Installation and Setup Guide for Device Fault Manager 2.0.3 on Windows

CiscoWorks

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7817163=
Text Part Number: 78-17163-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Installation and Setup Guide for Device Fault Manager 2.0.3 on Windows

IBM Runtime for AIX
The Software contains the IBM Runtime Environment for AIX(R), Java™ 2 Technology Edition Runtime Modules © Copyright IBM Corporation 1999, 2000 All Rights Reserved.

HP-UX Runtime Environment for the Java™ 2 Platform
The Software contains the HP-UX Runtime for the Java™ 2 Platform, distributed pursuant to and governed by Hewlett-Packard Co. ("HP") software license terms set forth in detail at: http://www.hp.com. Please check the Software to determine the version of Java runtime distributed to you.

DataDirect Technologies
Portions of this software are copyrighted by DataDirect Technologies, 1991-2002.

NetBSD
Copyright © 2001 Christopher G. Demetriou. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   This product includes software developed for the NetBSD Project. See http://www.netbsd.org/ for information about NetBSD.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. <<Id: LICENSE, v 1.2 2000/06/14 15:57:33 cgd Exp>>

RSA Data Security, Inc.
Copyright © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved. License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind. These notices must be retained in any copies of any part of this documentation and/or software.

AES
Copyright © 2003, Dr Brian Gladman <brg@gladman.me.uk>, Worcester, UK. All rights reserved.

License Terms:

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

Disclaimer: This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose. Issue Date: 26/08/2003

CONTENTS

Preface

This guide describes Device Fault Manager (DFM), provides instructions for installing DFM on a Windows system, and offers quick-start steps on the use of DFM.

Audience

This document is for anyone who installs and initially uses DFM.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** `font`
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font

Item	Convention
Selecting a menu item in paragraphs	**Option > Network Preferences**
Selecting a menu item in tables	Option > Network Preferences

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Product Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 describes the product documentation that is available.

Table 1 Product Documentation

Document Title	Available Formats
Release Notes for Device Fault Manager 2.0.3 on Windows	• Printed document that was included with the product. • On Cisco.com at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm203/rel_note/index.htm
Installation and Setup Guide for Device Fault Manager 2.0.3 on Windows	• PDF on the product CD-ROM. • On Cisco.com at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm203/install/windows/index.htm • Printed document available by order (part number DOC-7817162=).[1]
User Guide for Device Fault Manager (Software Release 2.0.3)	• PDF on the product CD-ROM. • On Cisco.com at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm203/ug/index.htm • Printed document available by order (part number DOC-7817161=).[1]
Supported Device Table for DFM 2.0.3	• On Cisco.com at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dev_sup/index.htm
Status of DFM Device Agent Bugs (DFM 1.x and DFM 2.x)	On Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dev_sup/dfm_agnt.htm
Context-sensitive online help	• Select an option, then click **Help**.

1. See Obtaining Documentation, page 17.

Related Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 2 describes the additional documentation that is available.

Table 2 Related Documentation

Document Title	Available Formats
Quick Start Guide for LAN Management Solution 2.5.1	• Printed document that was included with the product. • On Cisco.com at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/lms/index.htm
Data Migration Guide for LAN Management Solution 2.5.1	• Printed document that was included with the product. • On Cisco.com at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/lms/index.htm
Release Notes for CiscoWorks Common Services 3.0 (Includes CiscoView 6.1) on Windows	• Printed document that was included with the product. • On Cisco.com at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/cs303/index.htm

Table 2 Related Documentation (continued)

Document Title	Available Formats
Installation and Setup Guide for Common Services 3.0.3 (Includes CiscoView) on Windows	• PDF on the product CD-ROM. • On Cisco.com at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/cs303/index.htm • Printed document available by order (part number DOC-7817184=).[1]
User Guide for CiscoWorks Common Services 3.0.3	• PDF on the product CD-ROM. • On Cisco.com at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/cs303/index.htm • Printed document available by order (part number DOC-7817182=).[1]

1. See Obtaining Documentation, page 17.

Additional Information Online

Note We have adopted a new system for naming and numbering our patch/IDUs. For all releases after DFM 2.0 Patch/IDU 2.0.1, we will use the following conventions: *Patch/IDU* will be called *Service Pack*, and instead of version *x.y.z*, it will be called version *z*. For example, instead of DFM 2.0 Patch/IDU 2.0.2, a release would be called DFM 2.0 Service Pack 2.

Incremental Device Updates (IDUs) or service packs provide additional support for Cisco devices that were not supported when Device Fault Manager was released. When a new IDU/service pack is available, you can download it in one of the following ways:

- From Cisco.com:
  1. Log into Cisco.com at the following URL:

     http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm.
  2. Follow instructions online for downloading the IDU/service pack and the accompanying Readme.
- From the CiscoWorks home page:
  1. From the CiscoWorks home page, select **Common Services > Software Center > Software Update**. The Software Updates window opens.
  2. See *User Guide for CiscoWorks Common Services* for how to configure and use Software Center.

Note You cannot download DFM IDUs/service packs using the Device Update or Scheduled Device Download option from the Software Center.

IDUs/service packs are cumulative; that is, new IDUs/service packs contain the contents of any previous IDUs/service packs. To determine which version of an IDU/service pack is installed on your CiscoWorks Server:

1. In the CiscoWorks window, select **Common Services > Software Center > Software Update**. The Software Updates window opens.
2. Click **Device Fault Manager** in the Products Installed table. The Details of the Applications, Packages installed window opens.
3. Check the version of DFMI in the Packages Installed table.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco

service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended

solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions.

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Prerequisites

This chapter describes the prerequisites for installing Device Fault Manager (DFM) on a Windows system. It includes:

Product Overview

Device Fault Manager is a network management and analytical tool that enables you to monitor your network devices and determine the cause of device problems. Table 1-1 describes installation options that are displayed under different circumstances and lists the DFM components that can be installed in each case.

Table 1-1 DFM Installation Options and Their Components

Installation Option	Installation Option Components
Device Fault Manager 2.0.3	This option installs the entire DFM product on the local system, including: • DFM—Provides the graphical user interface (GUI) and back-end processes for DFM. • HPOV-NetView adapters for integrating DFM with HP OpenView and NetView, if already installed on the same box.
Device Fault Manager HPOV-NetView adapters	This option installs only the HPOV-NetView adapters, not the entire DFM product. This option is normally chosen to install the adapters on a remote machine running HP OpenView or NetView, to forward traps from these remote network management systems (NMSs) to a local DFM. For information on how to configure and start these adapters, see Installing and Upgrading HPOV-NetView Adapters, page 2-13.

Installation, Upgrade, and Migration Paths

This section outlines the steps for installing, upgrading, and migrating to DFM 2.0.3

Installation Paths

You must install DFM 2.0.3 on a system with CiscoWorks Common Services 3.0.3. You can install DFM 2.0.3 on a system with:

- CiscoWorks only (as a "standalone" DFM)
- Common Services and any of the following:
  - Other CiscoWorks applications, such as Campus Manager and Resource Manager Essentials (RME) that are included in a Cisco product bundle.

    Note If you are installing DFM with contents of the LAN Management Solution, check the installation order as described in the quick start guide (see Related Documentation, page 14).

  - Another NMS, such as NetView or HP OpenView (see Supported NMS Integration, page 1-11).

Before you install DFM, you should determine whether you will install DFM as a standalone or with other products. For more information, see Server Requirements and Recommendations, page 1-6.

Table 1-2 lists the basic installation sequence.

Table 1-2 Installation Roadmap

	Description	References
Step 1	Install Common Services 3.0.3.	*Installation and Setup Guide for Common Services 3.0.3 (Includes CiscoView) on Windows*
Step 2	If you want to install DFM on a system with an NMS (HP OpenView or NetView), install the NMS. **Note** If the desired NMS is not installed before DFM, you will have to reinstall DFM later.	• For supported versions of NMSs, see Supported NMS Integration, page 1-11 • For installation instructions, see vendor documentation
Step 3	If you want to install DFM on a system with the contents of the LAN Management Solution: **a.** Check the quick start guide for the order of installation. **b.** Install any products that should be installed before DFM.	*Quick Start Guide for LAN Management Solution 2.5.1*
Step 4	If HP OpenView or NetView is installed on a remote system *and* you want DFM to receive SNMP traps from one of them, install or upgrade the HPOV-NetView adapters on the remote system.	Installing and Upgrading HPOV-NetView Adapters, page 2-13

Upgrade/Migration Paths

You may upgrade DFM 2.0.3 on a system with Common Services 3.0.3. You can perform a local in-place upgrade from DFM 1.2.*x* or a remote upgrade. (For more information, see Chapter 3, "Upgrading and Migrating DFM.")

Table 1-3 lists the basic upgrade/migration sequence.

Note The specific upgrade sequence may vary depending on whether you are doing a local or remote upgrade, and whether you are upgrading from DFM 1.2.*x* or DFM 2.0.*x*.

Table 1-3 Upgrade/Migration Roadmap

	Description	References
Step 1	Upgrade your operating system, if required or desired.	Vendor documentation.
Step 2	Upgrade Common Services.	*Installation and Setup Guide for Common Services 3.0.3 (Includes CiscoView) on Windows*
Step 3	If you want to upgrade DFM on a system with an NMS (HP OpenView or NetView), do one of the following: • If the NMS is already installed, determine whether to upgrade it and do so if required. • Install the NMS. **Note** If the NMS is not installed before DFM, you will have to reinstall DFM later.	• For supported versions of NMSs, see Supported NMS Integration, page 1-11 • For installation instructions, see vendor documentation
Step 4	If you want to upgrade DFM on a system with the contents of the LAN Management Solution: **a.** Check the quick start guide for the order of installation. **b.** Install any products that should be installed before DFM.	*Quick Start Guide for LAN Management Solution 2.5.1 (Maintenance Kit)*
Step 5	If HP OpenView or NetView is installed on a remote system *and* you want DFM to receive SNMP traps from one of them, install or upgrade the HPOV-NetView adapters on the remote system.	Installing and Upgrading HPOV-NetView Adapters, page 2-13

Server Requirements and Recommendations

This section describes the server requirements and recommendations for Common Services and DFM 2.0.3.

