



## Working with the DFM Inventory

---

These topics offer methods for managing your DFM inventory:

- [Adding Devices to the Managed Inventory, page 6-2](#)
- [Saving the DFM Inventory, page 6-6](#)
- [Rediscovering Elements in the DFM Inventory, page 6-6](#)
- [Managing and Unmanaging DFM Inventory Elements, page 6-12](#)
- [Removing Managed Devices from the DFM Inventory, page 6-18](#)
- [Creating a Seed File from a Domain Manager, page 6-19](#)

The DFM inventory consists of all of the elements contained in the repository of a domain manager. This includes devices such as switches, routers, and hosts, and device components such as ports, interfaces, and environmental test points.

Typical inventory-related tasks include:

- Saving the inventory to a file
- Rediscovering elements in the inventory
- Managing or unmanaging inventory elements

All inventory-related operations are performed using the Administration Console, which is described in [Chapter 5, “The DFM Administration Console and Polling and Thresholds Console.”](#)

For information on how DFM assigns names to devices, refer to the [“System Information Probe”](#) section on [page 7-2](#).

# Adding Devices to the Managed Inventory

When a device is added to the managed inventory, DFM performs inventory collection to determine the device's configuration and its relationships to other managed elements. After inventory collection, DFM periodically performs ICMP polls to determine connectivity and performs SNMP polls to collect fault information.

You can use these methods to add devices to the managed inventory:

- [Adding Devices Using the Add Agent Command, page 6-2](#)
- [Adding Devices Using a Seed File, page 6-3](#)
- [Adding Devices from the Resource Manager Essentials Inventory, page 6-4](#)

## Adding Devices Using the Add Agent Command

The Administration Console provides this simple method for adding a single device to the managed inventory. If you change a device's community string, you must also change the device's community string in DFM using either this method or the seed file method (the seed file method is described in [“Adding Devices Using a Seed File”](#) section on page 6-3).



---

**Note**

When you use this method to add a device to the DFM inventory, the inventory information for that device is not available to other CiscoWorks applications through the Essentials database.

---

- 
- Step 1** Click the Add Agent toolbar button or select **Add Agent** from the Inventory menu. This displays the Add Agent dialog box.
- Step 2** Specify the hostname or IP address of the device by entering the hostname or IP address of the device to be managed into the Agent Name field.
- Step 3** If the read community string is not the default, enter it in the corresponding field. DFM uses public as the default read community string.

- Step 4** Click **OK** to add the device. This displays the Discovery Progress dialog.
- Step 5** After DFM discovers the added devices, click the Save Inventory toolbar button to save the updated information.
- 

Repeat this procedure to add additional devices to the inventory.

## Adding Devices Using a Seed File

To add multiple devices to the DFM inventory, you can import a seed file listing the managed devices to initiate inventory discovery. A seed file consists of two columns (separated by spaces or tabs). The first column names the network device, and the second column defines the read community string, as in this example:

```
# Sample seed file
192.168.1.200
access-router-1 private
192.168.2.100 public
host1.example.com.
```

If you change a device's community string, you must also change the device's community string in DFM using either this method or the Add Agent method (the Add Agent method is described in [“Adding Devices Using the Add Agent Command”](#) section on page 6-2)

For additional information on the format of a seed file, including preparing a seed file, refer to *Installation and Setup Guide for Device Fault Manager*. To create a seed file from a running domain manager, refer to the [“Creating a Seed File from a Domain Manager”](#) section on page 6-19.

To import devices from a seed file:

- 
- Step 1** Select **Device Fault Manager > Administration** to open the Administration Console.
  - Step 2** Select **Inventory > Import From Seed File** or click on the Import From Seed File toolbar button. This displays the Import From Seed File dialog box.
  - Step 3** Specify the complete path and the name of the seed file and click **OK**. This displays the Discovery Progress dialog box.




---

**Note** The seed file must be stored on the host where the domain manager runs.

---

When DFM imports devices from the seed file, it probes them to discover their configuration and adds their manageable elements to its inventory. For a large number of elements, this process may take several minutes.

