How do I disable the SNMP Trap Adapter?, page F-35](#)

[What do I have to do if I make a manual change to the SNMP Trap Adapter configuration file?, page F-35](#)

What does the SNMP Trap Adapter do?

The SNMP Trap Adapter listens for SNMP traps sent from devices (or another NMS), and forwards these traps to another network management system (NMS). These are pass-through traps; in other words, DFM does not process these traps.

What is the difference between the SNMP Trap Adapter and the Trap Notifier Adapter?

The SNMP Trap Adapter and the [Trap Notifier Adapter](#) are similar in that they both forward [SNMP traps](#) to other NMSs. The difference is how they treat the traps they receive:

- The SNMP Trap Adapter simply treats all received traps as pass-through traps and forwards them.
- The Trap Notifier Adapter converts alarms shown on the Monitoring Console into SNMP trap messages (using its own MIB), and then forwards them. (The MIB is described in [Appendix C, “SNMP Trap Notifier MIB.”](#))

Where is the SNMP Trap Adapter configuration file?

The SNMP Trap Adapter configuration file is *NMSROOT/objects/smarts/conf/trapd/trapd.conf*.

Where is the SNMP Trap Adapter log file?

The SNMP Trap Adapter log file is the same as the domain manager log file: *NMSROOT/objects/smarts/logs/DFM.log*.

What do I have to do to get the SNMP Trap Adapter running?

You normally do not have to do anything to configure the adapter for trap receiving, unless you want to use a listening port other than 162. You do have to configure the adapter for trap forwarding.

- For trap receiving:
 - Verify that the listening port is correct by selecting **Device Fault Manager > Administration > Trap Configuration > Trap Receiving**, clicking the **Help** button, and following the instructions.
 - Make sure you have configured your devices (or network management servers) to forward traps to the listening port specified by the adapter (normally 162).
- For trap forwarding:
 - Select **Device Fault Manager > Administration > Trap Configuration > Trap Forwarding**, click **Help**, and follow the instructions. You must restart the DfmServer process for your changes to take effect.

The SNMP Trap Adapter will always restart when CiscoWorks is restarted.

What if another NMS is already using the trap listening port?

If the standard UDP listening port, 162, is already being used, we suggest you use port 9000. You must reconfigure the SNMP Trap Adapter to listen on this port for trap receiving. Also make sure that any NMSs or devices that are forwarding traps use the correct port.

Can I configure the SNMP Trap Adapter to use a different community string for forwarding destinations?

You can do this if you have downloaded and installed DFM 1.2 Patch/IDU 1.2.8 or later (from <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>). For more information, refer to “Using the Command Line to Configure the SNMP Trap Adapter” section on page 10-38.

How do I disable the SNMP Trap Adapter?

You normally do not have to do anything to configure the adapter for trap receiving, unless you want to use a listening port other than 162. For trap forwarding, you do have to configure the adapter.

- For trap receiving, you should never disable the adapter for trap receiving.
- For trap forwarding:

Select **Device Fault Manager > Administration > Trap Configuration > Trap Forwarding**, click **Help**, and follow the instructions. You must restart the DfmServer process for your changes to take effect.

You cannot disable the SNMP Trap Adapter from starting automatically upon CiscoWorks restart, because this would disable trap receiving.

What do I have to do if I make a manual change to the SNMP Trap Adapter configuration file?

You must restart the DfmServer process.

RME Adapter

[What does the RME Adapter do?, page F-36](#)

[Where is the RME Adapter configuration file?, page F-36](#)

[Where is the RME Adapter log file?, page F-36](#)

[What do I have to do to get the RME Adapter running?, page F-36](#)

[How do I disable the RME Adapter?, page F-36](#)

[What do I have to do if I make a manual change to the RME Adapter configuration file?, page F-37](#)

What does the RME Adapter do?

The RME Adapter synchronizes the list of managed devices in a local remote Resource Manager Essentials (Essentials) inventory with the [DFM inventory](#). As soon as a device is added to Essentials, or the configuration of an Essentials device is changed, the device is [probed](#) and added to the DFM inventory. However, devices deleted from the Essentials inventory are not automatically deleted from the DFM inventory; you must do this manually. (Unless the device is deleted from the Essentials inventory, it will continue to be re-added to the DFM inventory whenever the inventories are synchronized.)