Note If you are installing DFM with the contents of the LAN Management Solution, the server requirements might be different. See the quick start guide for the appropriate bundle for additional information.

Minimum Server Requirements

The minimum system requirements for a CiscoWorks Server running Common Services 3.0.3 and Device Fault Manager 2.0.3 are shown in Table 1-4.

Table 1-4 Server System Minimum Requirements

Requirement Type	Minimum Requirements
System hardware	• IBM PC-compatible dual CPU system with 1.6 GHz or faster Pentium processor. • 17-inch color monitor. • CD-ROM drive.
System software	• ODBC Driver Manager[1] 3.5.10. • One of the following: – Windows Server 2003 Standard and Enterprise Editions with Service Pack 1. – Windows 2000 (Professional, Server, and Advanced Server) with Service Pack 4.[2] **Note** Windows terminal services is supported in remote administration mode only. **Note** DFM supports only US-English and Japanese language versions. Set the default locale to US-English for the US-English version and Japanese for the Japanese version.

Table 1-4 Server System Minimum Requirements (continued)

Requirement Type	Minimum Requirements
Available memory (RAM)	2 GB.
Available drive space	• 4 GB. The default installation directory is C:\Program Files\CSCOpx. • Swap space equal to double the amount of memory (RAM). For example, if your system has 2 GB of RAM, you need 4 GB of swap space. **Note** NTFS file system required for secure operation.
Additional required software	Common Services must be installed before you install DFM. For installation instructions, see *Installation and Setup Guide for Common Services (Includes CiscoView) on Windows*.
Additional optional software	To use the desktop on the server system, you need one of the following browsers: • Microsoft Internet Explorer 6.0 (build 6.0.2900.2180) with Service Pack 1. • Netscape Navigator 7.1. • Mozilla 1.7.1.

1. To verify the version of ODBC Driver Manager, from the Windows desktop, select **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**. Select the About tab. If necessary, install Microsoft Data Access Component (MDAC) 2.5 or later.
2. If you are using a Windows 2000 server, disable Hyper-Threading Technology (HTT). See http://www.intel.com/support/processors/sb/CS-017343.htm.

Server Recommendations

To select or configure a server system that best meets your needs, consider the number of ports and interfaces being managed. (For the maximum number of ports and interfaces, see Number of Ports/Interfaces that DFM Supports, page 1-12.)

Note If you choose to automatically synchronize DFM device inventory with the Common Services Device and Credentials Repository (DCR) and the synchronization causes DFM to exceed the limits, DFM stops adding devices to the managed inventory. (See Supported NMS Environments for Device Import, page 1-10.)

To find out how many trunk and access ports and interfaces are currently imported into DFM, use the sm_tpmgr command:

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

You will be prompted for a username (admin) and password (XXXXX). For ports, 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.

For interfaces, locate the line that is similar to the following:

```
Number of Interfaces: 351 [322/280]
```

In this example, 351 represents the number of discovered interfaces, out of which 322 are managed.

Client Requirements

The minimum system requirements for the CiscoWorks client are shown in Table 1-5.

Before you access DFM from a client system, you must configure the system. For more information about client system requirements and configuring clients, see *Installation and Setup Guide for Common Services (Includes CiscoView) on Windows.*

Table 1-5 Client System Requirements Summary

Requirement Type	Minimum Requirements
System hardware and software	One of the following client systems: • IBM PC-compatible system with at least a 1-GHz Pentium processor running: – Windows 2000 Professional, Server, and Advanced Server Service Pack 4[1] – Windows XP with Service Pack 2 – Windows Server 2003 Standard or Enterprise Edition with Service Pack 1, without terminal services • Sun SPARC Ultra 10 running Solaris 8 (Solaris 2.8) or Solaris 9 (Solaris 2.9) **Note** DFM supports only US-English and Japanese versions of Windows Operating System (OS) and Solaris OS. Set the default locale to US-English for the US-English OS, and Japanese for the Japanese OS. Color monitor with video card set to 24 bits color depth
Available memory (RAM)	512 MB

Table 1-5 Client System Requirements Summary (continued)

Requirement Type	Minimum Requirements
Available disk apace	1 GB swap space. **Note** Swap space should be equal to twice the amount of RAM.
Browser	One of these browsers: • On Windows clients: – Microsoft Internet Explorer 6.0 (build 6.0.2900.2180) with Service Pack 1 – Netscape Navigator 7.1 and 7.2 for Windows – Mozilla 1.7.1 • On Solaris clients: – Netscape Navigator 7.0 – Mozilla 1.7 and 1.7.5 For Solaris, use Netscape Navigator downloaded from the Sun website only.

1. To verify the existing service pack, from the Start menu, select **Run** and enter **`winver`**.

Supported NMS Environments for Device Import

DFM device inventory is taken from the Common Services Device and Credentials Repository (DCR). DCR is a common repository of devices, their attributes, and credentials. It is the central place where users add or import new devices.

DCR enables you to share devices lists with other applications as follows:

Using DCR, you can import devices from:

- A local network management system (NMS)—Common Services supports import from NetView and HP OpenView. For supported versions, see Supported NMS Integration, page 1-11.
- A remote NMS—The same NMSs supported locally are supported remotely.
- A file—File can be exported from another product and formatted for import to DCR.

By default, DFM is configured to automatically synchronize its device list with DCR. If the synchronization causes the DFM system to exceed its limit, the device and credentials list will be truncated. (See Number of Ports/Interfaces that DFM Supports, page 1-12.) Alternatively, you can configure DFM to allow only manual selection of devices in DCR that you want DFM to manage. When you do so, DFM displays a list of devices in DCR, but not in DFM, for you to choose from. For more information, see the *User Guide for Device Fault Manager 2.0.3*.

Supported NMS Integration

DFM supports integration with network management systems (NMSs) as follows:

- DFM listens for traps from managed devices on port 162 (the default). If another NMS on the system with DFM uses port 162, DFM uses port 9000 (and the installation script warns you that this is the case).
- DFM forwards traps to destinations that you specify, as follows:
  - To forward pass-through traps, see Configuring SNMP Trap Receiving and Forwarding, page 4-13.
  - To forward processed traps, see "Managing SNMP Trap Notifications" in the "Using Notification Services" chapter of *User Guide for Device Fault Manager*.

  For more information on pass-through and processed traps, see the appendix "Processed and Pass-through Traps, and Other Unidentified Traps and Events" in *User Guide for Device Fault Manager*.
- DFM provides the HPOV-NetView adapters, which forwards traps (sent from managed devices to the NMS) to DFM from remote or local hosts running:
  - HP OpenView 6.4 and 7.0.1
  - NetView 7.1 and 7.1.4

  Installing these adapters on remote machines is described in Installing and Upgrading HPOV-NetView Adapters, page 2-13.

Note To use the HPOV-NetView adapters with a local version of HP OpenView or NetView, make sure that HP OpenView or NetView is installed before you install DFM.

Supported Devices

Device adapter packages for all supported devices are installed when you install DFM. Information about devices installed with DFM can be found at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/DFM/dev_sup/index.htm

For information on how device support compares between DFM 1.2.*x* and DFM 2.0.3, see *Release Notes for Device Fault Manager 2.0.3* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm20/rel_note/index.htm.

As additional device adapter packages become available, you can download the IDUs that contain them, by logging into Cisco.com at:

http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-DFM

Number of Ports/Interfaces that DFM Supports

DFM supports configurations of up to 45,000 ports/interfaces, of which 6,750 (or 15%) are managed. This support was tested with an average of 30 ports/interfaces per device.

If you have an unrestricted license, DFM stops adding devices to its managed inventory when the supported number of ports/interfaces on the devices is reached.

If you have a restricted license, however, DFM stops adding devices to its managed inventory after the number of devices in managed inventory equals or surpasses the number of devices specified by the license. DFM displays licensing reminders as the number of devices nears the limit; see Restricted Version: Device Limit Exceeded, page A-6.

Installing and Uninstalling DFM

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

Preparing to Install DFM

The sections that follow help you to perform the following tasks before you install DFM:

- Determine whether your existing applications are already using ports that DFM uses; see Verifying TCP and UDP Ports that DFM Uses, page 2-2. (Existing applications should not use the ports that DFM uses.)
- Gather information that you might need to provide during the DFM installation; see Gathering Information to Provide During Installation, page 2-3.

Verifying TCP and UDP Ports that DFM Uses

Before installing DFM, make sure that the ports DFM uses will be used only by applications listed in Table 2-1. For a complete list of ports used by Common Services and other LAN Management Solution (LMS) applications, see the *Quick Start Guide for LAN Management Solution 2.5.1* on Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/lms/lms25/index.htm.

DFM uses the following TCP and UDP ports.

Table 2-1 DFM Ports

Protocol	Port Number	Service Name	Direction (of establishment) of Connection
ICMP	—	Ping	Server to Device
UDP	161	Simple Network Management Protocol (SNMP)	Server to Device, Device to Server
	162	SNMP Traps (Standard Port)—Default port number used by DFM for receiving traps	Server to Device, Device to Server
	9000	Used for trap receiving (if port 162 is occupied)	Client to Server
	9002	Used by DFM broker	Client to Server
TCP	49	TACACS+ and ACS	Server to ACS
	8888	Used by log server	Server internal
	15000	Used by log server	Server internal
	43445	Used by Fault History database engine (dfmFH)	Server internal
	43446	Used by inventory service database engine (DFMInv)	Server internal
	43447	Used by event processing database engine (dfmEPM)	Server internal
	43500-43520	Used by DFM CSTM (Common Services Transport Mechanism) for internal application messaging	Server internal

Gathering Information to Provide During Installation

You might need to supply the following information while you are installing DFM:

- 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 already obtained a license file, provide the path. If not, be sure to obtain one. You can do so before or after you install DFM; see Registering Your License, page A-3.

