



# Installation and Setup Guide for Device Fault Manager 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-7814965=  
Text Part Number: 78-14965-01



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.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Net Readiness Scorecard, Networking Academy, and ScriptShare are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, SMARTnet, StrataView Plus, Stratum, SwitchProbe, TeleRouter, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

Your right to copy the software and this documentation is limited by copyright law. Making unauthorized copies, adaptations, or compilation works is prohibited and constitutes a punishable violation of the law. Use of the software is governed by the license agreement accompanying such software.

The InCharge products mentioned in this document are covered by one or more of the following U.S. patents or pending patent applications: 5,528,516, 5,661,668, 6,249,755, 10,124,881 and 60,284,860.

The documentation is provided "as is" without warranty of any kind. In no event shall System Management ARTS Incorporated be liable for any loss of profits, loss of business, loss of use of data, interruption of business, or for indirect, special, incidental, or consequential damages of any kind, arising from any error in this documentation.

InCharge, the InCharge logo, SMARTS, the SMARTS logo, "Minds Over Networks," and "Ensuring Peak Availability and Performance of E-Business" are trademarks or registered trademarks of System Management ARTS Incorporated.

SMARTS uses the FLEXIm licensing product. FLEXIm is a trademark of Globetrotter Software Inc. For product information, search the web site, [www.globetrotter.com](http://www.globetrotter.com).

All other brand or product names are trademarks or registered trademarks of their respective companies or organizations.

Copyright 1999-2004 by System Management ARTS Incorporated. All rights reserved.

InCharge makes use of ptmalloc, a multi-threaded malloc implementation that includes the following notice.

Copyright (c) 1997 Wolfram Gloger.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that (i) the above copyright notices and this permission notice appear in all copies of the software and related documentation, and (ii) the name of Wolfram Gloger may not be used in any advertising or publicity relating to the software.

THE SOFTWARE IS PROVIDED “AS-IS” AND WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

IN NO EVENT SHALL WOLFRAM GLOGER BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

*Installation and Setup Guide for Device Fault Manager on Windows*

Copyright © 2002-2004, Cisco Systems, Inc.

All rights reserved.





## **Preface ix**

Audience **ix**

Conventions **ix**

Product Documentation **x**

Additional Information Online **xiii**

Obtaining Documentation **xiv**

    Cisco.com **xiv**

    Documentation CD-ROM **xiv**

    Ordering Documentation **xv**

    Documentation Feedback **xv**

Obtaining Technical Assistance **xvi**

    Cisco.com **xvi**

    Technical Assistance Center **xvi**

        Cisco TAC Website **xvii**

        Cisco TAC Escalation Center **xviii**

Obtaining Additional Publications and Information **xviii**

---

## **CHAPTER 1**

### **Prerequisites 1-1**

Product Overview **1-2**

Installation and Upgrade Roadmaps **1-3**

    Roadmap for a New DFM Installation **1-3**

    Roadmap for Upgrading to DFM 1.2 **1-5**

    Roadmap for Upgrading to DFM 1.2 Updated for Common Services  
    Version 2.2 **1-8**

Installation Paths **1-13**

Server Requirements and Recommendations 1-14

Client Requirements 1-19

Supported NMS Environments for Device Import 1-21

Supported NMS Integration 1-21

Supported Devices 1-22

**CHAPTER 2**

**Installing Device Fault Manager 2-1**

Performing a New Installation 2-2

    Performing a New Installation of DFM 1.2 2-2

    Performing a New Installation of DFM 1.2 Updated for Common Services  
Version 2.2 2-9

Upgrading Device Fault Manager 2-12

    Upgrading DFM 1.1 to DFM 1.2 2-12

    Upgrading DFM 1.1 to DFM 1.2 Updated for Common Services  
Version 2.2 2-20

    Upgrading DFM 1.2 to DFM 1.2 Updated for Common Services  
Version 2.2 2-23

    Exporting Local DFM Information to an Upgraded Remote DFM Host 2-24

Reinstalling Device Fault Manager 2-27

    Reinstalling DFM 1.2 2-27

    Reinstalling DFM 1.2 Updated for Common Services Version 2.2 2-33

Removing Device Fault Manager 2-37

Installing and Upgrading Adapters 2-38

    Types of Adapters: Local and Remote 2-38

        Local Adapters 2-38

        Remote Adapters 2-39

    Configuring and Starting Adapters 2-40

Installing or Upgrading the HPOV-NetView Adapter on a Remote Host	2-41
Installing or Upgrading the HPOV-NetView Adapter on a Remote Host Running CiscoWorks	2-42
Installing or Upgrading the HPOV-NetView Adapter on a Remote Host Not Running CiscoWorks	2-44
Installing or Upgrading the RME Adapter on a Remote Host	2-46
Installing or Upgrading the RME Adapter on a Remote DFM Host	2-46
Removing Adapters	2-49
Removing the HPOV-NetView Adapter from a Remote Host	2-49
Removing the HPOV-NetView Adapter from a Remote Host Running CiscoWorks	2-49
Removing the HPOV-NetView Adapter from a Remote Host Not Running CiscoWorks	2-50
Removing the RME Adapter from a Remote Host	2-51

---

**CHAPTER 3****Getting Started 3-1**

Enabling Devices to Send Traps to DFM	3-2
Enabling DFM to Send Traps to NMSs	3-2
Configuring the SNMP Trap Adapter	3-3
Using the GUI to Configure the SNMP Trap Adapter to Receive Traps	3-3
Using the GUI to Configure the SNMP Trap Adapter to Forward Traps	3-4
Integrating the SNMP Trap Adapter with Other Trap Daemons	3-5
Scenario One	3-6
Scenario Two	3-6
Scenario Three	3-7
Scenario Four	3-7
Scenario Five	3-7

- Preparing a Seed File **3-8**
  - Format of a Seed File **3-8**
  - How To Determine What to Put in a Seed File **3-9**
  - Choosing a Router Address for the Seed File: Special Considerations **3-10**
- Accessing Device Fault Manager **3-10**
- Importing Devices from a Seed File **3-11**
  - Changing the Default Read Community String **3-11**
- Opening the DFM Administration Console **3-12**
- Opening the DFM Polling and Thresholds Console **3-12**
- Checking Default Settings **3-13**
- Accessing the Device Inventory **3-13**
- Probing the DFM Inventory **3-14**
  - Synchronizing the DFM Inventory with the Essentials Inventory **3-14**
  - Rediscovering Devices in the Entire DFM Inventory **3-15**
- Opening the DFM Monitoring Console **3-16**
- Closing the DFM Monitoring Console **3-17**

---

**INDEX**



## 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. This guide applies to the following versions of DFM:

- DFM 1.2
- DFM 1.2 Updated for Common Services Version 2.2

Most installation and setup instructions are the same for both versions. Where there are differences, it is noted in the documentation.

