



Upgrading and Migrating DFM

This chapter describes upgrading and migrating Device Fault Manager (DFM) on a Windows system. It includes:

- [Upgrade and Migration Overview, page 3-1](#)
- [Migrating from DFM 1.2.x to DFM 2.x, page 3-4](#)
- [Performing a Local Migration from DFM 1.2.x to DFM 2.x, page 3-5](#)
- [Post-Upgrade Steps, page 3-18](#)

Upgrade and Migration Overview

This section provides overview information on upgrade and migration process topics:

- [Terminology: Upgrade and Migration, page 3-1](#)
- [Supported DFM Versions for Upgrade and Migration, page 3-2](#)
- [Data that Is Migrated to DFM 2.x, page 3-2](#)

Terminology: Upgrade and Migration

This topic describes the difference between the terms *migration* and *upgrade*.

Migration

Migration is the transfer of data from an older version of DFM to a newer version of DFM. It involves:

1. Backing up the older version of DFM data.
2. Installing the newer version of DFM.
3. Restoring the backed up data.

You can migrate data using either of these two methods:

- Local migration: installing DFM 2.0.3 and DFM 2.0.6 on top of DFM 1.2.x.
- Remote migration: installing DFM 2.0.3 and DFM 2.0.6 on a different machine.

For information on the data that is migrated to DFM 2.0.3, see [Data that Is Migrated to DFM 2.x, page 3-2](#). The migration procedures are provided in [Migrating from DFM 1.2.x to DFM 2.x, page 3-4](#).

Upgrade

Upgrading involves overwriting the existing DFM version with the new DFM version. The data and user settings of the old version are retained in the new version (in other words, the migration of data is automatic). However, for upgrades from DFM 1.2.x, this data migration not automatic; the user must intervene and run a special script, as documented in this guide.

You can upgrade using either of these two methods:

- Local upgrade: installing DFM 2.0.6 on top of DFM 2.0.x on the same machine. You can perform this upgrade using the DFM CD or using LMS 2.5 Update 2 (available from Cisco.com).
- Remote upgrade: installing DFM 2.0.6 on a different machine and then restoring the DFM 2.0.x data on the machine that has DFM 2.0.6.

The upgrade procedures are provided in [Upgrading DFM 2.0.x to DFM 2.0.6, page 3-13](#).

Supported DFM Versions for Upgrade and Migration

You can migrate or upgrade the following versions of DFM to DFM 2.0.6.

Device Fault Manager Version ¹	...Which Came with LAN Management Solution Version...	Reference
DFM 1.2	LMS 2.1	Migrating from DFM 1.2.x to DFM 2.x, page 3-4
DFM 1.2 Updated for Common Services Version 2.2	LMS 2.2	
DFM 2.0 ²	LMS 2.5	Upgrading DFM 2.0.x to DFM 2.0.6, page 3-13
DFM 2.0.3 ³	LMS 2.5.1	Upgrading DFM 2.0.x to DFM 2.0.6, page 3-13

1. Migration/upgrade is also supported when any patch/IDUs or service packs are installed on these versions of DFM.
2. In this scenario, all DFM 2.0.x data is preserved.
3. In this scenario, all DFM 2.0.x data is preserved.

Data that Is Migrated to DFM 2.x

The following data is restored when you perform a migration from DFM 1.2.x:

- Device list—The migration procedure adds devices to Common Services Device and Credentials Repository (DCR) and to DFM.
- Device managed state (managed or unmanaged).
- The following notification information:
 - Mail recipient information
 - Mail sender ID
 - SMTP addresses
 - Trap destination addresses
 - Trap destination ports

- Some polling and threshold settings—See [How Polling Settings Are Affected After Migration and Restoration, page 3-3](#) and [How Threshold Settings Are Affected After Migration and Restoration, page 3-3](#).

No other data is migrated.

How Polling Settings Are Affected After Migration and Restoration

[Table 3-1](#) lists DFM 1.2.x polling groups and settings and those in DFM 2.x that correspond to them. For a device to retain polling settings from DFM 1.2.x, a corresponding polling group (and settings) must exist in DFM 2.x and the device must belong to it.

In DFM 2.x, there are several additional polling groups not listed in [Table 3-1](#) (for more information, see *User Guide for Device Fault Manager*). A device might belong to a new polling group in DFM 2.x. For example, a voice gateway is a member of the Routers polling group in DFM 1.2.x and the Voice and Telephony polling group in DFM 2.x.

After upgrade, DFM 2.0.3 applies factory default settings to:

- Any device that belongs to a different polling group than it did in DFM 1.2.x.
- Any setting that was removed from a polling group in DFM 1.2.x.

The device support table lists the DFM 1.2.x and DFM 2.x groups; refer to [Product Documentation, page x](#).