Where is the RME Adapter configuration file?

There is no such file.

Where is the RME Adapter log file?

The RME Adapter log file is at *NMSROOT/conf/dfm/DfmChangeProbe.log*.

What do I have to do to get the RME Adapter running?

If Resource Manager Essentials (Essentials) is installed on the same machine as DFM, select **Device Fault Manager > Administration > Device Discovery > ChangeProbe**, click **Help**, and follow the instructions. As soon as the adapter detects Essentials, it starts running. You do not need to restart the DfmServer process; upon any CiscoWorks restart, the adapter automatically restarts.

If Essentials is on a remote machine, you must install the remote RME Adapter on the remote machine, as described in the appropriate installation guides.

How do I disable the RME Adapter?

Select **Device Fault Manager > Administration > Device Discover > ChangeProbe**, click **Help**, and follow the instructions.

If you have configured the adapter to restart upon CiscoWorks restart and you want to disable automatic restart of the adapter, you must unregister the DfmChangeProbe process. Follow the instructions for the notifier adapter processes in the [“Configuring the File Notifier Adapter”](#) section on page 10-17.

What do I have to do if I make a manual change to the RME Adapter configuration file?

There is no such configuration file.

Understanding and Modifying What DFM Console and Window Displays

[How do I control what devices and alarms DFM displays in the Alarm Log?, page F-38](#)

[In the Alarm Log, what do the Certainty, Count, Last Change, and First Notify columns represent?, page F-38](#)

[What do the different colors in the Alarm Log mean?, page F-39](#)

[What do the shades of purple \(compound\) and orange \(symptom\) in the Alarm Log mean?, page F-39](#)

[Can I change the colors displayed in the DFM consoles?, page F-39](#)

[What does it mean when an attribute is grayed out?, page F-39](#)

[Does DFM limit how many instances of an object it can display?, page F-39](#)

[Time and Timestamp Issues, page F-40](#)

[Clearing and Deleting Alarms, page F-41](#)

How do I control what devices and alarms DFM displays in the Alarm Log?

- To permanently remove all information about an element from the Alarm Log, do the following in the Administration Console:
 - a. Select the element and right-click **Unmanage**.
 - b. Select **Inventory > Reconfigure**.
 - c. Select **Inventory > Save Inventory**.
- To display only certain notifications in the Alarm Log, do one of the following:
 - Use the Alarm Log Filter Criteria dialog box to control *everything* that is displayed whenever the Alarm Log is opened. From the Alarm Log, select **Log > Filter** (see the “[Customizing the Alarm Log View with Filters](#)” section on page 13-7).
 - Use a subscription profile to control what is displayed whenever you open the Alarm Log (and other DFM consoles). From the Administration Console, select **Even > Maintain Profile** (see the “[Changing Your Subscription Profile](#)” section on page 13-22).

In the Alarm Log, what do the Certainty, Count, Last Change, and First Notify columns represent?

- *Certainty*—How reliable the alarm is. Certainty is always 100%, because in DFM fault analysis rule definitions, each alarm is associated with no more than one pattern of events; therefore, certainty is not applicable.
- *Count*—How many times the alarm has occurred since opening a console. Count is increased when the alarm recurs after becoming inactive (an alarm becomes inactive when has not recurred for ten minutes).
- *Last Change*—When the alarm was last generated, relative to the current time.
- *First Notify*—When the alarm was first generated.

What do the different colors in the Alarm Log mean?

- *Purple* indicates a **compound event**
- *Orange* indicates a **symptomatic event**
- *White with blue letters* indicates that the event has become inactive (because the event was either addressed or is no longer occurring). After ten polls, inactive events are removed from the display.
- *White with grey letters* indicates that the event state has changed to inactive because DFM no longer subscribes to the element.

What do the shades of purple (compound) and orange (symptom) in the Alarm Log mean?

The darker the shade, the higher the alarm count (in other words, the number of times the alarm has occurred since the console was opened).

Can I change the colors displayed in the DFM consoles?

No; these colors are predefined.

What does it mean when an attribute is grayed out?