## Audience

This guide is intended for anyone who installs and initially uses DFM.

## Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	<b>boldface font</b>
Variables for which you supply values	<i>italic font</i>
Displayed session and system information	screen font

Item	Convention
Information you enter	<b>boldface screen font</b>
Variables you enter	<i>italic screen font</i>
Menu items and button names	<b>boldface font</b>
Selecting a menu item	<b>Option &gt; Network Preferences</b>

**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**

Although every effort has been made to validate the accuracy of the information in the printed and electronic documentation, you should also review the DFM documentation on Cisco.com for any updates.

The following product documentation is available:

*Release Notes for Device Fault Manager 1.2 Updated for Common Services Version 2.2 on Windows*

This document describes new features in this release of DFM, and any known problems and their resolution on a Windows system. This document is available in the following formats:

- Hardcopy packaged with the DFM CD-ROM
- On Cisco.com at [http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm123cd/rel\\_note/win\\_rn.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm123cd/rel_note/win_rn.htm)

*Release Notes for Device Fault Manager 1.2 Updated for Common Services  
Version 2.2 on Solaris*

This document describes new features in this release of DFM, and any known problems and their resolutions on a Solaris system. This document is available in the following formats:

- Hardcopy packaged with the DFM CD-ROM
- On Cisco.com at  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm123cd/re1\\_note/sol\\_rn.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm123cd/re1_note/sol_rn.htm)

*Quick Start Guide for LAN Management Solution*

This document, and the Maintenance Kit version of the document, describes the basic requirements and procedures for installing, upgrading, and setting up the LAN Management Solution. This document is available in the following formats:

- Hardcopy packaged with the DFM CD-ROM
- On Cisco.com at  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000\\_b/lms/lmsmar03/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/lms/lmsmar03/index.htm)

*Installation and Setup Guide for Device Fault Manager on Windows*

This document describes how to install DFM on a Windows system and offers quick-start steps for using DFM. This document is available in the following formats:

- PDF on the DFM CD-ROM
- On Cisco.com at  
<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm123cd/install/windows/index.htm>
- Printed documentation available by order

*Installation and Setup Guide for Device Fault Manager on Solaris*

This document describes how to install DFM on a Solaris system and offers quick-start steps for using DFM. This document is available in the following formats:

- PDF on the DFM CD-ROM
- On Cisco.com at <http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm123cd/install/solaris/index.htm>
- Printed documentation available by order

*User Guide for Device Fault Manager*

This document describes DFM; provides instructions for configuring, administering, and operating it; and answers DFM frequently asked questions. This document is available in the following formats:

- PDF on the DFM CD-ROM and from the DFM online help
- On Cisco.com at [http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm123cd/u\\_gd/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm123cd/u_gd/index.htm)
- Printed documentation available by order

## Context-Sensitive Online Help

You can access the help in two ways:

- Select an option from the navigation tree, then click **Help**.
- Click the **Help** button in the dialog box.

# Additional Information Online

The following additional information is available online:

## *Device Fault Manager Frequently Asked Questions*

This document describes DFM frequently asked questions. This document is available on Cisco.com at

[http://www.cisco.com/en/US/products/sw/cscowork/ps2421/prod\\_troubleshooting\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/cscowork/ps2421/prod_troubleshooting_guides_list.html).

## *Fault History 1.1.1 Drop-in Readme for Solaris*

This document describes how to download and configure Fault History on Solaris. This document is available on Cisco.com at

<http://www.cisco.com/cgi-bin/tablebuild.pl/cw-fault-history>.

## *Fault History 1.1.1 Drop-in Readme for Windows*

This document describes how to download and configure Fault History on Windows. This document is available on Cisco.com at

<http://www.cisco.com/cgi-bin/tablebuild.pl/cw-fault-history>.

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/en/US/products/sw/cscowork/ps2421/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/sw/cscowork/ps2421/products_device_support_tables_list.html).

You can download device packages for new devices from Cisco.com and find information about all supported devices by logging into Cisco.com at

<http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>.

Device packages are released cumulatively; that is, new device packages contain the contents of any previous packages.

To determine which packages are installed on your CiscoWorks Server, select **Server Configuration > About the Server > Applications and Versions**.

You can also obtain any published patches from the download site.

# Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco web sites can be accessed from this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

<http://www.cisco.com/go/subscription>

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:  
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can email your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit your comments by mail by using the response card 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.

# Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

## Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

## Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

<http://www.cisco.com/en/US/support/index.html>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

## Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

## Obtaining Additional Publications and Information

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

[http://www.cisco.com/en/US/products/products\\_catalog\\_links\\_launch.html](http://www.cisco.com/en/US/products/products_catalog_links_launch.html)

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:

[http://www.cisco.com/en/US/about/ac123/ac114/about\\_cisco\\_packet\\_magazine.html](http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html)

- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:

[http://business.cisco.com/prod/tree.taf%3fasset\\_id=44699&public\\_view=true&kbns=1.html](http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html)

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

[http://www.cisco.com/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)

- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:

[http://www.cisco.com/en/US/learning/le31/learning\\_recommended\\_training\\_list.html](http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html)





# Prerequisites

---

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

- [Product Overview, page 1-2](#)
- [Installation and Upgrade Roadmaps, page 1-3](#)
- [Installation Paths, page 1-13](#)
- [Server Requirements and Recommendations, page 1-14](#)
- [Client Requirements, page 1-19](#)
- [Supported NMS Environments for Device Import, page 1-21](#)
- [Supported NMS Integration, page 1-21](#)
- [Supported Devices, page 1-22](#)

# 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. It consists of both internal components and a graphical user interface (GUI).