Table 3-1 Comparison of Polling Groups and Settings between DFM 1.2.x and DFM 2.x

Polling Groups		Polling Settings	
Devices that were members of these groups in DFM 1.2.x...	And become members of these groups in DFM 2.x...	Retain the values from these DFM 1.2.x polling settings... ¹	Reflected in these DFM 2.x polling settings
Optical Switches	Optical Networking	<ul style="list-style-type: none"> • Connectivity Polling • Environment Polling • Performance Polling - Processor and Memory • Performance Polling - Ports and Interfaces (includes access port) 	<ul style="list-style-type: none"> • Reachability settings • Environment • Processor and memory utilization • Connector port and interface • Access port
Switches	Switches and Hubs		
Routers	Routers		
Other Systems	Voice and Telephony	Connectivity Polling	Reachability settings

1. For any polling setting that was removed from a polling group in DFM 1.2.x, DFM 2.0.6 sets its value to the DFM 2.0.6 factory default value.

How Threshold Settings Are Affected After Migration and Restoration

Like polling settings, threshold settings are retained when a device (or device component) is a member of a DFM 2.x threshold group that corresponds to the DFM 1.2.x threshold group it was a member of. [Table 3-2](#) lists the corresponding threshold groups and settings.

There are additional threshold groups in DFM 2.x not listed in [Table 3-2](#) (for more information, see *User Guide for Device Fault Manager*). DFM 2.0.3 applies factory default threshold values to devices that are members of new DFM 2.x threshold groups. The device support table lists the DFM 1.2.x and DFM 2.x groups; refer to [Product Documentation](#), page x.

Table 3-2 Comparison of Threshold Groups and Settings between DFM 1.2.x and DFM 2.x

Threshold Groups		Threshold Settings/Categories	
Devices that were members of these in DFM 1.2.x...	And become members of these groups in DFM 2.x... ¹	Retain the values from these DFM 1.2.x threshold settings... ²	Reflected in these DFM 2.x threshold categories
Interface Groups	Interface Groups	For Interface Groups, Access Port Groups, and Trunk Port Groups, the threshold settings in DFM 1.2.x correspond closely to the threshold categories in DFM 2.x For a list of threshold categories for these groups, see <i>User Guide for Device Fault Manager</i> .	
Access Ports Groups	Access Port Groups		
Trunk Ports Groups	Trunk Port Groups		
Optical Switches	Optical Networking	<ul style="list-style-type: none"> • Connectivity • Environment • Processor and Memory 	<ul style="list-style-type: none"> • Reachability • Environment • Processor and Memory
Routers	Routers		
Switches	Switches and Hubs		

1. Each DFM 2.0 threshold group contains subgroups. This allows you to set threshold settings appropriately for each group of devices.
2. For any threshold setting that was removed from a threshold group in DFM 1.2.x, DFM 2.0 sets its value to the DFM 2.0 factory default value.

Migrating from DFM 1.2.x to DFM 2.x

You can perform a migration from DFM 1.2.x either locally or remotely.

Preparing to Migrate to DFM 2.x

Before you migrate, determine whether you need to gather additional information and media.

If you purchased an upgrade license of DFM 2.0.3 and are migrating from DFM 1.2.x, you are required to validate the upgrade by providing one of the following:

- The original CD containing DFM 1.2 (which shipped with LMS 2.1).
- The original CD containing DFM 1.2 Updated for Common Services Version 2.2 (which shipped with LMS 2.2).
- Login information for a remote server where the previous version of DFM (DFM 1.2.x) is running.



Caution

If validation is not successful, DFM is installed with an evaluation license; access to DFM functionality will be prohibited when the license expires.

You might need to provide the following information during the migration:

- DFM database password and a DFM username and password for use by DFM processes—Only required when you perform a custom installation; otherwise, this information is randomly generated. For more information on creating passwords, see the appendix “Password Information” in *Installation and Setup Guide for Common Services 3.0.3 (Includes CiscoView) on Windows*.
- License information—If you must supply license information, the installation script prompts you to enter one of the following:
 - Information that you will find printed on the software claim certificate—Product Identification Number (PIN) and Product Authorization Key (PAK).
 - Location of the license file—If you have a license file, provide its location. If not, be sure to obtain one. You can do so before or after you install DFM; see [Registering Your License, page A-2](#).



Note You can determine the status of your license from the CiscoWorks home page, by selecting **Common Services > Server > Admin > Licensing**.



Note

If you are installing DFM for evaluation purposes:

- You do not need to supply a license file or PIN and PAK.
- You might be interested in the following information:
 - [Upgrading Your Evaluation License, page A-3](#)
 - [Licensing Reminders, page A-3](#)

Performing a Local Migration from DFM 1.2.x to DFM 2.x

You can migrate to DFM 2.x on a local system as described in this section. [Table 3-3](#) provides an overview of the local upgrade procedure.