A grayed-out attribute indicates one of the following:

- The **domain manager** is not required to **poll** the device for this attribute value.
- The domain manager encountered an error while polling the device for this attribute value. (The device might be down, or it might be up but inaccessible due to network problems.)
- The same data is available from another portion of the MIB.
- This portion of the MIB is not available on this device model.

Does DFM limit how many instances of an object it can display?

DFM cannot display objects containing more than 1,000 instances. If the number of instances exceeds that limit, you will not be able to open or expand the object when you click its plus (+) sign.

Time and Timestamp Issues

[What time zone does a DFM timestamp represent?, page F-40](#)

[Can I change the server timestamp?, page F-40](#)

[What does the information in the general tab of the Notification Properties window represent?, page F-40](#)

[What do the attribute values in the Inventory Browser represent?, page F-40](#)

What time zone does a DFM timestamp represent?

DFM always uses the server time zone when displaying time information on the consoles. Keep this in mind if your devices use time zones that are different from those of the server.

Can I change the server timestamp?

Yes, by changing the timestamp of the DFM server host machine.

What does the information in the general tab of the Notification Properties window represent?

The following describes what the information in the General tab represents:

- The Notification information at the top of the window represents the absolute time of the last generated alarm (the same as Last Notify).
- Last Notify represents the absolute time of the last generated alarm (*Current Time - Last Change = Last Notify*).
- *Count* represents the number of times the alarm has occurred since opening a console. Count is increased when the alarm recurs after becoming inactive (an alarm becomes inactive when has not recurred for ten minutes).

What do the attribute values in the Inventory Browser represent?

All attribute values in the Inventory Browser represent the *current* state of the element.

Clearing and Deleting Alarms

How do I remove events I'm not interested in from the Alarm Log?, page F-41
What happens if I clear an alarm, but other clients (with the same privileges) are viewing the same server's console?, page F-41

Can I retrieve the value of an attribute that corresponds to when the alarm was generated?, page F-41

Why does an alarm count continue to increment after I delete the alarm?, page F-41

How do I remove events I'm not interested in from the Alarm Log?

There are two ways to do this:

- For active alarms, select the alarm and right-click **Acknowledge**. This removes the alarm from your Monitoring Console (but not from other users' Monitoring Consoles). If the alarm becomes inactive (does not occur for ten minutes) and then reoccurs, it is displayed in your Monitoring Console again.
- For inactive alarms:
 - To remove a specific inactive alarm, select the alarm and right-click **Delete**.
 - To remove all inactive alarms, select **Log > Remove Cleared Events**.

What happens if I clear an alarm, but other clients (with the same privileges) are viewing the same server's console?

As long as one console remains open in the session, the alarm will continue to return.

Can I retrieve the value of an attribute that corresponds to when the alarm was generated?

No. The values DFM presents are always current values.

Why does an alarm count continue to increment after I delete the alarm?

The alarm count will increment if the alarm becomes inactive (does not occur for ten minutes) but then becomes active again. (The count will not restart at 0.)

Basic Installation Questions

[What are the basics I should be aware of when installing DFM?, page F-42](#)

[What must I do to get DFM started?, page F-42](#)

[What happens if I exceed the managed device limit?, page F-43](#)

[How can I find out how many devices/objects DFM is currently managing?, page F-43](#)

[Can DFM coexist with Essentials, Campus Manager, CiscoView, or other Cisco products?, page F-43](#)

[What should I do after installing DFM?, page F-43](#)

What are the basics I should be aware of when installing DFM?

- Use the appropriate version of CD One or CiscoWorks Common Services:
 - Use DFM 1.2 Updated for Common Services Version 2.2 with either CD One, 5th Edition, or CiscoWorks Common Services 2.2.
 - Use DFM 1.2 with CD One, 5th Edition.
- If you are installing DFM with the LMS bundle, follow the installation order specified in the appropriate LMS Read Me First document or Quick Start Guide.
- If you want to use DFM with remote versions of Resource Manager Essentials (Essentials), HP OpenView, or NetView, you must install the appropriate adapters on the remote machines. (CiscoWorks need not be installed on the remote HP OpenView or NetView machines.)
- If you want your devices to forward traps to DFM, make sure you have configured them to do so.
- If another application is using the default listening port for receiving traps, configure the [SNMP Trap Adapter](#) to listen on another port.
- If you want DFM to forward traps, configure the [SNMP Trap Adapter](#) destination port (the recipient machine's server name and port).
- Make sure you have configured other applications to receive traps from DFM on the correct port.
- Make sure DNS is configured on both the server and client sides.