[Table 1-1](#) describes which DFM components are installed when you select one of the installation options.

**Table 1-1 DFM Installation Options and Their Contents**

Installation Option	Installation Option Contents
CiscoWorks Device Fault Manager	DFM; the base package for DFM incremental device support (which enables you to download support for new devices from Cisco.com); the RME Adapter for synchronizing DFM with a local version of Resource Manager Essentials (Essentials); and the HPOV-NetView Adapter for integrating DFM with local versions of HP OpenView and NetView. This option is normally chosen to install the entire DFM product on a local machine.
Device Fault Manager Incremental Device Support	<i>Only</i> the base package for DFM incremental device support, which enables you to download support for new devices from Cisco.com. This option is normally chosen to reinstall Incremental DeviceUpdate (IDU).
Device Fault Manager HPOV-NetView Adapter	<i>Only</i> the HPOV-NetView Adapter. (This option is only displayed if HP OpenView or NetView are installed.) This option is normally chosen to install the adapter 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 this adapter, refer to <a href="#">Table 2-4 on page 2-40</a> . You can also install remote adapters using DFM 1.2 Patch/IDU 1.2.7 or later.
Device Fault Manager RME Adapter	<i>Only</i> the RME Adapter. (This option is only displayed if Essentials is installed.) This option is normally chosen to install the adapter on a remote machine running Resource Manager Essentials (RME), to send a list of devices in the remote Essentials inventory to a local DFM. For information on how to configure and start this adapter, refer to <a href="#">Table 2-4 on page 2-40</a> . You can also install remote adapters using DFM 1.2 Patch/IDU 1.2.7 or later.

# Installation and Upgrade Roadmaps

This section contains installation and upgrade roadmaps for the following scenarios:

- [Roadmap for a New DFM Installation, page 1-3](#)
- [Roadmap for Upgrading to DFM 1.2, page 1-5](#)
- [Roadmap for Upgrading to DFM 1.2 Updated for Common Services Version 2.2, page 1-8](#)

## Roadmap for a New DFM Installation

[Table 1-2](#) provides an overview of how to perform a new DFM installation.

**Table 1-2** *DFM Installation Roadmap*

<b>If you want to use...</b>	<b>And...</b>	<b>You must...</b>	<b>For instructions, refer to...</b>
DFM as a standalone	N/A	Install DFM	<a href="#">Performing a New Installation, page 2-2</a>
DFM with Resource Manager Essentials	Essentials is installed on the DFM host	Install DFM (the RME Adapter will be installed)	<a href="#">Performing a New Installation, page 2-2</a>
	Essentials is <i>not</i> installed on the DFM host	Install RME Adapter on the remote Essentials host	<a href="#">Installing or Upgrading the RME Adapter on a Remote Host, page 2-46</a>

Table 1-2 DFM Installation Roadmap (continued)

If you want to use...	And...	You must...	For instructions, refer to...	
DFM with HP OpenView or NetView	HP OpenView or NetView is installed on the DFM host	Install DFM (the HPOV-NetView Adapter will be installed on the same drive as NetView)	<a href="#">Performing a New Installation, page 2-2</a>	
	HP OpenView or NetView is <i>not</i> installed on the DFM host	and CiscoWorks is installed on the HP OpenView or NetView host	Install HPOV-NetView Adapter on the same drive as NetView on the remote HP OpenView or NetView host	<a href="#">Installing or Upgrading the HPOV-NetView Adapter on a Remote Host Running CiscoWorks, page 2-42</a>
		and CiscoWorks is <i>not</i> installed on the HP OpenView or NetView host	Install HPOV-NetView Adapter on the remote HP OpenView or NetView host	<a href="#">Installing or Upgrading the HPOV-NetView Adapter on a Remote Host Not Running CiscoWorks, page 2-44</a>
DFM with another NMS	You want DFM to both receive traps from and forward traps (including correlation traps) to the NMS	<b>1.</b> Install Device Fault Manager	<a href="#">Performing a New Installation, page 2-2</a>	
		<b>2.</b> Enable devices to send traps to DFM	<a href="#">Enabling Devices to Send Traps to DFM, page 3-2</a>	
		<b>3.</b> Enable DFM to send traps to NMSs	<a href="#">Enabling DFM to Send Traps to NMSs, page 3-2</a>	

## Roadmap for Upgrading to DFM 1.2

Table 1-3 provides an overview of how to upgrade to DFM 1.2.



### Note

If you are upgrading to DFM 1.2 Updated for Common Services Version 2.2, refer to “[Roadmap for Upgrading to DFM 1.2 Updated for Common Services Version 2.2](#)” section on page 1-8.

**Table 1-3 DFM 1.2 Upgrade Roadmap**

If you want to upgrade to...	And...	You must...	For instructions, refer to...
DFM 1.2 as a standalone	DFM 1.1 (with or without any DFM 1.1 IDSs) is installed	1. Install CD One, 5th Edition	<i>Installation and Setup Guide for CD One on Windows</i>
		2. Upgrade to DFM 1.2	<a href="#">Upgrading DFM 1.1 to DFM 1.2, page 2-12</a>
DFM 1.2	DFM 1.1 (with or without any DFM 1.1 IDSs) is installed, along with other applications	1. Determine if all installed applications are supported by CD One, 5th Edition, and upgrade them, if required	Appropriate documentation
		2. Install CD One, 5th Edition	<i>Installation and Setup Guide for CD One on Windows</i>
		3. Upgrade to DFM 1.2	<a href="#">Upgrading DFM 1.1 to DFM 1.2, page 2-12</a>
		4. Upgrade any remote adapters to DFM 1.2	<a href="#">Installing and Upgrading Adapters, page 2-38</a>