Table 3-3 Procedure for Local Migration from DFM 1.2.x to DFM 2.0.3

	Tasks	Reference
Step 1	Back up your data.	This section
Step 2	Install DFM from the CD. (You may have to run the validation script, as documented in this section, to stop the Proof of Purchase nag message.)	
Step 3	Run the restorebackup.pl script to migrate your data.	
Step 4	Perform post-migration steps to complete basic configuration of DFM 2.x.	Post-Upgrade Steps, page 3-18

Follow these steps to migrate a local DFM 1.2.x host to DFM 2.x. If you are installing DFM 2.x on a clean machine (onto which you will migrate your DFM data), use the installation instructions in [Performing a New Installation, page 2-4](#).



Note Device import can take up to 3 hours, depending on the number of devices in your inventory.

- Step 1** Make sure your system meets the following prerequisites:
- Required (or desired) operating system upgrades have been performed, and required service packs are installed.
 - All installed applications are supported by CiscoWorks Common Services 3.0.3. If you have not upgraded to Common Services 3.0.3, DFM 1.2.x links will be disabled.
 - Common Services 3.0.3 has been installed. (See *Installation and Setup Guide for Common Services 3.0.3 (Includes CiscoView) on Windows*.)
 - If you want a locally installed NMS to send traps to DFM, HP OpenView or NetView has been installed. See [Supported NMS Integration, page 1-8](#).
- Step 2** Make sure you have the data described in [Preparing to Migrate to DFM 2.x, page 3-4](#).
- Step 3** Back up your DFM data by selecting **Server Configuration > Administration > Database Management > Back Up Data Now**. Click **Help**, and follow the instructions to back up your information.
- Step 4** As the local administrator, log on to the system on which you will upgrade DFM, and insert the DFM CD-ROM into the CD-ROM drive. The installer window appears, asking you if you want to install DFM.



Note If the CD-ROM is already in the CD-ROM drive and you stopped the installation process to close programs or if Autostart is disabled, click **Setup.exe** to restart the process.

The Welcome window appears.

- Step 5** Click **Next**. The Software License Agreement dialog box appears.
- The installation program stops CiscoWorks, performs a requirements check, and might display a request to enter license information; for more information, see [Appendix A, “Licensing.”](#)
- Step 6** In the Setup Type dialog box, select **Typical** to install the complete DFM package, which contains DFM and the HPOV-NetView adapters. (For more information on installation components, refer to [Table 1-1 on page 1-1](#).)



Note The HPOV-NetView adapters are installed whether or not HP Openview or NetView is installed.

Click **Next**. A Warning dialog box appears, advising you that when you install DFM, new tasks will be registered with ACS. If you have already registered DFM with ACS from another server, you do not need to register. However, if you do re-register DFM, you will lose any custom DFM roles that you created earlier in ACS.

- Step 7** Do one of the following:
- If you want to register (or re-register) DFM with the ACS server, click **Yes**. DFM will be registered with the ACS server.
 - If you do not want to register with the ACS server, click **No**. (You will be prompted to register later.)

- If you want to abort the installation, click **Cancel**.

The System Requirements dialog box displays the results of the requirements check and advises whether the installation can continue. One of the following should then occur:

- If there is not enough disk space for the installation, the installation program displays an error message and stops.



Note Do not be alarmed if you see the following message:

```
INFO: total size (MB) required = 87
```

This message applies to disk space required by the current set of individual packages being installed.

- If the minimum recommended requirements are not met, the installation program displays an error message and continues installing.

Step 8 The Select Components dialog box appears with the Install Device Fault Manager 2.0.3 radio button selected. Click **Next**.

Step 9 The Summary dialog box appears, displaying the current settings. Click **Next**.

Depending upon your configuration, you maybe reminded to run the restorebackup.pl script. The upgrade program performs the following actions:

- Copies the files to the CiscoWorks default installation directory *NMSROOT*.
- Exports data (see [Data that Is Migrated to DFM 2.x, page 3-2](#)).

Step 10 Click **OK**. The system prompt appears.

Step 11 If you did not register DFM with the ACS server in [Step 7](#), and you want to register now, use the AcsRegCli.pl script, as follows. (*NMSROOT* is the default installation directory, normally C:\Progra~1\CSCOpX.)

```
NMSROOT\bin\perl NMSROOT\bin\AcsRegCli.pl -register dfm
```

Step 12 Eject the CD-ROM.



Note Store the CD-ROM in a secure, climate-controlled area for safekeeping.

Step 13 Upgrade to DFM 2.0.6 by installing the LMS 2.6 Update on Windows (see [Installing the LMS 2.6 Update on Windows, page 2-6](#)).

Step 14 If you receive a nag message asking for your Proof of Purchase, run the validation script to stop the message (*NMSROOT* is the CiscoWorks installation directory, normally C:\Progra~1\CSCOpX). You will not be prompted to enter any information.

```
NMSROOT\bin\dfmValidateUpgrade.bat
```

Step 15 Restore your DFM data using restorebackup.pl:



Note Make sure you have backed up the latest DFM data, as described in [Step 3](#).