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 a PIN and a PAK.
- You might be interested in the following information:
  - Upgrading Your Evaluation License, page A-4
  - Licensing Reminders, page A-5

Performing a New Installation

Use these steps to perform a fresh installation of DFM.

Step 1 Make sure your system meets these prerequisites:

- Required (or desired) operating system upgrades have been performed.
- Common Services 3.0.3 has been installed. (See *Installation and Setup Guide for CiscoWorks 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 1-11.
- If HP OpenView is installed and operational, you have stopped all HP OpenView services (if not, the installation will take significantly longer).

Step 2 Close all open or active programs. Do not run other programs during the installation process.

Step 3 As the local administrator, log in to the machine on which you will install the DFM software, 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 4 In the Software License Agreement dialog box, click **Yes** to accept the license.

Step 5 If the Licensing Information dialog box appears, select a radio button and enter any required information.

Note For instructions on obtaining a license file or locating the PIN and PAK, see Preparing to Install DFM, page 2-1.

Step 6 Click **Next**. The Setup Type dialog box appears.

Step 7 Select **Typical** to install the complete DFM package, which contains DFM, the DFM IDU base package, and the HPOV-NetView adapters.

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

Note If you choose the *Typical* installation mode, DFM passwords (for user and database) will be randomly generated for you; you can view the passwords at the end of the installation. If you choose the *Custom* installation mode, you will be prompted to enter DFM passwords for user and database.

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 8 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 might 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.

The Summary dialog box appears, displaying the current settings.

Step 9 Click **Next**. The installation program copies the files to the CiscoWorks default installation directory *NMSROOT*.

Step 10 Depending upon your configuration, you may need to do the following:

- If you purchased an upgrade license of DFM 2.0.3 (because you were formerly using DFM 1.2.*x*), the following warning message is displayed when the installation completes:

  ```
  Please run the program
  C:\PROGRA~1\CSCOpx\bin\dfmValidateUpgrade.bat to validate that
  this is an upgrade.
  ```

  If you see this message, you must run this program after the installation completes (see Step 14). Click **OK**. The Setup Complete dialog box appears.

- If you did not register DFM with the ACS server in Step 8, 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 11 Eject the CD-ROM.

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

Step 12 Specify the clients that are allowed to connect to the DFM server. (DFM provides this fine-grain control as an additional security feature.)

a. Unregister the daemons with the daemon manager:

- For DfmServer:

```
# NMSROOT\bin\pdcmd -u DfmServer
```

- For DfmBroker:

```
# NMSROOT\bin\pdcmd -u DfmBroker
```

b. Decide which hosts you want to specify, using the --accept option with arguments shown in Table 2-2.

Table 2-2 Arguments to the --accept Option

Argument	Description
host1,*host2*,...	Allow only *host1*,*host2*,... to connect to the server. If the hostname is registered with DNS, you can specify the client by hostname. Otherwise, specify explicit IP addresses in a comma-separated list. Hostnames are resolved to one or more IP addresses, which are then used (the server does not use reverse lookups to determine the name of a connecting host). **Note** If you specify the clients as hostnames, be sure the hostnames are registered with DNS, especially if you are using DHCP.
=any	Allow all incoming connections (default).

For example, this command fragment would allow connections only from hosts lucy and ethel:

```
--accept=lucy,ethel
```

Note To allow connections from processes running on the same host, specify the host's name—do not use "localhost." This is because connections made using the DFM Broker will appear to come from the DFM Broker's host. Only connections that explicitly specify "localhost" as the target address will appear to come from localhost. Such target addresses might result in configurations that forward incoming connections (such as through software that provides an encrypted tunnel).

c. Re-register the daemons with the daemon manager, specifying the clients that can connect to the broker and server (in this example, the DFM broker port is 9002, and lucy and ethel are the clients):

- For DfmBroker (the following command is one line):

```
# NMSROOT\bin\pdcmd -r DfmBroker -e NMSROOT\objects\smarts\bin\brstart -f "--output
--port=9002 --accept=lucy,ethel --restore=NMSROOT\objects\smarts\conf\broker.rps"
```

- For DFMServer (the following command is one line):

```
# NMSROOT\bin\pdcmd -r DfmServer -e NMSROOT\objects\smarts\bin\sm_server -d DfmBroker -f
"--bootstrap=DFM_bootstrap.conf --accept=lucy,ethel --output --name=DFM"
```

d. Make sure that the client names and current IP addresses are registered with DNS if one or both of the following apply:

- You are running DHCP
- You specified the clients with hostnames

Step 13 To verify that the DfmServer process is running, log in to the CiscoWorks home page as the administrator and select **Common Services > Server > Admin > Processes**.

Step 14 If you purchased an upgrade license of DFM 2.0.3 (because you were formerly using DFM 1.2.*x*), and were prompted to validate the upgrade in Step 10, run the following command:

*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-5.)
- You must contact your Cisco representative to purchase a fully licensed version of DFM. (See Upgrading Your Evaluation License, page A-4.)

Step 15 If you plan to use the HPOV-NetView adapters with Device Fault Manager 2.0.3, make sure the machine running DFM is registered with DNS.

Step 16 To use DFM, select **Device Fault Manager** from the CiscoWorks home page. A Device Fault Manager window opens.

If you had any errors during installation, check the installation log in the root directory on the drive. (For example, the CiscoWorks CD One installation might create C:\Ciscoworks_setup001.log, the DFM installation might create C:\Ciscoworks_setup002.log, and so forth.) The Cisco Technical Assistance Center (TAC) might ask you to send them the installation log.

If you install HP OpenView or NetView later, you will have to either configure DFM SNMP trap receiving to use another port (as described in Configuring SNMP Trap Receiving and Forwarding, page 4-13), or reinstall DFM.

To integrate DFM with remote versions of HP OpenView and NetView, you must install the HPOV-NetView adapters as described in Installing and Upgrading HPOV-NetView Adapters, page 2-13.

Reinstalling DFM

You can use this procedure to reinstall DFM or to reinstall the HPOV-NetView adapters.

Step 1 If HP OpenView is installed and operational, make sure it has been stopped (or the installation will take significantly longer).

Step 2 Close all open or active programs. Do not run other programs during the reinstallation process.

Step 3 As the local administrator, log in to the machine on which you will install the DFM software, and insert the DFM CD-ROM into the CD-ROM drive. The installer window appears, asking you if you want to reinstall DFM.

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

Step 4 Click **Install**. The Welcome window appears.

Step 5 In the Setup Type dialog box, select **Custom** to select the components to reinstall. The Select Components dialog box appears.

The system displays these options (the choices may vary, depending on your configuration):

```
Reinstall Device Fault Manager 2.0.3
Reinstall HPOV-NetView adapters
```

Select the component you want to reinstall and click **Next**. The Start Copying Files window appears.

Step 6 Click **Next**.

Step 7 If you reinstalled *only* the HPOV-NetView adapters, you are prompted to enter the name of the machine running DFM. Enter the name of the host (the default is localhost).

Note Make sure the machine running DFM is registered with DNS.

The System Requirements dialog box displays the results of the requirements check and advises whether the reinstallation can continue. One of the following might 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.

The Summary dialog box appears, displaying the current settings.

Step 8 Click **Next**. The reinstallation proceeds.

Step 9 Remove the DFM CD-ROM from the drive.

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

Step 10 Reboot the machine.

Step 11 To verify that the DfmServer process is running, log in to the CiscoWorks home page as the administrator and select **Common Services > Server > Admin >Processes**.

Step 12 To use DFM, select **Device Fault Manager** from the CiscoWorks navigation tree.

If you had any errors during reinstallation, check the installation log in the root directory on the drive. (For example, the CiscoWorks CD One installation might create C:\Ciscoworks_setup001.log, the DFM installation might create C:\Ciscoworks_setup002.log, and so forth.) The Cisco Technical Assistance Center (TAC) might ask you to send them the installation log.

Uninstalling DFM

Caution You must use the CiscoWorks uninstallation program to remove DFM from your system. If you try to remove the files and programs manually, you can seriously damage your system.

Step 1 As the local administrator, log in to the system on which DFM is installed, and select **Start > Programs > CiscoWorks > Uninstall CiscoWorks** to start the uninstallation process.

A dialog box appears, listing the components selected for uninstallation.

Step 2 Click **Next.**

Messages showing the progress of the uninstallation appear.

The following message appears:

```
Uninstallation is complete. Click OK to finish.
```

Step 3 Click **OK**.

Installing and Upgrading HPOV-NetView Adapters

When you install DFM on a system with HP OpenView or NetView, the DFM installation script installs the HPOV-NetView adapters. These adapters take the traps that managed devices send to HP OpenView (or NetView) and forward them to DFM. For information on supported HP OpenView and NetView versions, see Supported NMS Integration, page 1-11.

This section explains how to install or upgrade the HPOV-NetView adapters on a remote host on which Common Services is installed, so the adapters can exchange information with DFM on a local host. You can also use these procedures to reinstall the HPOV-NetView adapters.

If you upgrade a local version of DFM, you must also upgrade any remote adapters.

Note To upgrade remote HPOV-NetView adapters, you must first remove the old adapters and then install the new version.

Note If you move DFM to a different machine, or you want to use a different instance of DFM, you must reinstall the HPOV-NetView adapters.

Reinstalling the HPOV-NetView Adapters on a Local Host

If you install NetView or HP OpenView on the local host *after* you have installed DFM, you should reinstall the HPOV-NetView adapters to configure them appropriately. See Reinstalling DFM, page 2-10.

Installing or Upgrading the HPOV-NetView Adapter on a Remote Host

Step 1 To upgrade a previous version of the HPOV-NetView adapters, remove the adapters as described in Uninstalling the HPOV-NetView Adapters, page 2-15.