Table 1-3 DFM 1.2 Upgrade Roadmap (continued)

If you want to upgrade to...	And...	You must...	For instructions, refer to...
DFM 1.2	You also want to upgrade your local operating system	<ol style="list-style-type: none"> <li>1. Upgrade your local operating system and install any required patches</li> </ol>	Your vendor documentation
		<ol style="list-style-type: none"> <li>2. Determine if all installed local applications are supported by CD One, 5th Edition, and upgrade them, if required</li> </ol>	Appropriate documentation
		<ol style="list-style-type: none"> <li>3. Install CD One, 5th Edition locally</li> </ol>	<i>Installation and Setup Guide for CD One on Windows</i>
		<ol style="list-style-type: none"> <li>4. Upgrade to DFM 1.2</li> </ol>	<a href="#">Upgrading DFM 1.1 to DFM 1.2, page 2-12</a>
		<ol style="list-style-type: none"> <li>5. Upgrade any remote adapters to DFM 1.2</li> </ol>	<a href="#">Installing and Upgrading Adapters, page 2-38</a>

Table 1-3 DFM 1.2 Upgrade Roadmap (continued)

If you want to upgrade to...	And...	You must...	For instructions, refer to...
DFM 1.2	You also want to upgrade your remote operating system from a local operating system that has not been upgraded	<ol style="list-style-type: none"> <li>1. Upgrade your remote operating system and install any required patches</li> </ol>	Your vendor documentation
		<ol style="list-style-type: none"> <li>2. Determine if all installed remote applications are supported by CD One, 5th Edition, and upgrade them if required</li> </ol>	Appropriate Documentation
		<ol style="list-style-type: none"> <li>3. Install CD One, 5th Edition remotely</li> </ol>	<i>Installation and Setup Guide for CD One on Windows</i>
		<ol style="list-style-type: none"> <li>4. Export local CD One, 4th Edition information to the upgraded CD One, 5th Edition remote host</li> </ol>	<i>Installation and Setup Guide for CD One on Windows</i>
		<ol style="list-style-type: none"> <li>5. Install DFM 1.2 remotely</li> </ol>	<a href="#">Performing a New Installation of DFM 1.2, page 2-2</a>
		<ol style="list-style-type: none"> <li>6. Export DFM 1.1 information to the upgraded DFM 1.2 remote host</li> </ol>	<a href="#">Exporting Local DFM Information to an Upgraded Remote DFM Host, page 2-24</a>

## Roadmap for Upgrading to DFM 1.2 Updated for Common Services Version 2.2

Table 1-4 provides an overview of how to perform an upgrade to DFM 1.2 Updated for Common Services Version 2.2.

**Table 1-4 DFM 1.2 Updated for Common Services Version 2.2 Upgrade Roadmap**

If you want to upgrade to...	And...	You must...	For instructions, refer to...
DFM 1.2 Updated for Common Services Version 2.2 as a standalone	DFM 1.1 (with or without any DFM 1.1 IDSs) is installed	<ol style="list-style-type: none"> <li>1. Install CD One, 5th Edition or Common Services 2.2</li> </ol>	<i>Installation and Setup Guide for CD One on Windows</i> or <i>Installation and Setup Guide for CiscoWorks Common Services (Includes CiscoView) on Windows</i>
		<ol style="list-style-type: none"> <li>2. Upgrade to DFM 1.2 Updated for Common Services Version 2.2</li> </ol>	<a href="#">Upgrading DFM 1.1 to DFM 1.2 Updated for Common Services Version 2.2, page 2-20</a>

**Table 1-4 DFM 1.2 Updated for Common Services Version 2.2 Upgrade Roadmap (continued)**

<b>If you want to upgrade to...</b>	<b>And...</b>	<b>You must...</b>	<b>For instructions, refer to...</b>
DFM 1.2 Updated for Common Services Version 2.2	DFM 1.1 (with or without any DFM 1.1 IDSs) is installed, along with other applications	<b>1.</b> Determine if all installed applications are supported by CD One, 5th Edition or Common Services 2.2, and upgrade them, if required	Appropriate documentation
		<b>2.</b> Install CD One, 5th Edition or Common Services 2.2	<i>Installation and Setup Guide for CD One on Windows</i> or <i>Installation and Setup Guide for CiscoWorks Common Services (Includes CiscoView) on Windows</i>
		<b>3.</b> Upgrade to DFM 1.2 Updated for Common Services Version 2.2	<a href="#">Upgrading DFM 1.1 to DFM 1.2 Updated for Common Services Version 2.2, page 2-20</a>
		<b>4.</b> Upgrade any remote adapters to DFM 1.2 Updated for Common Services Version 2.2	<a href="#">Installing and Upgrading Adapters, page 2-38</a>
DFM 1.2 Updated for Common Services Version 2.2 as a standalone	DFM 1.2 (with or without IDU 1.2.1 or Patch 1.2.2) is installed <sup>1,2</sup>	<b>1.</b> If desired, install Common Services 2.2	<i>Installation and Setup Guide for CiscoWorks Common Services (Includes CiscoView) on Windows</i>
		<b>2.</b> Upgrade to DFM 1.2 Updated for Common Services Version 2.2	<a href="#">Upgrading DFM 1.2 to DFM 1.2 Updated for Common Services Version 2.2, page 2-23</a>

**Table 1-4 DFM 1.2 Updated for Common Services Version 2.2 Upgrade Roadmap (continued)**

If you want to upgrade to...	And...	You must...	For instructions, refer to...
DFM 1.2 Updated for Common Services Version 2.2	DFM 1.2 (with or without IDU 1.2.1 or Patch 1.2.2) is installed, along with other applications <sup>1,2</sup>	<ol style="list-style-type: none"> <li>1. Determine if all installed applications are supported by Common Services 2.2, and upgrade them, if required</li> </ol>	Appropriate documentation
		<ol style="list-style-type: none"> <li>2. If desired, install Common Services 2.2</li> </ol>	<i>Installation and Setup Guide for CiscoWorks Common Services (Includes CiscoView) on Windows</i>
		<ol style="list-style-type: none"> <li>3. Upgrade to DFM 1.2 Updated for Common Services Version 2.2</li> </ol>	<a href="#">Upgrading DFM 1.2 to DFM 1.2 Updated for Common Services Version 2.2, page 2-23</a>