Note If you are installing DFM with other LAN Management Solution components, perform this step after all components are installed. Refer to the *Quick Start Guide for LAN Management Solution 2.5.1* for more information.

- a. Stop the daemon manager:

```
net stop crmdmgt
```

- b. Run the script:

```
NMSROOT\bin\perl NMSROOT\bin\restorebackup.pl -d backup_location -gen version
-t tempbackup_dir
```

where *NMSROOT* is the CiscoWorks installation directory, normally C:\Progra~1\CSCOpX.

Example:

```
C:\Progra~1\CSCOpX\bin\perl C:\Progra~1\CSCOpX\bin\restorebackup.pl
-d C:\Progra~1\CSCOpX\backup -t C:\tmp
```

where:

- C:\Progra~1\CSCOpX is the CiscoWorks installation directory.
- C:\Progra~1\CSCOpX\backup is the backup location you specified in [Step 3](#). This is mandatory.
- C:\tmp is a temporary location into which the backup files are extracted. These files are used by the restore backup script. This is optional and will be deleted after the data migration is complete. By default, the restore backup script uses C:\Progra~1\CSCOpX\tempbackupdata directory.

You can optionally include **-gen version** to specify a backup version to be migrated to DFM 2.x. By default, it will restore the latest backup data.

Depending upon your configuration, you may be prompted to give your approval when migration begins, and you may also be reminded to check for updates on Cisco.com. The script imports the seedfile into the DCR, imports the devices into DFM, and restores all of the data described in [Data that Is Migrated to DFM 2.x, page 3-2](#).



Note Device import can take up to 3 hours, depending on the number of devices in your inventory.

- c. Restart the daemon manager:

```
net start crmdmgt
```

Step 16 To check the status of device discovery and to complete your configuration of DFM, see [Post-Upgrade Steps, page 3-18](#).

If you had any errors, check *NMSROOT\log\restorebackup.log*. The Cisco Technical Assistance Center (TAC) might ask you to send them this log.

Performing a Remote Migration from DFM 1.2.x to DFM 2.x

Table 3-4 provides an overview of the remote migration when migrating DFM 1.2.x to DFM 2.x.

Table 3-4 Procedure for Remote Migration from DFM 1.2.x to DFM 2.0.3

	Tasks	Reference
Step 1	Install DFM 2.x on the remote host.	Performing a New Installation, page 2-4
Step 2	Validate the installation on the remote DFM 2.x host.	Validating the Installation on the Remote DFM 2.x Host, page 3-9
Step 3	Back up your data on the DFM 1.2.x host.	Backing Up Your Data on the Local DFM 1.2.x Host, page 3-10
Step 4	Run the DFMMigrate.pl script, assemble your DFM 1.2.x migration files, and copy the migration files onto the DFM 2.x host.	Generating Your DFM 1.2.x Migration Files from Your Local DFM 1.2.x Host, page 3-10
Step 5	Run the restorebackup.pl script on the DFM 2.x host to restore your data.	Restoring Your DFM Data on the Remote DFM 2.x Host, page 3-12
Step 6	Perform post-migration steps to complete basic configuration of DFM 2.x.	Post-Upgrade Steps, page 3-18

Installing DFM 2.x on the Remote Host

Install DFM 2.x on your remote host, as described in [Performing a New Installation, page 2-4](#). You will be reminded to run the restorebackup.pl script, which is described in [Restoring Your DFM Data on the Remote DFM 2.x Host, page 3-12](#). (Depending upon your configuration, you may also be reminded to check for updates on Cisco.com.)

Validating the Installation on the Remote DFM 2.x Host

If you have not done so already, validate the installation on the system where DFM 2.x is installed using the following commands:

```
NMSROOT\bin\dfmValidateUpgrade.bat
```

where *NMSROOT* is the default installation directory, normally C:\Progra~1\CSCOpX. The following prompt is displayed:

```
This utility will validate your proof of purchase of the product and allows you to obtain an upgrade license.
```

```
Please select the source for upgrade validation:
```

1. Validate from a CD (old version).
2. Validate from a remote server (old version).

```
Please enter option [1 / 2]:
```

Enter 1 or 2 and follow the instructions provided by the prompts. For example, if you enter 1:

```
Please insert the previous versions of DFM CD into the CDROM drive and provide the absolute path to the CD drive:
```

```
D:
```

```
Validation succeeded.
```

For example, if you enter 2:

```
Please enter the remote CiscoWorks server host name or the IP address: dfm-host
Please enter the remote CiscoWorks server http port number: 1741
Please enter the remote CiscoWorks server login name: admin
Please enter the remote CiscoWorks server login password: *****
Please be patient. Upgrade validation is in progress from a remote server.
Validation succeeded.
```



Note

If validation does not succeed, you can continue with the upgrade, however:

- DFM is licensed for evaluation only and operates in *nag* mode for no more than 90 days before ceasing operation. (See [Evaluation Version: Before Expiry, page A-3.](#))
- You must contact your Cisco representative to purchase a fully licensed version of DFM. (See [Upgrading Your Evaluation License, page A-3.](#))

Backing Up Your Data on the Local DFM 1.2.x Host

On the local DFM 1.2.x host, back up your DFM data using Common Services.