Step 2 Make sure the following are installed on the remote host:

- HP OpenView or NetView
- Common Services 3.0.3

Step 3 As the local administrator, log in to the machine on which you will install the HPOV-NetView adapters, and insert the DFM CD-ROM into the CD-ROM drive. The installer window appears, asking you if you want to install DFM.

Note Be sure to install the adapter on the same drive as HP OpenView or NetView.

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 4 Click **Next**. The Setup Type dialog box appears.

Step 5 Select **Custom** to select a component to install and click **Next**. The Select Components dialog box appears.

Step 6 Select **Device Fault Manager HPOV-NetView adapters** and click **Next**.

Step 7 When prompted, enter the machine name or IP address of the machine on which DFM is running.

Note Do not use the default, localhost. Also, make sure the machine running DFM is registered with DNS.

Step 8 Click **Next**. HP OpenView and NetView are stopped. The System Requirements dialog box displays the results of the requirements check and advises whether installation can continue.

Step 9 Click **OK**. The installation program copies the files to the directory in which Common Services was installed.

Step 10 Remove the DFM CD-ROM from the drive.

Step 11 Click **OK** to reboot the machine.

Step 12 Restart HP OpenView or NetView to activate the adapters (using the **ovstart** or **nvstart** command).

If you had any errors during installation (or upgrade), check the installation log in the root directory on the drive. (For example, the Common Services installation might create C:\Ciscoworks_setup001.log, the DFM installation might create C:\Ciscoworks_setup002.log, and so forth.) The Cisco Technical Assistance Center (TAC) might ask you to send them the installation log.

Uninstalling the HPOV-NetView Adapters

When you remove a local version of DFM, the HPOV-NetView adapters are also removed. To remove remote adapters, follow the instructions in this section.

Caution You must use the CiscoWorks uninstallation program to remove the adapters from your system. If you try to remove the files and programs manually, you can seriously damage your system.

Step 1 As the local administrator, log in to the system on which the remote HPOV-NetView adapters are installed, and select **Start > Programs > CiscoWorks > Uninstall CiscoWorks** to start the uninstallation process. The Uninstall window appears, displaying a list of the installed applications.

Step 2 Deselect everything except **Device Fault Manager HPOV-NetView adapters**.

Step 3 Click **Next**. A dialog box listing the components selected for removal appears.

Step 4 Click **Next** to begin removing the HPOV-NetView adapters. Messages showing the progress of the uninstallation appear, and the uninstallation completes.

Step 5 Click **OK**.

If you had any errors during uninstallation, check the installation log in the root directory on the drive. (For example, the CiscoWorks CD One installation might create C:\Ciscoworks_setup001.log, the DFM installation might create C:\Ciscoworks_setup002.log, and so forth.) The Cisco Technical Assistance Center (TAC) might ask you to send them the installation log.

Upgrading and Migrating DFM

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

Upgrade and Migration Overview

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

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

For information on the data that is migrated to DFM 2.0.3, see Data that Is Migrated to DFM 2.0.3, page 3-3. The migration procedures are provided in Migrating from DFM 1.2.x to DFM 2.0.3, page 3-6.

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 2.0.3 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 2.0.3 on a different machine and then restoring the DFM 2.0.*x* data on the machine that has DFM 2.0.3.

The upgrade procedures are provided in Upgrading DFM 2.0.x to DFM 2.0.3, page 3-19.

Supported DFM Versions for Upgrade and Migration

You can migrate or upgrade the following versions of DFM to DFM 2.0.3.

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 2.0.3, page 3-6
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 2.0.3, page 3-19

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.

Data that Is Migrated to DFM 2.0.3

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 3-4 and How Threshold Settings Are Affected After Migration and Restoration, page 3-5.

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 2.0.3 and the device must belong to it.

In DFM 2.0.3, 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 2.0.3. 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 2.0.3.

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 12.

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	• Connectivity Polling • Environment Polling • Performance Polling - Processor and Memory • Performance Polling - Ports and Interfaces (includes access port)	• 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 2.0.3 sets its value to the DFM 2.0.3 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 2.0.3 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 2.0.3 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 2.0.3 threshold groups. The device support table lists the DFM 1.2.*x* and DFM 2.0.3 groups; refer to Product Documentation, page 12.

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

<table>
<tr><th colspan="2">Threshold Groups</th><th colspan="2">Threshold Settings/Categories</th></tr>
<tr><th>Devices that were members of these in DFM 1.2.x...</th><th>And become members of these groups in DFM 2.x...[1]</th><th>Retain the values from these DFM 1.2.x threshold settings...[2]</th><th>Reflected in these DFM 2.x threshold categories</th></tr>
<tr><td>Interface Groups</td><td>Interface Groups</td><td colspan="2" rowspan="3">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 User Guide for Device Fault Manager.</td></tr>
<tr><td>Access Ports Groups</td><td>Access Port Groups</td></tr>
<tr><td>Trunk Ports Groups</td><td>Trunk Port Groups</td></tr>
<tr><td>Optical Switches</td><td>Optical Networking</td><td rowspan="3">• Connectivity
• Environment
• Processor and Memory</td><td rowspan="3">• Reachability
• Environment
• Processor and Memory</td></tr>
<tr><td>Routers</td><td>Routers</td></tr>
<tr><td>Switches</td><td>Switches and Hubs</td></tr>
</table>

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 2.0.3

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

Preparing to Migrate to DFM 2.0.3

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-3.

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-4
  - Licensing Reminders, page A-5

Performing a Local Migration from DFM 1.2.*x* to DFM 2.0.3

You can migrate to DFM 2.0.3 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 2.0.3.	Post-Upgrade Steps, page 3-26

Follow these steps to migrate a local DFM 1.2.*x* host to DFM 2.0.3. If you are installing DFM 2.0.3 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 1-11.

Step 2 Make sure you have the data described in Preparing to Migrate to DFM 2.0.3, page 3-6.

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 1-2.)

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 2.0.3, page 3-3).

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

Step 11 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 12 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 13 Eject the CD-ROM.

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

Step 14 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 crmdmgtd
```

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 inStep 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 2.0.3. 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 2.0.3, page 3-3.

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 crmdmgtd
```

Step 15 To check the status of device discovery and to complete your configuration of DFM, see Post-Upgrade Steps, page 3-26.

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 2.0.3

Table 3-4 provides an overview of the remote migration when migrating DFM 1.2.*x* to DFM 2.0.3.

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

	Tasks	Reference
Step 1	Install DFM 2.0.3 on the remote host.	Performing a New Installation, page 2-4
Step 2	Validate the installation on the remote DFM 2.0.3 host.	Validating the Installation on the Remote DFM 2.0.3 Host, page 3-13
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 3-14
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 3-15

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

	Tasks	Reference
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 2.0.3 Host, page 3-17
Step 6	Perform post-migration steps to complete basic configuration of DFM 2.0.3.	Post-Upgrade Steps, page 3-26

Installing DFM 2.0.3 on the Remote Host

Install DFM 2.0.3 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 2.0.3 Host, page 3-17. (Depending upon your configuration, you may also be reminded to check for updates on Cisco.com.)

Validating the Installation on the Remote DFM 2.0.3 Host

Validate the installation on the system where DFM 2.0.3 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-5.)
- You must contact your Cisco representative to purchase a fully licensed version of DFM. (See Upgrading Your Evaluation License, page A-4.)

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 2.0.3 so you can migrate your data from your local DFM 1.2.*x* host to your remote DFM 2.0.3 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 2.0.3 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.

a. Move to the directory into which you copied the cw-dfm-20UpgradeKit-win.zip file in Step 1.

b. Unzip the file. It will create a directory called cw-dfm-20-UpgradeKit-win.

c. Move to the cw-dfm-20-UpgradeKit-win\smarts directory, which contains the migration script.

d. 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:

NMSROOT	CiscoWorks installation directory (normally C:\Progra~1\CSCOpx).
DFM.rps_directory	Full pathname of directory containing DFM 1.2.*x* DFM.rps file. For DFM 1.2.*x* installations, this file is located in *NMSROOT*\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 files from your local DFM 1.2.*x* host to the corresponding directory on the remote DFM 2.0.3 host:

- Copy the three files in *NMSROOT*\cw-dfm-20-UpgradeKit-win\smarts\conf\ to the following location on the DFM 2.0.3 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 2.0.3 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 3-14) to a safe location on the DFM 2.0.3 host.

Restoring Your DFM Data on the Remote DFM 2.0.3 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 2.0.3 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 3-15.

Step 2 Restore your DFM data using restorebackup.pl.

a. Stop the daemon manager:

```
net stop crmdmgtd
```

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 Step 5 of Generating Your DFM 1.2.x Migration Files from Your Local DFM 1.2.x Host, page 3-15. 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 2.0.3, page 3-3.