**Table 1-4 DFM 1.2 Updated for Common Services Version 2.2 Upgrade Roadmap (continued)**

If you want to upgrade to...	And...	You must...	For instructions, refer to...
DFM 1.2 Updated for Common Services Version 2.2	You also want to upgrade your local operating system <sup>1,2</sup>	<ol style="list-style-type: none"> <li>1. Upgrade your local operating system and install any required patches</li> </ol>	Your vendor documentation
		<ol style="list-style-type: none"> <li>2. Determine if all installed local applications are supported by CD One, 5th Edition or Common Services 2.2, and upgrade them, if required</li> </ol>	Appropriate documentation
		<ol style="list-style-type: none"> <li>3. Install CD One, 5th Edition or Common Services 2.2 locally</li> </ol>	<i>Installation and Setup Guide for CD One on Windows</i> or <i>Installation and Setup Guide for CiscoWorks Common Services (Includes CiscoView) on Windows</i>
		<ol style="list-style-type: none"> <li>4. Install DFM 1.2 Updated for Common Services Version 2.2</li> </ol>	<a href="#">Upgrading DFM 1.1 to DFM 1.2 Updated for Common Services Version 2.2, page 2-20</a> or <a href="#">Upgrading DFM 1.2 to DFM 1.2 Updated for Common Services Version 2.2, page 2-23</a>
		<ol style="list-style-type: none"> <li>5. If you are upgrading from DFM 1.1, upgrade any remote adapters to DFM 1.2 Updated for Common Services Version 2.2</li> </ol>	<a href="#">Installing and Upgrading Adapters, page 2-38</a>

Table 1-4 DFM 1.2 Updated for Common Services Version 2.2 Upgrade Roadmap (continued)

If you want to upgrade to...	And...	You must...	For instructions, refer to...
DFM 1.2 Updated for Common Services Version 2.2	You also want to upgrade your remote operating system from a local operating system that has not been upgraded <sup>1,2</sup>	<ol style="list-style-type: none"> <li>1. Upgrade your remote operating system and install any required patches</li> </ol>	Your vendor documentation
		<ol style="list-style-type: none"> <li>2. Determine if all installed remote applications are supported by CD One, 5th Edition or Common Services 2.2, and upgrade them if required.</li> </ol>	Appropriate documentation
		<ol style="list-style-type: none"> <li>3. Install CD One, 5th Edition or Common Services 2.2 remotely</li> </ol>	<i>Installation and Setup Guide for CD One on Windows</i> or <i>Installation and Setup Guide for CiscoWorks Common Services (Includes CiscoView) on Windows</i>
		<ol style="list-style-type: none"> <li>4. Export local CD One, 4th Edition information to the upgraded CD One, 5th Edition or Common Services 2.2 remote host</li> </ol>	<i>Installation and Setup Guide for CD One on Windows</i> or <i>Installation and Setup Guide for CiscoWorks Common Services (Includes CiscoView) on Windows</i>
		<ol style="list-style-type: none"> <li>5. Install DFM 1.2 Updated for Common Services Version 2.2 remotely</li> </ol>	<a href="#">Performing a New Installation, page 2-2</a>

**Table 1-4 DFM 1.2 Updated for Common Services Version 2.2 Upgrade Roadmap (continued)**

If you want to upgrade to...	And...	You must...	For instructions, refer to...
DFM 1.2 Updated for Common Services Version 2.2 (continued)	You also want to upgrade your remote operating system from a local operating system that has not been upgraded	<b>6.</b> Export DFM information to the upgraded DFM 1.2 Updated for Common Services Version 2.2 remote host	<a href="#">Exporting Local DFM Information to an Upgraded Remote DFM Host, page 2-24</a>

1. If DFM 1.2 is currently installed, instead of installing from the CD, download the latest IDU from the DFM download page at [http://www.cisco.com/en/US/products/sw/cscowork/ps2421/prod\\_upgrades\\_and\\_downloads.html](http://www.cisco.com/en/US/products/sw/cscowork/ps2421/prod_upgrades_and_downloads.html). The IDU contains the same functionality as DFM 1.2 Updated for Common Services Version 2.2.
2. If you choose to upgrade to Common Services 2.2 and your DFM has an IDU later than DFM 1.2 IDU 1.2.3, you will not lose any existing device support.

## Installation Paths

You can install DFM 1.2 on:

- CD One, 5th Edition (as a standalone DFM)
- Resource Manager Essentials 3.4

You can install DFM 1.2 Updated for Common Services Version 2.2 on:

- CD One, 5th Edition (as a standalone DFM)
- Common Services 2.2 (as a standalone DFM)
- Resource Manager Essentials 3.5

To support integration with remote HP OpenView and NetView, and to support device list synchronization with remote Essentials systems, you must also install individual adapters on the remote NMS machines. For more information, refer to the [“Installing and Upgrading Adapters” section on page 2-38](#).

# Server Requirements and Recommendations

The server system requirements for installing DFM 1.2 are shown in [Table 1-5](#). These requirements apply when installing DFM on:

- CD One, 5th Edition
- Resource Manager Essentials 3.4 when the Availability application is not running

The server system requirements for installing DFM 1.2 Updated for Common Services Version 2.2 are shown in [Table 1-6](#). These requirements apply when installing DFM on:

- CD One, 5th Edition
- Common Services 2.2
- Resource Manager Essentials 3.5 when the Availability application is not running

[Table 1-5](#) and [Table 1-6](#) also provide configuration recommendations when running DFM with CD One, Essentials, or Common Services. These major considerations can help you select or configure a server system that best meets your needs:

- The number of ports being managed. Configurations of over 30,000 ports (of which 15% are trunk ports) are not supported.