-
- Step 1** From the Common Services home page, select **Server Configuration > Administration > Database Management > Back Up Data Now**.
- Step 2** In the Back Up Data Now dialog box, enter the path and name for the backup directory.
- Step 3** Click **Finish** to start the backup.
-

By default, the information will be placed in the *NMSROOT*\backup directory.

Generating Your DFM 1.2.x Migration Files from Your Local DFM 1.2.x Host

This procedure explains how to generate and collect the files required by DFM 2.x so you can migrate your data from your local DFM 1.2.x host to your remote DFM 2.x host, and then restore the migrated data on the DFM 2.0.3 host. In this procedure you will do the following:

- Use the DFMMigrate.pl script to create files that contain the device list and device management state information, and the polling and threshold information.
- Optionally, copy the Mail Notifier Adapter and Trap Notifier Adapter files so you can migrate the adapter configurations.

-
- Step 1** Copy the DFM Upgrade Kit to your local DFM 1.2.x host. The Upgrade Kit contains the DFMMigrate.pl script and other required files. Use one of the following methods:
- Copy the Upgrade Kit to a temporary directory from the following location in the remote DFM 2.0.3 installation. *NMSROOT* is the remote DFM 2.0.3 installation directory (normally C:\Progra~1\CSCOpX).
- ```
NMSROOT\bin\cw-dfm-20-UpgradeKit-win.zip
```

- Download the Upgrade Kit by logging in to Cisco.com and going to <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>. Extract the kit as described in the Readme file located on the download site.

**Step 2** Locate your copy of the 1.2.x DFM.rps file:

- In a DFM 1.2.x installation, the DFM.rps file is normally located in *NMSROOT*\objects\smarts\repos\icf\DFM.rps (where *NMSROOT* is the CiscoWorks installation directory, normally C:\Progra~1\CSCOpX).
- For a backup copy, the file will be located in the backup directory you specified when you backed up the file using CiscoWorks Common Services.

**Step 3** Make sure the DFM.rps file is named **DFM.rps**, otherwise **Step 4** will fail.

**Step 4** Use the DFMMigrate.pl script to create the required migration files.

- Move to the directory into which you copied the cw-dfm-20UpgradeKit-win.zip file in **Step 1**.
- Unzip the file. It will create a directory called cw-dfm-20-UpgradeKit-win.
- Move to the cw-dfm-20-UpgradeKit-win\smarts directory, which contains the migration script.
- Run the DFMMigrate.pl script:



**Caution**

Be sure to run DFMMigrate.pl from the cw-dfm-20-UpgradeKit-win\smarts directory; the script requires files that are relative to that directory.

```
NMSROOT\bin\perl DFMMigrate.pl -n NMSROOT -o DFM.rps_directory
```

The command variables are as follows:

|                          |                                                                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>NMSROOT</i>           | CiscoWorks installation directory (normally C:\Progra~1\CSCOpX).                                                                                                     |
| <i>DFM.rps_directory</i> | Full pathname of directory containing DFM 1.2.x DFM.rps file. For DFM 1.2.x installations, this file is located in <i>NMSROOT</i> \objects\smarts\repos\icf\DFM.rps. |

For example (the following command is one line):

```
C:\Progra~1\CSCOpX\bin\perl DFMMigrate.pl -n C:\Progra~1\CSCOpX -o C:\tmp
```

This creates the necessary DFM 1.2.x migration text files (ICseed.txt, ICinventory.txt, and ICptm.xml) and places them in *NMSROOT*\cw-dfm-20-UpgradeKit-win\smarts\conf.

**Step 5** Copy the following migration files from your local DFM 1.2.x host to the corresponding directory on the remote DFM 2.x host:

- Copy the three files in *NMSROOT*\cw-dfm-20-UpgradeKit-win\smarts\conf\ to the following location on the DFM 2.x host:  
*NMSROOT*\objects\smarts\conf
- Optionally, copy the Mail Notifier and Trap Notifier Adapter files from the following location on the DFM 1.2.x host:

*NMSROOT*\objects\smarts\conf\notifier\mail\_notify.conf and  
*NMSROOT*\objects\smarts\conf\notifier\trap\_notify.conf

to the following location on the DFM 2.x host:

*NMSROOT*\objects\smarts\conf\notifier

- Copy the DFM 1.2.x backup files (from [Backing Up Your Data on the Local DFM 1.2.x Host, page 3-10](#)) to a safe location on the DFM 2.x host.