## Adding Devices from the Resource Manager Essentials Inventory

When Resource Manager Essentials 3.4 is installed locally, the DfmChangeProbe process automatically queries the Essentials database that is used by CiscoWorks, and sends device information to the DFM inventory. If a device is added to the Essentials inventory, DFM immediately probes the device to analyze its properties and status, and adds it to the DFM inventory. The log file for this DFM and Essentials synchronization is *NMSROOT/conf/dfm/DfmChangeProbe.log*.

When Resource Managers Essentials 3.x is installed remotely, you must upgrade the RME Adapter on the remote machine so that the adapter can exchange information with DFM on a local host. For more information, see the *Installation and Setup Guide for Device Fault Manager*.




---

**Note** If the synchronization causes DFM to exceed its device limit, the Essentials device list will be truncated. For information on the device limit, see the appropriate *Installation and Setup Guide for Device Fault Manager*.

---

For more information on how the DFM inventory is synchronized with the Essentials inventory, refer to the [“Synchronizing the DFM Inventory with the Essentials Inventory”](#) section on page 6-11.

To disable the DfmChangeProbe process (or re-enable it):

- 
- Step 1** Select **Device Fault Manager > Administration > Device Discovery > Change Probe**. (To re-enable the process, select **Start Process**.)
- Step 2** Highlight the DfmChangeProbe process and click **Stop**.
- 

If you disable the process and reboot your system, the DfmChangeProbe process will be restarted. To disable the process from automatic startup after reboot, unregister the process.

- To unregister the process on Solaris, use this command:

```
# NMSROOT/bin/pdcmcmd -u DfmChangeProbe
```

- To unregister the process on Windows, use this command:

```
# NMSROOT\bin\pdcmcmd.exe -u DfmChangeProbe
```

If you unregistered the process and want to reconfigure to start DfmChangeProbe upon reboot, you must reregister the process.

- To reregister the process on Solaris, use this command (which is one line):

```
# NMSROOT/bin/pdcmcmd -r DfmChangeProbe -d
EssentialsDbEngine,EssentialsDbMonitor -e NMSROOT/bin/cwjava -f
"-Xnoclassgc com.cisco.nm.dfm.changeprobe.DfmChangeProbe"
```

- To reregister the process on Windows, use this command (which is one line):

```
# NMSROOT\bin\pdcmcmd -r DfmChangeProbe.exe -d
EssentialsDbEngine,EssentialsDbMonitor -e NMSROOT\bin\cwjava -f
"-Xnoclassgc com.cisco.nm.dfm.changeprobe.DfmChangeProbe"
```

To query a remote Essentials database, you must use the remote RME Adapter. For information on installing this adapter, refer to *Installation and Setup Guide for Device Fault Manager*.

## Saving the DFM Inventory

DFM automatically saves important inventory information to a file every six hours. In addition to inventory information, DFM also saves information regarding the group and settings applied to the managed elements. If DFM is restarted, it tries to load the saved information from the inventory file.

The inventory file is saved to the *NMSROOT/objects/smarts/repos/icf* directory. The name of the saved inventory file is taken from the name of the domain manager.

To manually save the inventory, do one of the following from the Administration Console (normally, after you select **Reconfigure**):

- Click the Save Inventory toolbar button.
- Select **Inventory > Save Inventory**.

At runtime, the device inventory is stored in memory to enhance performance. DFM saves the inventory data in a file, allowing it to recover the information if the server is rebooted. The data in the inventory file is stored in a non-viewable format.

When you select **Inventory > Reconfigure**, changes are saved to the runtime, in-memory inventory. Changes are saved to the inventory file only when you select **Inventory > Save Inventory**.

## Rediscovering Elements in the DFM Inventory

DFM provides several methods for rediscovering devices. 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.

**Note**

---

If a link or device is slow, DFM may only partially rediscover the device. DFM will not move the device to the Undiscovered class. If you encounter this problem, increase the device polling interval and timeout.