## Note

If you use the RME Adapter to synchronize the DFM inventory with a list of Essentials devices, and the synchronization causes DFM to exceed this limit, the Essentials device list will be truncated. (Refer to the [“Supported NMS Environments for Device Import”](#) section on [page 1-21](#).)

To find out how many trunk and access ports are currently imported into DFM, use the `sm_tpmgr` command (described in more detail in the *User Guide for Device Fault Manager*, available from online help):

```
# NMSROOT\objects\smarts\bin\sm_tpmgr.exe --server=DFM --sizes
```

Locate the line that is similar to the following:

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

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

- Whether you plan to use DFM with the Essentials Availability application. (If you plan to use Availability, you must run Essentials and DFM on different machines.)

**Note**

---

If you are installing DFM with the contents of a Cisco product bundle, the server requirements may be different. See the Read Me First document or the quick start guide for the appropriate bundle for additional information.

---

**Table 1-5 DFM 1.2 Server System Requirements and Recommendations**

Requirement Type	Required or Recommended Configuration
System Hardware	<ul style="list-style-type: none"> <li>• IBM PC-compatible computer with 450 MHz Intel Pentium processor</li> <li>• Color monitor</li> <li>• CD-ROM drive</li> </ul>
Memory (RAM)	<ul style="list-style-type: none"> <li>• 512 MB</li> </ul>
Available Drive Space	<ul style="list-style-type: none"> <li>• 4 GB</li> <li>• Swap space equal to double the amount of memory (RAM). For example, if your system has 512 MB of RAM, you need 1024 MB of swap space.</li> <li>• NTFS file system required for secure operation.</li> </ul>
System Software	<ul style="list-style-type: none"> <li>• Windows 2000 Professional and Server with Service Pack 2</li> </ul> <p><b>Note</b> DFM supports only US-English and Japanese versions of Windows operating systems. DFM does not support any other language versions. Set the default locale to US-English or Japanese.</p>
Additional Software (Optional)	<p>One of the following browsers (if you are using the CiscoWorks desktop on the server system):</p> <ul style="list-style-type: none"> <li>• Microsoft Internet Explorer 5.5 with Service Pack 2, or Microsoft Internet Explorer 6.0</li> <li>• Netscape Navigator 4.77, 4.78, or 4.79</li> </ul>

**Table 1-6 DFM 1.2 Updated for Common Services Version 2.2 Server System Requirements and Recommendations**

Requirement Type	Required or Recommended Configuration for CD One	Required or Recommended Configuration for Common Services 2.2 and Essentials 3.5
System Hardware	<ul style="list-style-type: none"> <li>• IBM PC-compatible computer with 450 MHz Intel Pentium processor</li> <li>• Color monitor</li> <li>• CD-ROM drive</li> </ul>	<ul style="list-style-type: none"> <li>• IBM PC-compatible computer with 500 MHz Intel Pentium processor</li> <li>• Color monitor</li> <li>• CD-ROM drive</li> </ul>
Memory (RAM)	<ul style="list-style-type: none"> <li>• 512 MB</li> </ul>	512 MB
Available Drive Space <sup>1</sup>	<ul style="list-style-type: none"> <li>• 4 GB</li> <li>• Swap space equal to double the amount of memory (RAM). For example, if your system has 512 MB of RAM, you need 1024 MB of swap space.</li> <li>• NTFS file system required for secure operation.</li> </ul>	<ul style="list-style-type: none"> <li>• 4 GB</li> <li>• Paging file space equal to double the amount of memory (RAM). For example, if your system has 256 MB of RAM, you need 512 MB of page file.</li> <li>• NTFS file system required for secure operation.</li> <li>• At least 16 MB in Windows temporary directory (%TEMP%).</li> </ul>
System Software <sup>2,3</sup>	<ul style="list-style-type: none"> <li>• Windows 2000 Professional and Server with Service Pack 2</li> </ul>	<ul style="list-style-type: none"> <li>• ODBC Driver Manager 3.5.10.</li> <li>• Windows 2000 Professional; Windows 2000 Server with Service Pack 3; Windows 2000 with Service Pack 4<sup>4</sup></li> <li>• Windows Advanced Server without enabling terminal services.</li> </ul>

**Table 1-6 DFM 1.2 Updated for Common Services Version 2.2 Server System Requirements and Recommendations (continued)**

Requirement Type	Required or Recommended Configuration for CD One	Required or Recommended Configuration for Common Services 2.2 and Essentials 3.5
Additional Software (Optional) Browsers	<ul style="list-style-type: none"> <li>Microsoft Internet Explorer 5.5 with Service Pack 2, or Microsoft Internet Explorer 6.0.</li> <li>Netscape Navigator 4.77, 4.78, or 4.79.</li> </ul>	<ul style="list-style-type: none"> <li>Microsoft Internet Explorer 6.0 (version 6.0.2600.0000); Internet Explorer 6.0 with Service Pack 1 (version 6.0.2800.1106); Java Virtual Machine (JVM) 5.1.3182; Java plug-in version 1.3.1; Java plug-in version 1.4.1_02<sup>4</sup></li> </ul> <p>To verify the JVM, select <b>View &gt; Java Console</b> from Internet Explorer.</p> <ul style="list-style-type: none"> <li>Netscape Navigator 4.78; Netscape Navigator 4.79; Netscape Navigator 7.1<sup>4</sup></li> </ul>

1. Do not install CiscoWorks on a FAT file system.
2. For Common Services installations, you cannot install CiscoWorks on a system configured as a primary or backup domain controller or as a terminal server. Do not install CiscoWorks in an encrypted directory. CiscoWorks do not support directory encryption.
3. DFM supports only US-English and Japanese versions of Windows operating systems. DFM does not support any other language versions. Set the default locale to US-English or Japanese.
4. This is supported if you have installed the LAN Management Solution 2.2 Update 1. You can download the update by logging into Cisco.com and selecting **Products and Services > Network Management CiscoWorks > CiscoWorks LAN Management Solution Software > Software Center > Download Software Image > LMS Bundle Downloads..**

**Note**

Installation will continue with a warning message on Windows Advanced Server if terminal services are enabled in remote admin mode, but will abort when terminal services are enabled in application mode.