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 crmdmgtd
```

Step 3 To check the status of device discovery and to complete your configuration of DFM, see Post-Upgrade Steps, page 3-26.

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 2.0.3

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

Preparing to Upgrade to DFM 2.0.3

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 3.0.3 (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-3.

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-4
  - Licensing Reminders, page A-5

Performing a Local Upgrade from DFM 2.0.x to DFM 2.0.3

You can upgrade to DFM 2.0.3 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 2.0.3

	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 2.0.3.	Post-Upgrade Steps, page 3-26

Follow these steps to migrate a local DFM 2.0.x host to DFM 2.0.3. If you are installing DFM 2.0.3 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 2.0.*x* links will remain enabled, but Common Services will issue a warning message.
- 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 1-11.

Step 2 Make sure you have the data described in Preparing to Migrate to DFM 2.0.3, page 3-6.

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 1-2.)

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 2.0.3 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 2.0.3, page 3-3).

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 2.0.3

Table 3-6 provides an overview of the remote upgrade procedure when upgrading DFM 2.0.*x* to DFM 2.0.3.

Table 3-6 Procedure for Remote Upgrade from DFM 2.0.x to DFM 2.0.3

	Tasks	Reference
Step 1	Install DFM 2.0.3 on the remote system.	Performing a New Installation, page 2-4
Step 2	Back up your DFM 2.0.*x* data on the local host.	Backing Up Your DFM 2.0.x Data, page 3-24
Step 3	Copy the backup files from your local DFM 2.0.*x* host to the remote DFM 2.0.3 host.	Copy the Backup Files from Your Local DFM 2.0.x Host, page 3-24
Step 4	Run the restorebackup.pl script on the DFM 2.0.3 host to restore your data.	Restoring the DFM Data on Your Remote DFM 2.0.3 Host, page 3-25
Step 5	Perform post-upgrade steps to complete basic configuration of DFM 2.0.3.	Post-Upgrade Steps, page 3-26

Installing DFM 2.0.3 on the Remote Host

Install DFM 2.0.3 on your remote host, as described in Performing a New Installation, page 2-4. (Depending upon your con figuration, 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 3-24.

Step 2 Copy the backup files from your local DFM 2.0.x host to a safe location on the remote DFM 2.0.3 host.

Restoring the DFM Data on Your Remote DFM 2.0.3 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 2.0.3 host, restore your DFM data using restorebackup.pl.

a. Stop the daemon manager:

```
net stop crmdmgtd
```

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 3-24 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. 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 2.0.3, page 3-3.

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 crmdmgtd
```

Step 2 To check the status of device discovery and to complete your configuration of DFM, see Post-Upgrade Steps, page 3-26.

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 4-13.
- Familiarize yourself with new device management procedures; see Performing Device Management, page 4-5.
- Verify discovery status; see Verifying Devices Added to DFM, page 4-6.

- Perform SNMP trap configuration tasks; see Configuring SNMP Trap Receiving and Forwarding, page 4-13.
- Start using DFM to monitor the network; see Viewing Alerts, page 4-18 and What Next?, page 4-19.

If you plan to use HPOV-NetView adapters on a remote system, with Device Fault Manager 2.0.3 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 4-18.
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.

Getting Started

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

Configuration Roadmap

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

Table 4-1 Configuration Roadmap

Task	Steps	References
Add devices to DFM managed inventory.	1. Add devices and credentials to Common Services Device and Credentials Repository (DCR).	• Managing Device Credentials, page 4-5 • Importing Devices to the Device and Credentials Repository, page 4-5
	2. Verify that devices were discovered (and troubleshoot problems, if necessary).	• Verifying Devices Added to DFM, page 4-6 • Troubleshooting Device Discovery, page 4-9

Table 4-1 Configuration Roadmap (continued)

Task	Steps	References
Configure Trap Receiving	3. Determine which of the following approaches to SNMP trap receiving to take and perform the appropriate steps:	—
	• Send SNMP traps directly to DFM: a. Update DFM trap receiving port if necessary. b. Enable devices to send traps to DFM.	— • Updating the SNMP Trap Receiving Port, page 4-13 • Enabling Devices to Send Traps to DFM, page 4-14
	• Integrate DFM SNMP trap receiving with other NMSs or trap daemons.	• Integrating DFM Trap Receiving with NMSs or Trap Daemons, page 4-15
(Optional) Configure DFM Trap Forwarding	4. Configure DFM to forward traps.	Configuring SNMP Trap Forwarding, page 4-18

After you complete the tasks in Table 4-1:

- You can monitor the network using the Alerts and Activities display (see Viewing Alerts, page 4-18).
- You can use DFM and continue to configure it; see What Next?, page 4-19.

Using the CiscoWorks Home Page

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

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

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

Note For more information about how DFM integrates with Common Services, Device Center, and the CiscoWorks home page, see *User Guide for Device Fault Manager 2.0.3*.

Registering Applications with the CiscoWorks Home Page

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

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

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

For information about registering a DFM server to the CiscoWorks home page, see *User Guide for Device Fault Manager 2.0.3*. For complete information about Common Services, see *User Guide for CiscoWorks Common Services 3.0.3*.

Understanding and Configuring Security

DFM supports the following security-related mechanisms:

- SNMPv3 protocol (Authentication/No-Privacy option)—DFM supports the authentication/no-privacy option between the server and the device.
- Security on the CiscoWorks server—You can configure the following aspects of security for the server on which DFM resides:
  - **Secure Socket Layer (SSL)**—DFM can use SSL protocol between the server and the browser. You can enable and disable SSL for the server. If you enable SSL, you should set up a self-signed security certificate to enable SSL communication. For more information, see *User Guide for Device Fault Manager 2.0.3*.
  - **Local security or Cisco Secure ACS**—Access to tasks within DFM is controlled either by local security, provided by Common Services, or by Cisco Security ACS. Local security is enabled on the server by default. DFM supports integration with Cisco Secure ACS. You use Common Services to select the type of security you want.

Note For more information, see *User Guide for Device Fault Manager 2.0.3*.

Managing Device Credentials

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

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

To perform these tasks, see *User Guide for CiscoWorks Common Services 3.0.3*. For scenarios for DFM, see Performing Device Management, page 4-5.

Performing Device Management

There are two distinct sets of device management tasks:

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

Importing Devices to the Device and Credentials Repository

You can import devices to DCR from an NMS or from a file. The file format is documented in *User Guide for Common Services 3.0.3*.

Adding Devices to DFM

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

Step 1 On the DFM home page, select **Device Management > Device Selector**.

Step 2 To manually select devices to add to DFM:

a. Deselect the Synchronize with Device Credentials Repository check box. (By default, the check box is selected.)

b. After new devices have been added to DCR, click **Ctrl** and select devices from the Devices not in Device Fault Manager list.

c. Click the > **Add >>** button.

d. Click **OK**.

Step 3 To automatically add devices to DFM:

a. Select the Synchronize with Device Credentials Repository check box.

b. Click **OK**.

For more information, see *User Guide for Device Fault Manager 2.0.3*.

Verifying Devices Added to DFM

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

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

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

Viewing the Device Summary

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

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

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

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

Viewing Device Details

Step 1 On the DFM home page, select **Device Management > Device Details**. The Device Report page opens. In the Device Selector pane, a device group for each current device state is displayed.

Step 2 Select a device group or devices from a group and click **View**. The Device Details report opens in a new window and displays the following information.

Column	Description
Device Name	IP address or DNS name for the device. Clicking this link launches the Detailed Device View, which lists the device components and their managed state (from here you can also change the managed state).
IP Address	IP address for the device.
Status	The device state: Known, Learning, Questioned, Pending, or Unknown. For device state definitions, see Viewing the Device Summary, page 4-7. If devices are not in the Known state, see Troubleshooting Device Discovery, page 4-9.
Device Type	The device type; for example, Content Networking, Routers, Switches and Hubs, and so on. For more information, see *User Guide for Device Fault Manager 2.0.3*.
First Added	Date and time the device was first added to DFM.
Last Discovered	Date and time of most recent discovery.

Viewing Discovery Status

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

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

The View Discovery Status table displays the following information:

Column	Description
Device Name	IP address or DNS name for the device.
Status	Device state—Known, Learning, Questioned, Pending, or Unknown. For device state definitions, see Viewing the Device Summary, page 4-7. If devices are not in the Known state, see Troubleshooting Device Discovery, page 4-9.
DFM Processing	Processing status—One of the following: • Active—DFM is managing the device. • Suspended—DFM is not managing the device. • N/A—DFM cannot manage the device; the device state is Questioned.
Last Discovered	Date and time of most recent discovery.

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

Troubleshooting Device Discovery

To troubleshoot device discovery, try the following:

- If a device is not responding, confirm all device credentials and readd the device. See Changing Device Credentials, page 4-10.
- Increase SNMP timeout settings if device rediscovery times out for several devices. See Modifying SNMP Timeout and Retries, page 4-10.
- View device error information on the Edit Device Configuration page. See Rediscovering a Device, page 4-11.

- Verify that the device is operational during the import and that it supports MIB II.
- Check the reason for devices in the Questioned state. See Understanding Device Discovery Messages, page 4-11.

After troubleshooting your problem, check the device status. See Viewing Discovery Status, page 4-11.

Changing Device Credentials

You change device credentials using Common Services DCR.

Modifying SNMP Timeout and Retries

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

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

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

Step 1 Select **Device Management > SNMP Config**. The SNMP Configuration page appears.

Step 2 Select a new SNMP Timeout setting. The default is 4 seconds.

Step 3 Select a new Number of Retries setting. The default is 3 retries.

Step 4 Click **Apply**. Click **Yes** to confirm.

Rediscovering a Device

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

Step 1 Select **Device Management > Rediscover/Delete**. The Rediscover/Delete Devices page appears.

Step 2 Select the devices or group(s) you want to rediscover.

Step 3 Click **Rediscover**.

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

Viewing Discovery Status

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

Understanding Device Discovery Messages

Table 4-2 lists messages that might be shown for devices in the Questioned state.

Table 4-2 Import Error Messages

Message	Meaning	Action
SNMP Timeout	The device is in the Questioned state because the SNMP read-only community string for the device is incorrect.	See Changing Device Credentials, page 4-10 to enter the correct read community string for the device.
Others: Missing IP Address or Data Collector Timeout	The device is in the Questioned state because of some other reason. It could be that DNS resolution for the device failed or the data collector timed out.	Click the device on the Rediscover/Delete Devices page. The error message displays the exact problem. • If the IP address is missing: – Readd the device with the correct IP address. or – Make sure that DFM can resolve the device name: try adding the domain name as part of the device name. • If the data collector times out, restart the daemon manager to get all data collectors in sync.

Configuring SNMP Trap Receiving and Forwarding

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

- An NMS
- A trap daemon

To send traps directly to DFM, perform the tasks in Enabling Devices to Send Traps to DFM, page 4-14. To integrate SNMP trap receiving with an NMS or a trap daemon, follow the instructions in Integrating DFM Trap Receiving with NMSs or Trap Daemons, page 4-15.