## Restoring Your DFM Data on the Remote DFM 2.x Host



### Note

When restoring your data, device import can take up to 3 hours, depending on the number of devices in your inventory.

**Step 1** On the remote DFM 2.x host, confirm that you have properly copied the files described in [Step 5 of Generating Your DFM 1.2.x Migration Files from Your Local DFM 1.2.x Host, page 3-10](#).

**Step 2** Restore your DFM data using `restorebackup.pl`.

- Stop the daemon manager:

```
net stop crmdmgttd
```

- Run the script:

```
NMSROOT\bin\perl NMSROOT\bin\restorebackup.pl -d backup_location -gen version
-t tempbackup_dir
```

where *NMSROOT* is the default installation directory, normally `C:\Progra~1\CSCOpX`.

Example:

```
C:\Progra~1\CSCOpX\bin\perl C:\Progra~1\CSCOpX\bin\restorebackup.pl
-d C:\Progra~1\CSCOpX\backup -t C:\tmp
```

where:

- `C:\Progra~1\CSCOpX` is the CiscoWorks installation directory.
- `C:\Progra~1\CSCOpX\backup` is the location into which you copied your backup files in [Step 5 of Generating Your DFM 1.2.x Migration Files from Your Local DFM 1.2.x Host, page 3-10](#). This is mandatory.
- `C:\tmp` is a temporary location into which the backup files are extracted. These files are used by the restore backup script. This is optional and will be deleted after the data migration is complete. By default, the restore backup script uses `C:\Progra~1\CSCOpX\tempbackupdata` directory.

You can optionally include `-gen version` to specify a backup version to be migrated to DFM 2.0.3. By default, it will restore the latest backup data.

The migration script imports the seedfile into the DCR, imports the devices into DFM, and migrates all of the data described in [Data that Is Migrated to DFM 2.x, page 3-2](#).



### Note

Device import can take up to 3 hours, depending on the number of devices in your inventory.

- Restart the daemon manager:

```
net start crmdmgttd
```

- Step 3** To check the status of device discovery and to complete your configuration of DFM, see [Post-Upgrade Steps, page 3-18](#).
- 

If you had any errors, check `NMSROOT\log\restorebackup.log`. The Cisco Technical Assistance Center (TAC) might ask you to send them this log.

## Upgrading DFM 2.0.x to DFM 2.0.6

You can perform an upgrade either locally or remotely, as described in these topics.

### Preparing to Upgrade to DFM 2.0.6

Before you migrate, determine whether you need to gather additional information and media.

You might need to provide the following information during the migration:

- DFM database password and a DFM username and password for use by DFM processes—Only required when you perform a custom installation; otherwise, this information is randomly generated. For more information on creating passwords, see the appendix “Password Information” in *Installation and Setup Guide for Common Services 3.0.5 (Includes CiscoView) on Windows*.
- License information—If you must supply license information, the installation script prompts you to enter one of the following:
  - Information that you will find printed on the software claim certificate—Product Identification Number (PIN) and Product Authorization Key (PAK).
  - Location of the license file—If you have a license file, provide its location. If not, be sure to obtain one. You can do so before or after you install DFM; see [Registering Your License, page A-2](#).



---

**Note** You can determine the status of your license from the CiscoWorks home page, by selecting **Common Services > Server > Admin > Licensing**.

---



**Note** If you are installing DFM for evaluation purposes:

- You do not need to supply a license file or PIN and PAK.
  - You might be interested in the following information:
    - [Upgrading Your Evaluation License, page A-3](#)
    - [Licensing Reminders, page A-3](#)
-

## Performing a Local Upgrade from DFM 2.0.x to DFM 2.0.6

You can upgrade to DFM 2.0.6 on a local system as described in this section. [Table 3-5](#) provides an overview of the local upgrade procedure.

**Table 3-5 Procedure for Local Migration from DFM 2.0.x to DFM 2.0.6**

|        | Tasks                                                                      | Reference                                     |
|--------|----------------------------------------------------------------------------|-----------------------------------------------|
| Step 1 | Back up your data.                                                         | This section                                  |
| Step 2 | Install DFM from the CD.                                                   |                                               |
| Step 3 | Perform post-migration steps to complete basic configuration of DFM 2.0.6. | <a href="#">Post-Upgrade Steps, page 3-18</a> |

Follow these steps to migrate a local DFM 2.0.x host to DFM 2.0.6. If you are installing DFM 2.0.6 on a clean machine (onto which you will migrate your DFM data), use the installation instructions in [Performing a New Installation, page 2-4](#).



### Note

If you have DFM 2.0.3 (supplied with LMS 2.5.1), install the LMS 2.5 Update 2 by downloading it from Cisco.com, and installing it..

If you have DFM 2.0 (which came with LMS 2.5), install the LMS 2.5 December 2005 Update, and then install the LMS 2.5 Update 2.