---

DFM can reprobe the managed inventory using these methods:

- [Scheduling Automatic Inventory Collection, page 6-7](#)
- [Performing Manual Inventory Collection, page 6-10](#)
- [Synchronizing the DFM Inventory with the Essentials Inventory, page 6-11](#)

These methods cause a domain manager to reprobe all managed devices or the Essentials inventory to discover any changes. For example, if a card is added to a switch, a probe is necessary for DFM to discover the new card and add it to the inventory.

## Scheduling Automatic Inventory Collection

DFM provides two ways to schedule inventory collection:

- [Using the Rediscovery Schedule, page 6-8](#)
- [Using the Automatic Inventory Collection Check Box, page 6-9](#)

**Note**

---

It is recommended that you use the Rediscovery Schedule instead of the Inventory Collection Check Box.

---

## Using the Rediscovery Schedule

The Rediscovery Schedule option allows you to schedule regular inventory collection by specifying a specific date, time, and duration for the discovery. When you use this selection, the entire inventory is reprobred.

**Note**

---

It is recommended that you use the Rediscovery Schedule instead of the Inventory Collection Check Box.

---

To use the Rediscovery Schedule option:

- 
- Step 1** Select **Administration > Device Discovery > Rediscovery Schedule**.
- Step 2** Enter the desired start date, time, and frequency, and click **OK**.
- 

If the Rediscovery Schedule job is stopped by the CiscoWorks Job Manager, you must remove the job and then repeat the Rediscovery Schedule procedure.

To remove the job:

- 
- Step 1** Select **CiscoWorks Server > Administration > Job Management**.
- Step 2** Select the job and click **Remove Job**.
- 

If you want to reprobe only the devices in the update pending list (versus the entire managed inventory), refer to the [“Using the Automatic Inventory Collection Check Box”](#) section on page 6-9.

## Using the Automatic Inventory Collection Check Box

The Automatic Inventory Collection check box, located in the Administration Console under the Inventory tab of the domain manager's property sheet, allows you to choose the extent to which the inventory is reprobbed, and the interval between reprobes. By default, DFM does not periodically reprobe its inventory.

**Note**

---

It is recommended that you use the Rediscovery Schedule instead of the Inventory Collection Check Box. As a result, you will have to manually rediscover pending devices (described in the following) by selecting **Inventory>Inventory Collection Pending** from the Administration Console.

---

These check boxes let you specify the magnitude of the collection:

- **Short Inventory Collection Interval**—Determines the interval between reprobes of devices in the update pending list. You can schedule intervals in days, hours, minutes, or seconds.

The update pending list consists of devices that are managed but have not yet been rediscovered or probed. For example, when DFM receives a cold start trap (or a warm start trap or module insertion trap), the device that sent the trap is added to the update pending list. Devices that have not yet been probed are referred to as pending.

- **Long Inventory Collection Interval**—Determines the interval between reprobes of the entire managed inventory. You can schedule intervals in days, hours, minutes, or seconds.

**Note**

---

Since a scheduled probe of the inventory updates the Essentials database and directs DFM to update its inventory, it is recommended that the Long Inventory Collection Interval remain disabled.

---

To schedule regular collection of the entire managed inventory starting on a specified date, use the Rediscovery Schedule GUI option as described in the [“Using the Rediscovery Schedule”](#) section on page 6-8.

## Performing Manual Inventory Collection

**Note**

---

If you remove and reattach an element (such as a switch), the element's status will not be updated until the next scheduled inventory collection. You should manually rediscover the element, as described in this section.

---

There are three methods for manually triggering an inventory update from the Administration Console. You would normally do this after selecting **Reconfigure**:

- Select a device in the left panel and select **Inventory > Rediscover**, which forces a domain manager to probe the selected device.
- Select **Inventory > Inventory Collection Pending**, which forces a domain manager to probe elements in the update pending list (not the entire inventory).
- Select **Inventory > Inventory Collect All**, which forces a domain manager to reprobe all managed devices as well as any devices in the update pending list.

After DFM probes the elements, click the Save Inventory toolbar button to save the updated information.

**Note**

---

Unscheduled manual updates to the DFM inventory are local operations. Scheduled updates to the Essentials database, and the synchronization of the DFM inventory with the Essentials database, can erase manual updates.