Updating the SNMP Trap Receiving Port

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

Step 1 On the Configuration tab of the DFM home page, select **Other Configurations > SNMP Trap Receiving**.

Step 2 Enter the port number in the Receiving Port entry box.

Step 3 Click **Apply**.

For a list of ports that DFM uses, see Verifying TCP and UDP Ports that DFM Uses, page 2-2.

Enabling Devices to Send Traps to DFM

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

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

- Enabling Cisco IOS-Based Devices to Send Traps to DFM, page 4-14
- Enabling Catalyst Devices to Send SNMP Traps to DFM, page 4-15

Enabling Cisco IOS-Based Devices to Send Traps to DFM

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

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

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

For more information, see the appropriate command reference guide.

Step 1 Log in to Cisco.com.

Step 2 Select **Products & Solutions > Cisco IOS Software**.

Step 3 Select the Cisco IOS Software release version used by your Cisco IOS-based devices.

Step 4 Select **Technical Documentation** and select the appropriate command reference guide.

Enabling Catalyst Devices to Send SNMP Traps to DFM

For devices running Catalyst software, provide the following commands:

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

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

For more information, see the appropriate command reference guide.

Step 1 Log in to Cisco.com.

Step 2 Select **Products & Solutions > Switches**.

Step 3 Select the appropriate Cisco Catalyst series switch.

Step 4 Select **Technical Documentation** and select the appropriate command reference guide.

Integrating DFM Trap Receiving with NMSs or Trap Daemons

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

- Add the host where DFM is running to the list of trap destinations in your network devices. See Enabling Devices to Send Traps to DFM, page 4-14. Specify port 162 as the destination trap port. (If another NMS is already listening for traps on the standard UDP trap port (162), use port 9000, which DFM will use by default.)
- If your network devices are already sending traps to another management application, configure that application to forward traps to DFM. See appropriate documentation for the management application.

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

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

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

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

With DFM installed on…	You can configure DFM to…		Advantages
	Receive traps on this port and…	Forward traps to an NMS on this port	
A host with an NMS	162 (standard listening port and DFM default)	9000 (nonstandard listening port) **Note** You must configure the NMS to listen on this port.	• DFM provides a reliable trap reception and forwarding mechanism. • Devices do not need to be reconfigured to send traps to another host or port. • DFM and the NMS run on the same host.
	9000	162	• DFM provides a reliable trap reception and forwarding mechanism. • No reconfiguration of the NMS is required; it continues to listen for traps on default port 162. • DFM and the NMS run on the same host.
A host and an NMS installed on a remote host	162	162 (on the remote host)	• DFM provides a reliable trap reception and forwarding mechanism. • NMS continues to receive traps on port 162. • Network devices continue to send traps to port 162.

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

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

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

With DFM installed on…	And the NMS receiving traps on this port …	Configure DFM to receive traps (forwarded from the NMS) on this port…	Advantages
A host with an NMS	162 (standard listening port)	9000 (nonstandard listening port; DFM will use this port automatically if port 162 is occupied)	• No reconfiguration of the NMS is required. • No reconfiguration of network devices is required. • DFM and the NMS run on the same host. • DFM does not receive traps dropped by the NMS.
A host and an NMS installed on a remote host	162 (on the remote host) **Note** You must install the HPOV-NetView adapters on the remote host.	162	• No reconfiguration of the NMS is required. • No reconfiguration of network devices is required. • DFM does not receive traps dropped by the NMS.

Configuring SNMP Trap Forwarding

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

Step 1 On the Configuration tab of the DFM home page, select **Other Configurations > SNMP Trap Forwarding**.

Step 2 For each host, enter:

- An IP address or DNS name for the hostname.
- A port number on which the host can receive traps.

Step 3 Click the **Apply** button.

Viewing Alerts

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

Starting DFM

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

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

- Device Management
- Notification Services

- Fault History
- Configuration

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

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

What Next?

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

Table 4-5 summarizes how to continue setting up DFM.

Table 4-5 Setting Up DFM

Task	Description
Configure views for the Alerts and Activities display	View groups control which groups of devices are the focus of the Alerts and Activities display. DFM provides two default view groups. You can add additional view groups.
Configure notifications	In addition to learning about alerts by monitoring the Alerts and Activities display, you can subscribe users to receive e-mail and hosts to receive DFM-generated SNMP traps in response to alerts.

Table 4-5 Setting Up DFM (continued)

Task	Description
Configure polling parameters and thresholds	DFM provides default values for polling parameters and threshold values. However, you can update the values as needed for your network. You should plan to apply the changes when activity on the DFM server is low.
Configure purging	By default, DFM purges the database daily at midnight. You can modify the schedule.
Configure rediscovery	DFM provides a single default schedule for rediscovery. You can use that schedule, or suspend it and create additional rediscovery schedules.

To use DFM more fully, you might want to perform additional configuration tasks. See the online help or *User Guide for Device Fault Manager 2.0.3* for information on using and configuring DFM.

Licensing

This appendix provides licensing information for DFM. It contains the following sections:

Licensing Overview

Installation ensures that you possess a registered and a licensed copy of DFM 2.0.3. The installation script asks the first application installed on Common Services 3.0.1 to enter licensing information. The following licensing information is shipped with the product, printed on the software claim certificate.

Field	Description
Product Identification Number (PIN)	PIN identifies the type of installation, which may be one of the following: • Evaluation installation—For an evaluation copy, licensing details are not required. • Fresh installation. • Upgrade installation.
Product Authorization Key (PAK)	PAK is used to register DFM 2.0.3 on Cisco.com and contains resource limitations. A license file is sent to you after you register the PAK on Cisco.com.

During the installation, if you are prompted to enter licensing information, you can enter either of the following:

- PIN (and PAK)—PIN is mandatory. You are permitted to enter the PAK number later, if required.
- License file location—If you have registered the PAK on Cisco.com and received the license file, you can browse to enter its location.

Note You can obtain a license file before or after you install DFM. (See Registering Your License, page A-3.)

Licensing for a Fresh Installation

The installation script asks the first application installed on Common Services 3.0.1 for the PIN, PAK, and license file location details.

For instance, when DFM 2.0.3 is installed over Common Services 3.0.1, the installer verifies whether or not the system already has the PIN, PAK, and license file details. The details are available if the information was entered earlier using another CiscoWorks application.

If the details are not available, then during the DFM 2.0.3 installation, the installer requests the PIN and PAK or the license file location.

For an evaluation copy of DFM 2.0.3, licensing details are not required. When prompted for licensing information, enter **E** (for evaluation).

Note A message appears at the end of the installation, urging you to obtain a valid license key from Cisco.com within 90 days.

Registering Your License

To register your license:

Step 1 Register the PAK with Cisco.com to get the license file:

- Use this site if you are a registered user of Cisco.com: http://www.cisco.com/go/license.
- Use this site if you are *not* a registered user of Cisco.com: http://www.cisco.com/go/license/public.

Note The PAK is printed on the software claim certificate.

The license file will be e-mailed to you.

Step 2 Copy the license file to the CiscoWorks Common Services server with read permission for casuser.

Step 3 Enter the license file location from the CiscoWorks home page. (Select **Common Services > Server > Admin > Licensing**. For more information, see Common Services online help.)

Note If you had an upgrade license and subsequently obtained an evaluation license for a later version of the software, you should enter the license location on your local server.

If you had an evaluation license and are prompted to validate your license, proceed to Validating Your Upgrade License, page A-4.

Upgrading Your Evaluation License

You can upgrade your evaluation license to a registered and licensed copy of DFM 2.0.3.

Step 1 Contact your Cisco representative about obtaining a PAK.

Step 2 After obtaining a PAK, follow the instructions in Registering Your License, page A-3. The evaluation copy will be converted to a registered copy of DFM 2.0.3.

Validating Your Upgrade License

Proof of Purchase (POP) is required to validate an upgrade license of DFM 2.0.3. If you purchased an upgrade license, at the end of the DFM installation, you are prompted to run a CLI script to validate the upgrade license. The script in turn prompts you to do one of the following:

- Insert the original CD containing DFM 1.2 or DFM 1.2 Updated for Common Services Version 2.2.
- Enter login information for a remote server where the previous version of DFM (DFM 1.2.*x*) is running.

To run the script, see the appropriate upgrade scenario in Chapter 3, "Upgrading and Migrating DFM."

If you do not run the script or if upgrade validation fails, DFM is licensed for evaluation only and operates in *nag* mode for no more than 90 days before ceasing operation. (See Upgrading Your Evaluation License, page A-4.)

Licensing Reminders

DFM provides reminders in the following circumstances:

- Evaluation Version: Before Expiry, page A-5
- Purchased Version: No License File, page A-5
- Restricted Version: Device Limit Exceeded, page A-6

Evaluation Version: Before Expiry

If you have installed the evaluation version of DFM, you must obtain the license file from Cisco.com before expiry of the default evaluation license. For details, see Upgrading Your Evaluation License, page A-4.

Before expiry of the evaluation license, see the following prompt for 10 days:

```
Go to Cisco.com and purchase DFM
```

This message is displayed as an alert after you log in and try to access DFM. If you fail to upgrade your evaluation license after 10 days, all DFM processes will run, but access to DFM functionality will be prohibited.

Purchased Version: No License File

If you have installed a purchased version of DFM, you must register DFM using the PAK number. For details, see Registering Your License, page A-3. You must register DFM within 50 days of installation. If you fail to register DFM after 50 days, you will see the following prompt:

```
Go to Cisco.com and get the product registered.
```

DFM 2.0.3 is fully functional. However, you will continue to receive the alert until you register your license.

Restricted Version: Device Limit Exceeded

If you have a restricted license, DFM notifies you when your device inventory approaches the device limit. After the device limit has been reached, DFM displays the following message:

```
This software has a RESTRICTED license for managing a limited number
of devices. Please click here for current licensing information.
Please contact your Cisco representative to determine if additional
licenses can be purchased for this server.
```

DFM 2.0.3 remains functional, but will shortly stop adding devices to managed inventory.