Do not use nonstandard java options through the `_JAVA_OPTIONS` environment variable.


# Client Requirements

The minimum system requirements for the CiscoWorks client are shown in [Table 1-7](#).

**Table 1-7 Client System Requirements Summary**

Requirement Type	Minimum Requirements for CD One	Minimum Requirements for Common Services 2.2
System Hardware and Software	<p>Client system: Any of the following with video cards set to 256 colors:</p> <p><b>Tip</b> Use Windows clients for optimal performance.</p> <ul style="list-style-type: none"> <li>• IBM PC-compatible computer with 450 MHz Pentium processor running:               <ul style="list-style-type: none"> <li>– Windows NT 4.0 Workstation and Server with Service Pack 6a.</li> <li>– Windows 98.</li> <li>– Windows 2000 Professional and Server with Service Pack 2.</li> </ul> </li> <li>• SPARC Ultra 10 running Solaris 2.7 or Solaris 2.8.</li> <li>• IBM RS/6000 workstation running AIX 4.3.3.</li> <li>• HP900 workstation running HP-UX 11.0.</li> </ul>	<p>Client system: Any of the following with video card set to 256 colors:</p> <p><b>Tip</b> Use Windows clients for optimal performance.</p> <ul style="list-style-type: none"> <li>• IBM PC-compatible computer with at least a 300 MHz Pentium processor running:               <ul style="list-style-type: none"> <li>– Windows 2000 with Service Pack 3 (Professional and Server).</li> <li>– Windows 2000 with Service Pack 4<sup>1</sup>.</li> <li>– Windows XP with Service Pack 1.</li> <li>– Windows XP with ServicePack 1a<sup>1</sup>.</li> </ul> </li> </ul> <p>DFM supports English and Japanese Windows OS as clients.</p> <ul style="list-style-type: none"> <li>• SPARC Ultra 10 running Solaris 2.7 or 2.8.</li> </ul>

Table 1-7 Client System Requirements Summary (continued)

Requirement Type	Minimum Requirements for CD One	Minimum Requirements for Common Services 2.2
Memory (RAM)	128 MB	256 MB
Browser	<p>On clients running Windows NT 4.0 Workstation and Server with Service Pack 6a, Windows 98, Windows 2000 Professional and Server with Service Pack 2:</p> <ul style="list-style-type: none"> <li>• Microsoft Internet Explorer 5.5 with Service Pack 2, or Microsoft Internet Explorer 6.0.</li> <li>• Java Virtual Machine (JVM) version 5.0.0.3182 or current shipping version.</li> </ul> <p>To verify the JVM version, select <b>View&gt;Java Console</b>.</p> <ul style="list-style-type: none"> <li>• Netscape Navigator 4.77, Netscape Navigator 4.78, or Netscape Navigator 4.79.</li> </ul> <p>On Solaris clients (Solaris 2.7 and 2.8):</p> <ul style="list-style-type: none"> <li>• Netscape Navigator 4.76.</li> </ul> <p>On AIX 4.3.3, HP-UX 11.0 clients:</p> <ul style="list-style-type: none"> <li>• Netscape Navigator 4.77, Netscape Navigator 4.78, or Netscape Navigator 4.79.</li> </ul>	<p>On clients running Windows and Windows XP:</p> <ul style="list-style-type: none"> <li>• Microsoft Internet Explorer 6.0 (version 6.0.2600.0000), or Internet Explorer 6.0 with Service Pack 1 (version 6.0.2800.1106).</li> <li>• Java Virtual Machine (JVM) 5.1.3182, Java plug-in version 1.3.1, or Java plug-in version 1.4.1_02<sup>1</sup>.</li> </ul> <p>To verify the JVM version, select <b>View&gt;Java Console</b> from Internet Explorer and <b>Tools&gt;Server&gt;Java Console</b> from Netscape Navigator.</p> <ul style="list-style-type: none"> <li>• Netscape Navigator 4.78, Netscape Navigator 4.79, or Netscape Navigator 7.1<sup>1</sup>.</li> </ul> <p>On Solaris clients (Solaris 2.7 and 2.8):</p> <ul style="list-style-type: none"> <li>• Netscape Navigator 4.76, or Netscape Navigator 7.0<sup>1</sup>.</li> </ul> <p> <b>Caution</b> Use Netscape Navigator downloaded from the Sun Microsystems website only.</p>

1. This is supported if you have installed the LAN Management Solution 2.2 Update 1. You can download the update by logging into Cisco.com and selecting **Products and Services > Network Management CiscoWorks > CiscoWorks LAN Management Solution Software > Software Center > Download Software Image > LMS Bundle Downloads**.

# Supported NMS Environments for Device Import

DFM can synchronize the DFM inventory with a list of devices managed by local or remote versions of Resource Manager Essentials 3.5. If the import causes the DFM system to exceed its device limit, the Essentials list will be truncated. (Refer to [“Server Requirements and Recommendations”](#) section on page 1-14.)

Synchronizing is done automatically if you install DFM on the same host that is running Essentials, or if you locally install Essentials later. If Essentials is running on a remote host, you must install the RME Adapter on the remote Essentials host as described in the [“Installing or Upgrading the RME Adapter on a Remote Host”](#) section on page 2-46.

## Supported NMS Integration

DFM includes several adapters that collect inventory information, gather network event information, and send event notifications to the domain manager or other SNMP recipients, such as NMSs. The adapters are automatically installed when you install DFM.