You can download the required software from Cisco.com, <http://www.cisco.com/kobayashi/sw-center/cw2000/lan-planner.shtml>.



### Note

Device import can take up to 3 hours, depending on the number of devices in your inventory.

- Step 1** Make sure your system meets the following prerequisites:
- Required (or desired) operating system upgrades have been performed, and required service packs are installed.
  - All installed applications are supported by CiscoWorks Common Services 3.0.3. If you have not upgraded to Common Services 3.0.5, DFM 2.0.x links will remain enabled, but Common Services will issue a warning message.
  - Common Services 3.0.5 has been installed. (See *Installation and Setup Guide for Common Services 3.0.5 (Includes CiscoView) on Windows*.)
  - If you want a locally installed NMS to send traps to DFM, HP OpenView or NetView has been installed. See [Supported NMS Integration, page 1-8](#).
- Step 2** Make sure you have the data described in [Preparing to Migrate to DFM 2.x, page 3-4](#).
- Step 3** Back up your DFM data by selecting **Server Configuration > Administration > Database Management > Back Up Data Now**. Click **Help**, and follow the instructions to back up your information.

- Step 4** As the local administrator, log on to the system on which you will migrate DFM, and insert the DFM CD-ROM into the CD-ROM drive. The installer window appears, asking you if you want to install DFM.



---

**Note** If the CD-ROM is already in the CD-ROM drive and you stopped the installation process to close programs or if Autostart is disabled, click **Setup.exe** to restart the process.

---

The Welcome window appears.

- Step 5** Click **Next**. The Software License Agreement dialog box appears.

The installation program stops CiscoWorks, performs a requirements check, and might display a request to enter license information; for more information, see [Appendix A, “Licensing.”](#)

- Step 6** In the Setup Type dialog box, select **Typical** to install the complete DFM package, which contains DFM and the HPOV-NetView adapters. (For more information on installation components, refer to [Table 1-1 on page 1-1.](#))



---

**Note** The HPOV-NetView adapters are installed whether or not HP Openview or NetView is installed.

---

- Step 7** Click **Next**. The installation program checks dependencies and system requirements.

- Step 8** The System Requirements dialog box displays the results of the requirements check and advises whether the installation can continue. One of the following should then occur:

The installation program checks dependencies and system requirements:

- If there is not enough disk space for the installation, the installation program displays an error message and stops.



---

**Note** Do not be alarmed if you see the following message:

```
INFO: total size (MB) required = 87
```

This message applies to disk space required by the current set of individual packages being installed.

---

- If the minimum recommended requirements are not met, the installation program displays an error message and continues installing.

- Step 9** The Select Components dialog box appears with the Install Device Fault Manager 2.0.6 radio button selected. Click **Next**.

- Step 10** The Summary dialog box appears, displaying the current settings. Click **Next**.

Depending upon your configuration, you may be reminded to check for updates on Cisco.com. The upgrade proceeds without displaying any more questions. The upgrade program performs the following actions:

- Copies the files to the CiscoWorks default installation directory *NMSROOT*.
- Exports data (see [Data that Is Migrated to DFM 2.x, page 3-2](#)).

- Step 11** Click **OK**. The system prompt appears.

Step 12 Unmount and eject the CD-ROM.



**Note** Store the CD-ROM in a secure, climate-controlled area for safekeeping.

If you had any errors, check `NMSROOT\log\restorebackup.log`. The Cisco Technical Assistance Center (TAC) might ask you to send them this log.

## Performing a Remote Upgrade from DFM 2.0.x to DFM 2.0.6

[Table 3-6](#) provides an overview of the remote upgrade procedure when upgrading DFM 2.0.x to DFM 2.0.6.

**Table 3-6 Procedure for Remote Upgrade from DFM 2.0.x to DFM 2.0.6**

|        | Tasks                                                                                    | Reference                                                                       |
|--------|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Step 1 | Install DFM 2.0.6 on the remote system.                                                  | <a href="#">Performing a New Installation, page 2-4</a>                         |
| Step 2 | Back up your DFM 2.0.x data on the local host.                                           | <a href="#">Backing Up Your DFM 2.0.x Data, page 3-16</a>                       |
| Step 3 | Copy the backup files from your local DFM 2.0.x host to the remote DFM 2.0.6 host.       | <a href="#">Copy the Backup Files from Your Local DFM 2.0.x Host, page 3-17</a> |
| Step 4 | Run the <code>restorebackup.pl</code> script on the DFM 2.0.6 host to restore your data. | <a href="#">Restoring the DFM Data on Your Remote DFM 2.0.6 Host, page 3-17</a> |
| Step 5 | Perform post-upgrade steps to complete basic configuration of DFM 2.0.6.                 | <a href="#">Post-Upgrade Steps, page 3-18</a>                                   |

### Installing DFM 2.0.6 on the Remote Host

Install DFM 2.0.6 on your remote host, as described in [Performing a New Installation, page 2-4](#). (Depending upon your configuration, you may be reminded to check for updates on Cisco.com.)