How is DFM 2.*x* Different from DFM 1.2.*x*?

The differences between DFM 2.*x* and DFM 1.2.*x* are listed in the following sections:

What's New in DFM?

DFM 2.*x* provides a completely new user interface and many new features:

- **Alerts and Activities Display**—DFM introduces the Alerts and Activities display, which provides real-time information about the operational status of your network. You can bring up a display and leave it running, providing an ongoing monitoring tool that signals you when something needs attention. When a fault occurs in your network, DFM generates an event or events that are rolled up into an alert. If the alert occurs on an element in your active view (a logical grouping of device groups), it is shown on your Alerts and Activities display.
- **Fault History**—Fault History is installed when you install DFM. Fault History is integrated with:
  - DFM Alerts and Activities display—You can launch a Fault History report from Alerts and Activities.
  - Common Services Device Center—You can launch a Fault History report for a device that you are troubleshooting in the Device Center.

  DFM 2.*x* also introduces Search by Group; in addition to searching Fault History by device and by alert or event ID, you can search by device group.
- **Customizable event names**—This feature enables you to change event names to names that are more meaningful to you. These customized names are reflected in both the Alerts and Activities display and any Fault History reports you generate.

  More detailed notification messages—When an alert occurs, DFM generates an SNMP trap using CISCO-EPM-NOTIFICATION-MIB. The SNMP trap format includes the attributes of the alert and the events that caused the alert. For more information, see Appendix C, "Notification MIB," in *User Guide for Device Fault Manager 2.0.3*.

  Note The SNMP Trap Notifier MIB is no longer used.

- **Easier notification configuration**—You can fully configure e-mail notification and trap notification from the DFM user interface without the need to modify the configuration on the management server.
- **SYSLOG notification**—DFM adds SYSLOG notification.

- **Additional security—**DFM supports:
  - SSL protocol between the client and the server.
  - SNMP V3 protocol (authNoPriv) between the server and the device.
  - Integration with Cisco Secure Access Control Server (ACS).
- **Automatic device import**—DFM integrates with the Common Services Device and Credentials Repository (DCR) and, by default, automatically imports devices from DCR.
- **Integration with Device Center**—Common Services Device Center is a device troubleshooting tool. DFM integrates with Device Center so that from Device Center, you can:
  - View active fault details: If there is an active fault, the alert ID is displayed on Device Center. You can click the alert ID to open a display with event details, alert status, description, duration, and the date and time the alert was last updated.
  - Launch a Fault History report for the device.

Behavior Changes

Discovery

- DFM now pings a device before performing discovery. This has the following effects:
  - Discovery fails if a device is using a proxy IP. Reconfigure the device access level to use ICMP only.
  - Discovery fails if a device's IP is a virtual IP. Reconfigure the device to use a valid IP address.
- Discovery of device cards is enhanced because DFM checks the cardTable attribute in OLD-CISCO-CHASSIS-MIB.
- DFM does not create interfaces of type ISDN, LAPD, and Other for Cisco Access Routers.

- After you upgrade DFM, you will see an increase in the number of ports and interfaces that are managed for the following devices:
  - Cisco MDS 9000 Series Multilayer Switches
  - Cisco SN 5400 Series Storage Routers
  - Cisco Catalyst 2950 Series Switches (2950-ST-24-LRE, 2955C-12, 2955S-12, 2955T-12)
  - Cisco Catalyst 3550 Series Switches (3550-24-PWR-SMI and -EMI)
  - Cisco Catalyst 3750 Series Switches (3750-stack)

  DFM 1.2.*x* did not create ports and interfaces for these devices because they do not support IF-MIB. DFM creates ports and interfaces for them whether they support IF-MIB or not.

Additional MIB Support

- CISCO-FRAME-RELAY-MIB
- CISCO-PAGP-MIB

User Interface Changes

The DFM 2.*x* user interface is quite different from that of DFM 1.2.*x*. To help you access the applications you need to use, Table B-1 lists the click-by-click navigation paths you would use to access functions in DFM 1.2.*x*. Then it provides the comparable navigation paths to use in DFM 2.*x*.

Table B-1 DFM 1.2.x Navigation Compared to DFM 2.x Navigation

DFM 1.2.*x*	DFM 2.*x*	DFM 2.*x* Description
Device Fault Manager > Administration > Administration Console	**Device Fault Manager > Alerts and Activities** (From the Alerts and Activities display, click a device to open a Detailed Device View.)	From the Detailed Device View, you can: • View device detail information • Manage and unmanage devices • Acknowledge alerts • Annotate events
	(From the CiscoWorks home page) **Common Services > Device and Credentials > Device Management** **Device Fault Manager > Device Management > Device Selector**	Device management, such as add, import, and delete. **Note** In DFM 2.*x*, you import devices into a Device and Credentials Repository (DCR) that is shared by CiscoWorks applications. You select devices from the DCR (or automatically synchronize devices with the DCR) for DFM to manage.
	Device Fault Manager > Device Management > Device Details	View device inventory.
	Device Fault Manager > Configuration > Polling and Thresholds	Configure polling parameters and manage thresholds.
	Device Fault Manager > Configuration > Polling and Thresholds > Operations	Reconfigure DFM to use updated polling parameters and threshold values.

Table B-1 DFM 1.2.x Navigation Compared to DFM 2.x Navigation (continued)

DFM 1.2.*x*	DFM 2.*x*	DFM 2.*x* Description
Device Fault Manager > Monitoring Console	**Device Fault Manager >** Alerts and Activities	Alarm display from which you can: • Launch tools, such as Fault History and Common Services Device Center • Export data to a PDF file or a comma-separated-values file • Print data You can also change the display to show the information that interests you most, as follows: • Select and create views or groups of device groups; use a view that contains the device groups of interest to you. • Filter the display to show alerts based on their severity, status, and originating device.
Device Fault Manager > Administration > Device Discovery > Change Probe	**Device Fault Manager > Device Management > Device Selector** **Note** The change probe process is obsolete in DFM 2.*x*.	Select devices manually or configure DFM to automatically synchronize device inventory with Device and Credentials Repository (DCR). **Note** Applications on different servers can use the same master DCR. For more information, see *User Guide for CiscoWorks Common Services 3.0.3*.
Device Fault Manager > Administration > Device Discovery > Rediscovery Schedule	**Device Fault Manager > Configuration > Other Configurations >** Rediscovery Schedule	• Edit the default rediscovery schedule. • Create additional rediscovery schedules.

Table B-1 DFM 1.2.x Navigation Compared to DFM 2.x Navigation (continued)

DFM 1.2.*x*	DFM 2.*x*	DFM 2.*x* Description
Device Fault Manager > Administration > Trap Configuration > Trap Receiving	**Device Fault Manager > Configuration > Other Configurations > SNMP Trap Receiving**	Change the port number that DFM uses to listen for SNMP traps. **Note** Although the SNMP Trap Adapter file used in DFM 1.2.*x* is still present in the DFM 2.*x* filesystem, DFM 2.*x* does not use it.
Device Fault Manager > Administration > Trap Configuration > Trap Forwarding	**Device Fault Manager > Configuration > Other Configurations > SNMP Trap Forwarding**	Configure hostnames and port numbers for trap forwarding. **Note** Although the SNMP Trap Adapter file used in DFM 1.2.*x* is still present in the DFM 2.*x* filesystem, DFM 2.*x* does not use it.
Device Fault Manager > Administration > Fault Notification > File Notifier	—	If you need to log events to a file, contact the Technical Assistance Center for the workaround for CSCsa83426.
Device Fault Manager > Administration > Fault Notification > Mail Notifier	**Device Fault Manager > Notification Services > E-Mail Notification**	Configure e-mail notifications for alarms. **Note** Although the Mail Notifier Adapter file used in DFM 1.2.*x* is still present in the DFM 2.*x* filesystem, DFM 2.*x* does not use it.
Device Fault Manager > Administration > Fault Notification > Trap Notifier	**Device Fault Manager > Notification Services > Trap Notification**	Configure trap notifications for alarms. **Note** Although the Trap Notifier Adapter file used in DFM 1.2.*x* is still present in the DFM 2.*x* filesystem, DFM 2.*x* does not use it.

Table B-1 DFM 1.2.x Navigation Compared to DFM 2.x Navigation (continued)

DFM 1.2.*x*	DFM 2.*x*	DFM 2.*x* Description
Device Fault Manager > Administration > Fault History Database Sizing	**Device Fault Manager > Configuration > Other Configurations > Daily Purging Schedule**	Trim the Fault History database. **Note** DFM 2.*x* keeps 31 days of history and trims the database daily at the time you specify.
Device Fault Manager > Fault History: • Search by Devices • Search by Fault Conditions	**Device Fault Manager > Fault History:** • Alert Filtering – Search Alarm ID – Search by Device – Search by Group • Event Filtering – Search by Event ID – Search by Device – Search Alert ID – Search by Group	Generate a 31-day Fault History report based on search criteria.
	Device Fault Manager > Alerts and Activities > Tools > Fault History	Generate a 24-hour Fault History report for all alerts in your current view.
	Device Fault Manager > Alerts and Activities Click an alert ID. The Alerts and Activities Detail display appears. In the Tools column next to the device component of interest, select **Fault History**.	Generate a 24-hour Fault History report for all events on a device component.