---

## Synchronizing the DFM Inventory with the Essentials Inventory

When the DfmChangeProbe process is running (which happens regardless of when Essentials is installed), it automatically queries the Essentials database for device information, causing DFM to probe the devices to analyze their properties and status. If a device is added to the Essentials inventory or the community strings on an Essentials device are changed, DFM immediately probes the devices to analyze their properties and status, and adds this information to the DFM inventory. The DFM inventory is not updated with devices deleted from Essentials; these devices must be manually deleted from the DFM inventory.



---

**Note**

If the synchronization causes DFM to exceed its device limit, the Essentials device list will be truncated. For information on the device limit, see the appropriate *Installation and Setup Guide for Device Fault Manager*.

---

The synchronization is allowed with a local version of Resource Manager Essentials 3.4, or a remote version of Resource Manager Essentials 3.x. If you decide you do not want DFM to manage Essentials devices, disable the DfmChangeProbe process.

For information on disabling and re-enabling the process, refer to the [“Adding Devices from the Resource Manager Essentials Inventory”](#) section on page 6-4.

# Managing and Unmanaging DFM Inventory Elements

The term *managed element* refers to an instance of the inventory whose `IsManaged` attribute is set to `TRUE`, meaning that it is monitored by a domain manager. This means that the element is regularly polled to determine its status and connectivity. Conversely, an unmanaged element refers to a member of the topology whose `IsManaged` attribute is set to `FALSE`. Although the DFM inventory contains information about them, unmanaged elements are not polled.

The manage and unmanage operations enable you to control whether a domain manager monitors a particular device or element. It is useful to unmanage a device when, for example, a switch or a card is taken offline for maintenance and you do not want to receive error or performance notifications regarding that device.



## Note

---

If you have downloaded and installed DFM 1.2 Patch/IDU 1.2.9 (or later) you can use Manage or Unmanage from the Polling and Thresholds Console to perform bulk unmanage and manage operations on ports and interfaces (see the “[How to Manage or Unmanage Elements](#)” section on page 6-16). In addition, you can check the new Unmanaged Ports/Interfaces and Unmanaged Systems classes to see which elements are currently unmanaged (see the “[Determining the Managed/Unmanaged Status of an Element](#)” section on page 6-18). DFM 1.2 Patch/IDU 1.2.9 also allows you to disable connectivity polling (ping) for an IP address (or group of IP addresses) without disabling availability polling (SNMP), which will not affect the managed state of the device in the DFM system, as described in the “[Disabling ICMP Polling](#)” section on page 9-2. You can download the latest patch/IDU from the DFM download site: <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>.

---

These topics provide guidelines and procedures for managing and unmanaging inventory elements:

- [Rules Governing Manage and Unmanage Operations](#), page 6-13
- [Listing Managed Ports and Interfaces](#), page 6-14
- [How to Manage or Unmanage Elements](#), page 6-16
- [Determining the Managed/Unmanaged Status of an Element](#), page 6-18

## Rules Governing Manage and Unmanage Operations

You can explicitly set the managed or unmanaged status for the following types of devices or elements:

- Systems such as routers, switches, and hosts
- Logical devices such as processors, interfaces, and ports

The following rules govern the interaction between the managed and unmanaged states of elements:

- A service cannot be managed if it is hosted by or part of an unmanaged system.
- A logical device cannot be managed if it is a part of an unmanaged system.
- If a managed service or logical device is later associated with an unmanaged system, the service or logical device automatically becomes unmanaged.



---

**Note**

Manage and unmanage operations are recursive. For example, if you unmanage a switch, all of the ports and cards that belong to that switch are also unmanaged.

- When a system is managed (unmanaged) all associated services, service access points, components, and physical packages are managed (unmanaged). However, when managing a system, any service or logical device that was explicitly unmanaged remains unmanaged.



---

**Note**

If you manually change a null interface to managed, it will switch back to unmanaged after being rediscovered.

- When a service is managed (unmanaged), all service access points associated with the service are managed (unmanaged).
- When a network adapter is managed (unmanaged), all related service access points are managed (unmanaged).