What must I do to get DFM started?

To get DFM started, you must [import some devices](#).

What happens if I exceed the managed device limit?

DFM will perform slowly and you proceed at your own risk.

How can I find out how many devices/objects DFM is currently managing?

Run the following command:

```
# NMSROOT/objects/smarts/bin/sm_tpmgr --server=DFM -sizes
```

Locate the line that is similar to the following:

```
Number of Ports: 761 [92/92]
```

In this example, 761 represents the number of discovered ports, out of which 92 are managed. Unless you have reconfigured DFM to manage access ports, you can assume these 92 ports are trunk ports.

Can DFM coexist with Essentials, Campus Manager, CiscoView, or other Cisco products?

DFM can be installed on the same machine as Resource Manager Essentials (Essentials). Check the LMS bundle requirements to verify whether DFM can be installed with any other LMS bundle products (such as Campus Manager and CiscoView). For more information, see the LMS bundle documentation at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/lms/index.htm. For other Cisco products, check the appropriate product documentation.

What should I do after installing DFM?

- Select **Server Configuration > Administration > Process Management > Process Status** to verify that the following are running:
 - DfmBroker (the [DFM broker](#) process)
 - DfmServer (the [domain manager](#) process)
 - Adapter processes (depending on which adapters you want enabled):
 - DfmChangeProbe (the [RME Adapter](#) process)
 - DfmFileNotifier (the [File Notifier Adapter](#) process)
 - DfmTrapNotifier (the [Trap Notifier Adapter](#) process)
 - DfmMailNotifier (the [Mail Notifier Adapter](#) process)
- Verify that the [DFM broker](#) file has been created:
NMSROOT/objects/smarts/repos/icf/DFM.rps

- Verify that the following log files have been created in *NMSROOT/objects/smarts/logs*:
 - DFM.log (the [domain manager](#) log)
 - brstart.log (the [DFM broker](#) log)
 - DfmChangeProbe.log (if you are using the [RME Adapter](#))
- Watch the notifications and evaluate whether you should:
 - Modify any [thresholds](#)
 - [Unmanage](#) any objects, or vice versa (for example, you might want to unmanage an interface that is not used and is generating AdministrativelyDown alarms so you do not see these alarms)

Process Management

[What are the DFM processes?](#), page F-44

[What processes automatically start when DFM starts?](#), page F-44

[Do the DFM processes rely on any other processes?](#), page F-45

[How do I know if DFM is running properly on a day-to-day basis?](#), page F-45

What are the DFM processes?

All CiscoWorks DFM processes are listed in “[DFM and CiscoWorks Processes](#)” section on page 11-12.

What processes automatically start when DFM starts?

DFM automatically starts the following processes/adapters:

- DfmBroker (the [DFM broker](#) process)
- DfmServer (the [domain manager](#) process)
- DfmChangeProbe (the [RME Adapter](#) process, if Essentials is installed)
- [HPOV-NetView Adapter](#) (if HP OpenView or NetView is installed)
- [SNMP Trap Adapter](#)

If you have enabled the notifier adapters, they will not be restarted when CiscoWorks restarts. You can configure them to do so (see the “[DFM and CiscoWorks Processes](#)” section on page 11-12).

Do the DFM processes rely on any other processes?

Yes. When stopping a process, you must first stop any processes that depend on it. These dependencies are listed in the “[DFM and CiscoWorks Processes](#)” section on page 11-12.

How do I know if DFM is running properly on a day-to-day basis?

DFM will not alert you if it goes down. However, if you have installed the Fault History drop-in (available from Cisco.com at <http://www.cisco.com/cgi-bin/tablebuild.pl/cw-fault-history>), you will be able to see if the DfmServer process has gone down. (In this case, you might want to change your settings for SNMP timeouts and discovery retries.)