Terminology Changes

Terminology has changed since DFM 1.2.*x* as follows:

- *Symptom* is replaced by *event*. Events are rolled up into *alerts*.
- *Compound* is not used and there is no replacement. A compound differs from an alert; there could be multiple compounds on a single device, whereas an alert is a roll-up of all events for a device.
- Levels of device certification (*validated, certified, template, undiscovered, uncertified*) are replaced by new device states:
  - *Known*—The device is successfully imported and fully managed by DFM. (Corresponds to *validated* and *certified*).
  - *Learning*—DFM is discovering the device. This is the initial state, when the device is first added to DFM or is being rediscovered.
  - *Questioned*—DFM cannot manage the device. (Can sometimes correspond to *undiscovered*.)
  - *Pending*—The device is being deleted. DFM is waiting for confirmation from all of its data collectors before purging the device and its details.
  - *Unknown*—The device is not supported by DFM. (Corresponds to *unsupported* and *uncertified*).
- *Manage* is replaced by *Activate*; *unmanage* is replaced by *suspend*.
- When a DFM 1.2.*x* fault was *acknowledged*, it was removed from the Alarm Log. In DFM 2.*x*, when an event is *acknowledged*, it remains in the Alerts and Activities display.
- DFM 1.2.*x* assigned devices to groups based on *matching criteria*. DFM 2.*x* assigns devices to groups based on *group rules*.
- DFM 2.*x* eliminates the term *device class* and introduces *device type*.
- DFM 1.2.*x* displayed managed elements organized by *device class*—for example: *Bridge, Host, Hub, MSFC, Probe, Router, RSM, Switch*. DFM 2.*x* displays devices organized by *device group*:
  - Inventory device groups are organized by device state.
  - Polling and Threshold groups are organized by device type; for example, Routers, Switches and Hubs, and Voice and Telephony. (For more information, see *User Guide for Device Fault Manager 2.0.3*.

Device Group Changes

In DFM 1.2.*x*, you could browse the device inventory by selecting a device class. In DFM 2.*x*, you can examine device groups.

Table B-2 Device Group Changes

DFM 1.2.*x* Device Classes	DFM 2.*x* Device Groups
Bridge	Wireless
Host	Cisco Interfaces and Modules Content Networking Network Management Voice and Telephony
Hub	Switches and Hubs
MSFC	Cisco Interfaces and Modules
Probe	Cisco Interfaces and Modules Network Management
Router	Broadband Cable Cisco Interfaces and Modules Content Networking Routers Security and VPN Switches and Hubs Universal Gateways and Access Servers Voice and Telephony Wireless
RSFC	Cisco Interfaces and Modules
RSM	Cisco Interfaces and Modules

Table B-2 Device Group Changes (continued)

DFM 1.2.*x* Device Classes	DFM 2.*x* Device Groups
Switch	Content Networking DSL and Long Reach Ethernet (LRE) Optical Networking Routers Storage Networking Switches and Hubs Wireless Voice and Telephony
Terminal Server	Universal Gateways and Access Servers

Protocol Support Updates

Table B-3 Protocols

Protocol	DFM 1.2.*x*	DFM 2.*x*
SSL	Not SSL-compliant	Uses SSL protocol between the server and the browser. You enable and disable SSL for the server. See *User Guide for Common Services 3.0.3*.
SNMP	• Supports SNMPv1 and SNMPv2 for polling and receiving traps • Forwards traps as SNMPv2	• Supports SNMPv1 and SNMPv2 for polling and receiving traps. • Forwards traps as SNMPv2. • Partially supports SNMPv3: – Uses SNMPv3 protocol between the server and the device. – Supports the Authentication No Privacy (authNoPriv) option.

Configuring DFM with Cisco Secure ACS

This section describes how to configure DFM with Cisco Secure ACS:

CiscoWorks Login Module

The CiscoWorks server provides the mechanism used to authenticate users for CiscoWorks applications. CiscoWorks Common Services supports two modes of user authentication and authorization:

- ACS—In this mode, authentication and authorization services are provided by an Access Control Server (ACS). To use this mode, you must have a Cisco Secure ACS installed on your network.

  The supported Cisco Secure ACSs for Windows are:

  - Cisco Secure ACS 3.2
  - Cisco Secure ACS 3.2.3
  - Cisco Secure ACS 3.3.2
  - Cisco Secure ACS 3.3.3
- Non ACS—In this mode, authentication and authorization services are provided by the CiscoWorks server.

The fallback option in ACS mode is different from that of non-ACS mode. Here, fallback is provided only for authentication.

- If the user authentication with ACS fails, the authentication is tried with CiscoWorks local mode.
- If user authentication succeeds, the user is allowed to change the login module to non-ACS mode, provided the user has permission to do so in non-ACS mode.

For more information, see *User Guide for CiscoWorks Common Services 3.0.3* and the CiscoWorks Common Services 3.0.3 online help.

CiscoWorks Server Authentication Roles

By default, the CiscoWorks server authentication provides five roles in ACS mode. They are listed here from least privileged to most privileged:

1. Help Desk—User with this role has privileges to access network status information from the persisted data. User does not have the privilege to contact any device or schedule a job that will reach the network.

   For example, this user can use the Alerts and Activities display.

2. Approver—User with this role has privileges to approve all DFM tasks and can perform all Help Desk tasks.

   For example, this user can search the Fault History database.

3. Network Operator—User with this role has privileges to perform all tasks that involve collecting data from the network. User does not have write access on the network. User can also perform all the Approver tasks.

   For example, this user can configure logging parameters.

Note In DFM, a user with this role by default can perform the same DFM tasks as a Network Administrator.

4. Network Administrator—User with this role has the privilege to change the network. User can also perform the Network Operator tasks.

   For example, this user can add devices to DFM from the DCR.

5. System Administrator—User with this role has the privilege to perform all CiscoWorks system administration tasks. See the Permissions Report on the CiscoWorks server (**Common Services > Server > Reports > Permission Report**).

   For example, this user can configure SNMP trap forwarding (**Configuration > Other Configurations > SNMP Trap Forwarding**).

We recommend that you do not modify the default CiscoWorks roles.

You can create your own custom roles on Cisco Secure ACS. See *User Guide for CiscoWorks Common Services 3.0.3* and the CiscoWorks Common Services 3.0.3 online help for further details.

Before You Begin: Integration Notes

This section contains notes that you should read before you begin Cisco Secure ACS and CiscoWorks server integration:

- We recommend that you integrate the CiscoWorks server and Cisco Secure ACS after installing all of the LAN Management Solution applications.

  If you have integrated the CiscoWorks server and Cisco Secure ACS before installing DFM 2.0.3, you are prompted with this message at the time of DFM 2.0.3 installation:

  ```
  CiscoWorks Server is in ACS mode
  The application that you are installing requires new tasks to be
  registered with ACS. If you have already registered this
  application with ACS from another server, you do not need to
  register it again. However if you re-register the application, you
  will lose any custom roles that you had created earlier for this
  application in ACS.

  Enter (Y)es to Register, (N)o to continue without registering,
  (Q)uit : [N]
  ```

  - If you enter **Y**, DFM 2.0.3 gets registered with the ACS server.
  - If you enter **N**, DFM 2.0.3 does not get registered with the ACS server.

    After the installation, you can register DFM 2.0.3 with the ACS server, using the AcsRegCli.pl script:

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

    For example (the following command is one line):

    C:\Program~1\CSCOpx\bin\perl C:\Progra~1\CSCOpx\bin\AcsRegCli.pl -register dfm

- For DFM, you must ensure that the CiscoWorks server System Identity Setup user has the privilege to perform all DFM tasks on Cisco Secure ACS.
- If you have installed your application after configuring the CiscoWorks Login Module to ACS mode, then the application users are not granted any permissions. However, the application is registered to the Cisco Secure ACS. On the Cisco Secure ACS server, you must assign the appropriate permissions to the application.

  See the information on server configuration in the *User Guide for Common Services 3.0.3*.

- Multiple instances of same application using the same Cisco Secure ACS will share settings. Any changes will affect all instances of that application.
- If the application is configured with Cisco Secure ACS and then the application is reinstalled, the application will inherit the old settings.

  This is applicable if you are using Cisco Secure ACS version 3.2.3.
- The role that you create is not shared across all the LAN Management Solution applications. It is shared across all CiscoWorks servers that are configured to that particular Cisco Secure ACS.

  You have to create new roles for each of the LAN Management Solution applications that are running on the CiscoWorks server.

  For example, say you have configured 10 CiscoWorks servers with a Cisco Secure ACS, and you have created a role in DFM (for instance, DFMSU). This role is shared for the DFM application running in all 10 CiscoWorks servers. This role is not shared for any other LAN Management Solution applications that are running on the CiscoWorks server.
- You can have different users with different access privileges to the CiscoWorks applications.

  For example, say you have a user, CWSU. This user can be a System Administrator for Common Services, an Approver for RME, a Network Operator for Campus, a Network Administrator for DFM, and a Help Desk user for IPM.
- For details on configuring the CiscoWorks server in ACS mode, see the information on server configuration in the *User Guide for Common Services 3.0.3*.

Configuring DFM on Cisco Secure ACS

After registering the CiscoWorks server with Cisco Secure ACS, perform the following on Cisco Secure ACS:

Step 1 Click **Shared Profile Components** to verify that the Device Fault Manager application entry is present.

Step 2 Based on your authentication setting (per user or per group) on Cisco Secure ACS, click either User Setup or Group Setup.

On Cisco Secure ACS, you can verify the per user or per group setting for DFM using Interface **Configuration > TACACS + (Cisco IOS)**.

Step 3 Assign the appropriate privileges to the user or group to allow them to use DFM.

For DFM, you must ensure that the CiscoWorks server System Identity Setup user has the privilege to perform all DFM tasks on Cisco Secure ACS.

Verifying the DFM and Cisco Secure ACS Configuration

Do the following after performing the above-mentioned tasks on the Cisco Secure ACS server.

Step 1 Log in to CiscoWorks with the username defined in the Cisco Secure ACS.

Step 2 Based on your privilege on the Cisco Secure ACS, verify that you can perform only certain tasks on the CiscoWorks server.

For example, if you have only Help Desk privileges, then you can only view the device summary.

Step 3 Based on the network device setting for the user or group on the Cisco Secure ACS, verify that you can view only certain devices in the CiscoWorks server.

A

B

C

D

E

H

I

L

M

N

O

P

Q

R

S

T

U