### Backing Up Your DFM 2.0.x Data

On the local DFM 2.0.x host, back up your DFM data using Common Services.

- 
- Step 1 From the Common Services home page, select **Server > Admin > Backup**.
  - Step 2 In the Backup dialog box, enter the path and name for the backup directory.
  - Step 3 Click **Finish** to start the backup.
- 

By default, the information will be placed in the `NMSROOT\backup` directory.

## Copy the Backup Files from Your Local DFM 2.0.x Host

- 
- Step 1** On your local DFM 2.0.x host, locate the files you backed up in [Backing Up Your DFM 2.0.x Data, page 3-16](#).
- Step 2** Copy the backup files from your local DFM 2.0.x host to a safe location on the remote DFM 2.0.6 host.
- 

## Restoring the DFM Data on Your Remote DFM 2.0.6 Host



**Note** When migrating your data, device import can take up to 3 hours, depending on the number of devices in your inventory.

---

- Step 1** On your upgraded DFM 2.0.6 host, restore your DFM data using `restorebackup.pl`.

- a. Stop the daemon manager:

```
net stop crmdmgt
```

- b. Run the script:

```
NMSROOT\bin\perl NMSROOT\bin\restorebackup.pl -d backup_location -gen version
-t tempbackup_dir
```

where *NMSROOT* is the default installation directory, normally `C:\Progra~1\CSCOpX`.

Example:

```
C:\Progra~1\CSCOpX\bin\perl C:\Progra~1\CSCOpX\bin\restorebackup.pl
-d C:\Progra~1\CSCOpX\backup -t C:\tmp
```

where:

- `C:\Progra~1\CSCOpX` is the CiscoWorks installation directory.
- `C:\Progra~1\CSCOpX\backup` is the location into which you copied your backup files in [Backing Up Your DFM 2.0.x Data, page 3-16](#). This is mandatory.
- `C:\tmp` is a temporary location into which the backup files are extracted. These files are used by the restore backup script. This is optional and will be deleted after the data migration is complete. By default, the restore backup script uses `C:\Progra~1\CSCOpX\tempbackupdata` directory.

You can optionally include `-gen version` to specify a backup version to be migrated to DFM 2.0.6. By default, it will restore the latest backup data. Depending upon your configuration, you may be reminded to check for updates on Cisco.com.

The migration script imports the seedfile into the DCR, imports the devices into DFM, and migrates all of the data described in [Data that Is Migrated to DFM 2.x, page 3-2](#).



**Note** Device import can take up to 3 hours, depending on the number of devices in your inventory.

---

- c. Restart the daemon manager:

```
net start crmdmgt
```

- Step 2** To check the status of device discovery and to complete your configuration of DFM, see [Post-Upgrade Steps, page 3-18](#).
- 

If you had any errors, check the upgrade log, `NMSROOT\log\restorebackup.log`. The Cisco Technical Assistance Center (TAC) might ask you to send them this log.

## Post-Upgrade Steps

After the upgrade script completes, DFM discovers devices and updates its managed inventory. DFM might take some time to complete this task. Afterward, you should do the following:

- Reconfigure the Rediscovery Schedule (which is not migrated during an upgrade); select **Configuration > Other Configurations > Rediscovery Schedule**.
- Reconfigure SNMP trap forwarding (which is not migrated during an upgrade); see [Updating the SNMP Trap Receiving Port, page 4-11](#).
- Familiarize yourself with new device management procedures; see [Performing Device Management, page 4-6](#).
- Verify discovery status; see [Verifying Devices Added to DFM, page 4-7](#).
- Perform SNMP trap configuration tasks; see [Configuring SNMP Trap Receiving and Forwarding, page 4-10](#).
- Start using DFM to monitor the network; see [Viewing Alerts, page 4-14](#) and [What Next?, page 4-15](#).

If you plan to use HPOV-NetView adapters on a remote system, with Device Fault Manager 2.0.6 on a local system, perform these steps:

1. Make sure the system running DFM is registered with DNS.
2. Upgrade all remote adapters as described in [Installing and Upgrading HPOV-NetView Adapters, page 2-13](#).



### Note

If you install another NMS—such as Cisco Voice Manager—*after* installing DFM, you must:

1. Configure DFM to forward traps to the listening port for the NMS. See [Configuring SNMP Trap Forwarding, page 4-14](#).
2. Make sure the NMS is configured to receive traps at the port you specified in Step 1. Refer to the appropriate documentation for the NMS.

If a local version of HP OpenView or NetView is already installed (or is installed later), CiscoWorks automatically configures the adapters to forward SNMP traps to DFM. To configure remote versions of HP OpenView and NetView to forward SNMP traps to DFM, you must install the HPOV-NetView adapters on the remote systems as described in [Installing and Upgrading HPOV-NetView Adapters, page 2-13](#).

---