---

**Note**

DFM allows you to manage ports belonging to a group that has no settings. Although the port can be managed, it will not be polled.

---

## Listing Managed Ports and Interfaces

To find out how many trunk and access ports are currently in the DFM inventory, use the `sm_tpmgr` command:

```
# NMSROOT\objects\smarts\bin\sm_tpmgr.exe --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.



### Note

---

The following script is supported only if you have downloaded and installed DFM 1.2 Patch/IDU 1.2.10 (or later) from the DFM download site: <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>.

---

To list specific ports and interfaces by their types, names, group membership, or managed state, use the `sm_adapter` command in conjunction with the `getNetworkAdapters.asl` script. The syntax is as follows (this command is one line):

```
# NMSROOT\objects\smarts\bin\sm_adapter.exe --server=DFM [-Dargument]  
utils/getNetworkAdapters.asl
```

The arguments to the -D option are described in the following table.

<b>-DNetworkAdapterType=Interface   Port   all</b>		
	List interfaces, ports, or both (all). The default is all.	
<b>-DPortType=ACCESS   TRUNK   all</b>		
	(Ports only.) List access ports, trunk ports, or all ports. The default is all.	
<b>-DGroupName=<i>“device”</i>   CFG-<i>“group/type”</i></b>		
	List ports or interfaces for a specified device, or for a specified DFM trunk port, access port, or interface group. Use the following formats:	
	<i>device</i>	List information for a device, using name or IP address.
	CFG- <i>“group/type”</i>	List information for a port or interface group. <i>group</i> can be Interface Groups, Access Port Groups, or Trunk Port Groups. <i>type</i> can be any subgroup under the port or interface group. For example:  “CFG-Interface Groups/1GB Ethernet”
<b>-DManagedState=managed   unmanaged   all</b>		
	List managed or unmanaged ports or interfaces. The default is managed.	

The following examples show how you can use the `getNetworkAdapters.asl` script.

- To list all managed interfaces and ports:

```
sm_adapter -s DFM utils/getNetworkAdapters.asl
```

- To list all managed and unmanaged ports and interfaces on the lab-gw.cisco.com device:

```
sm_adapter -s DFM -DNetworkAdapterType=all -DPortType=all
-DGroupName="lab-gw.cisco.com" -DManagedState=all
utils/getNetworkAdapters.asl
```

- To list all managed ports and interfaces on the lab-gw.cisco.com device:

```
sm_adapter -s DFM -DGroupName="lab-gw.cisco.com"
utils/getNetworkAdapters.asl
```

- To list all managed interfaces on the lab-gw.cisco.com device:

```
sm_adapter -s DFM -DNetworkAdapterType=Interface
-DGroupName="lab-gw.cisco.com" -DManagedState=managed
utils/getNetworkAdapters.asl
```

- To list all unmanaged interfaces on the lab-gw.cisco.com device:

```
sm_adapter -s DFM -DNetworkAdapterType=Interface
-DGroupName="lab-gw.cisco.com" -DManagedState=unmanaged
utils/getNetworkAdapters.asl
```

- To list all network adapters that belong to the 10/100 Mb Ethernet Trunk Ports group:

```
sm_adapter -s DFM -DNetworkAdapterType=Port -DPortType=TRUNK
-DGroupName="CFG-Port Groups - Trunk Ports/10/100 Mb Ethernet"
-DManagedState=all utils/getNetworkAdapters.asl
```

## How to Manage or Unmanage Elements

Use this procedure to manage or unmanage individual devices and components in DFM.

- 
- Step 1** Right-click on the device or element that you want to manage or unmanage.
  - Step 2** Select **Manage** or **Unmanage** from the pop-up menu.
  - Step 3** Select **Rediscover** from the Inventory menu.
  - Step 4** After DFM discovers the newly managed or unmanaged device, click the Save Inventory toolbar button to save the updated information.
- 

Use this procedure to unmanage all members of a port or interface group.



### Note

The following function is supported only if you have downloaded and installed the latest Incremental Device Update (IDU) from the DFM download site:  
<http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>



---

**Note** The following procedure will unmanage all ports or interfaces in the selected group.

---

- 
- Step 1** From the Polling and Thresholds Console, in the Thresholds tab, select the port or interface group you wish to unmanage (for example, Interface Groups > ATM).
- Step 2** From the Available Settings list, select Disable Interface/Port Analysis.
- Step 3** Click **Add** to make the setting active.
- Step 4** Click **Apply**.
- Step 5** Select **Reconfigure** from the Group menu.
- Step 6** Select **Save Inventory** from the Inventory menu to update the DFM inventory.
- 

You can also selectively create interface and port groups, and unmanage those groups, using the following procedure.



---

**Note** The following function is supported only if you have downloaded and installed DFM 1.2 Patch/IDU 1.2.9 (or later) from the DFM download site: <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>. To disable only ICMP polling (ping) polling on interfaces, refer to the “Disabling ICMP Polling” section on page 9-2.

---

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

## Determining the Managed/Unmanaged Status of an Element

The value of the IsManaged attribute shows the managed status of an element. IsManaged is a Boolean attribute: TRUE when an element is managed and FALSE when the element is unmanaged.

To check the value of an element's IsManaged attribute:

- 
- Step 1** Select the element in the left panel of the Administration Console.
- Step 2** Select the Attributes tab in the right panel of the Administration Console and locate the IsManaged attribute in the Name column. The value of this attribute indicates the managed (unmanaged) status of the element.
- 

If you have downloaded and installed DFM 1.2 Patch/IDU 1.2.9 or later, you can determine which elements are unmanaged from the Polling and Thresholds Console, by selecting the Thresholds tab and viewing the members of the following groups:

- Unmanaged Systems
- Unmanaged Ports/Interfaces
- System Elements

You can download and install Patch/IDU 1.2.9 (or later) from the DFM download site: <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>.

## Removing Managed Devices from the DFM Inventory

Devices can be removed from DFM's inventory through the Administration Console or from any console listing inventory elements. However, since the removal of devices may produce unexpected side effects and incorrect analysis results, it is recommended that you:

- Unmanage devices that are unused but remain in the inventory. See the [“Managing and Unmanaging DFM Inventory Elements”](#) section on page 6-12 for additional information.

- Rediscover the inventory when devices, or one or more of their components, have been physically removed from the inventory, and save the updated information.

**Note**

---

Deleting devices is a local operation. It does not delete devices from the Essentials database. Deleted devices will reappear in the DFM inventory whenever the Essentials collection process probes the Essentials inventory and sends that information to DFM.

---

To remove devices from the DFM inventory:

- 
- Step 1** Right-click on the device to be deleted.
- Step 2** Select **Delete** from the pop-up menu.
- 

## Creating a Seed File from a Domain Manager

You can extract the IP addresses and read community strings of the SNMP agents managed by DFM by using a seed file. This is useful when you want to pass DFM device information to another application.

To extract the list of SNMP agents, use the `sm_tpmgr` command. The Solaris command is:

```
# NMSROOT/objects/smarts/bin/sm_tpmgr -s DFM --dump-agents > seedfile.txt
```

The Windows command is:

```
# NMSROOT\objects\smarts\bin\sm_tpmgr.exe -s DFM --dump-agents > seedfile.txt
```

This command must be executed on the host where the domain manager is running. The resulting text file lists the SNMP agent IP addresses in one column and their corresponding read community strings in a second column.

The `sm_tpmgr` command has the following arguments:

**Table 6-1** *sm\_tpmgr Arguments*

Argument	Description
<code>-s domain_mgr</code>	Specifies the name of the domain manager (DFM).
<code>--dump-agents</code>	Extracts the information regarding the SNMP agents from the domain manager.
<code>&gt; file</code>	Redirects the output to the specified <i>file</i> . If omitted, the output is displayed.
<code>--help</code>	Displays <code>sm_tpmgr help</code> .

For information on adding devices to DFM using seed files, refer to the [“Adding Devices Using a Seed File”](#) section on page 6-3. For additional information on the format of a seed file, including preparing a seed file, refer to *Installation and Setup Guide for Device Fault Manager*.