NMS integration adapters include:

- SNMP Trap Adapter, which listens on a user-specified port for traps sent to DFM from managed devices, and forwards the traps to specified destinations. (Configuring this adapter is described in the [“Enabling DFM to Send Traps to NMSs”](#) section on page 3-2.)
- HPOV-NetView Adapter, which forwards traps (sent from managed devices to the NMS) to DFM from remote or local hosts running:
  - HP OpenView 6.2
  - NetView 6.01
  - NetView 7.1 (supported only on DFM 1.2 Updated for Common Services Version 2.2 when it is installed on CiscoWorks Common Services 2.2)

For remote machines without CiscoWorks the remote HPOV-NetView adapter is supported on:

- For DFM 1.2:
  - Solaris 2.7 or 2.8
  - Windows 2000 Professional or Server with Service Pack 2
- For DFM 1.2 Updated for Common Services Version 2.2:
  - Solaris 2.7 or 2.8
  - Windows 2000 Professional or Server with Service Pack 3 or higher; Windows Advanced Server

Installing this adapter on remote machines is described in the “[Installing or Upgrading the HPOV-NetView Adapter on a Remote Host](#)” section on page 2-41.

**Note**

---

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

---

If the standard UDP trap port (162) is being used by another NMS, you must configure the SNMP Trap Adapter to use a different UDP port, such as port 9000. Refer to the “[Configuring the SNMP Trap Adapter](#)” section on page 3-3.

## 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/en/US/products/sw/cscowork/ps2421/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/sw/cscowork/ps2421/products_device_support_tables_list.html)

You can download device packages for new devices from Cisco.com and find information about all supported devices by logging into Cisco.com at

<http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>.

Device packages are released cumulatively; that is, new device packages contain the contents of any previous packages.

To determine which packages are installed on your CiscoWorks Server, select **Server Configuration > About the Server > Applications and Versions**.

You can also obtain any published patches from the download site.





# Installing Device Fault Manager

---

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

- [Performing a New Installation, page 2-2](#)
- [Upgrading Device Fault Manager, page 2-12](#)
- [Reinstalling Device Fault Manager, page 2-27](#)
- [Removing Device Fault Manager, page 2-37](#)
- [Installing and Upgrading Adapters, page 2-38](#)
- [Removing Adapters, page 2-49](#)

This chapter contains instructions for installing both DFM 1.2 and DFM 1.2 Updated for Common Services Version 2.2. Differences in the installations are noted. Keep the following in mind when deciding whether to upgrade to DFM 1.2 Updated for Common Services Version 2.2:

- Upgrading from DFM 1.2 to DFM 1.2 Updated for Common Services Version 2.2 allows your system to manage devices that were not supported when DFM 1.2 was released, and also provides a number of DFM bug fixes. The devices and bug fixes are listed in the *Release Notes for Device Fault Manager 1.2 Updated for Common Services Version 2.2 on Windows*.
- If you do not plan to upgrade to Common Services 2.2, it may be easier to download and install the latest DFM IDU from:  
[http://www.cisco.com/en/US/products/sw/cscowork/ps2421/prod\\_upgrades\\_and\\_downloads.html](http://www.cisco.com/en/US/products/sw/cscowork/ps2421/prod_upgrades_and_downloads.html).

The IDU includes the same functionality as DFM 1.2 Updated for Common Services Version 2.2, plus additional device support and bug fixes. (If you do upgrade to Common Services 2.2, you can always download and install the DFM IDU after upgrading or re-enabling DFM from the CD.)

- If you upgrade to DFM 1.2 Updated for Common Services Version 2.2, and your system contains installed IDUs that were released *after* DFM 1.2.3, you will not lose any existing device support.

## Performing a New Installation

This section explains how to perform these new installations:

- [Performing a New Installation of DFM 1.2, page 2-2](#)
- [Performing a New Installation of DFM 1.2 Updated for Common Services Version 2.2, page 2-9](#)

## Performing a New Installation of DFM 1.2

Follow these steps to perform a new DFM 1.2 installation on a Windows system.

---

**Step 1** Make sure your system meets these prerequisites:

- Required (or desired) operating system upgrades have been performed, and required service packs are installed.
- All installed applications are supported by CD One, 5th Edition. Applications not supported by CD One, 5th Edition will be disabled when you upgrade CD One.
- CD One, 5th Edition has been installed. (Refer to *Installation and Setup Guide for CD One on Windows*.)

- If desired, HP OpenView or NetView has been installed (to use the HPOV-NetView Adapter with a local version of HP OpenView or NetView).

**Note**

---

NetView must be installed on the same drive as DFM (for local integration) or on the same drive as the HPOV-NetView Adapter (for remote integration).

---

- If HP OpenView is installed and operational, stop all HP OpenView services (or 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 on 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.

---

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

**Step 5** Click **Next**. The Setup Type dialog box appears.

**Step 6** Select **Typical** to install the complete DFM package, which contains DFM, the DFM incremental device support base package, the HPOV-NetView Adapter, and the RME Adapter. (For more information on installation components, refer to [Table 1-1 on page 1-2](#).)

**Step 7** Click **Next**. The Start Copying Files window appears.

**Step 8** Click **Next**. The installation program checks dependencies and system requirements.

**Step 9** The Requirements Verification dialog box displays the results of the requirements check and advises whether the installation can continue. One of the following should then occur:

- If minimum requirements are met, click **OK**. The Setup screen appears, displaying installation progress while files are copied. The Setup Complete dialog box appears.
- If recommended requirements are not met, an error message appears. To continue the installation, click **OK**.

If DFM detects another application using port 162, DFM displays the following message:

```
WARNING: Installation has detected port 162 in use. DFM is set to use
port 9000 for receiving SNMP traps.
```

If you see this message, after the installation completes, you must configure the SNMP Trap Adapter to use a different UDP port, such as port 9000. (Refer to the [“Configuring the SNMP Trap Adapter”](#) section on page 3-3.)

**Step 10** A dialog box appears, asking if you want to connect this instance of DFM with VHM 1.0. Do one of the following:

- If you will be using a remote version of VHM 1.0 with DFM, click **Yes**.  
The installation program copies the files to the CiscoWorks default installation directory C:\Program Files\CSCOPx (*NMSROOT*). The Restart window appears.  
Proceed to [Step 13](#).
- If you will not be using a remote version of VHM 1.0 with DFM, click **No**.  
Proceed to [Step 11](#).




---

**Note** You *must* give the same answer to this question when you install adapters. If you answer **No** and provide a DFM username and password, you *must* provide the same username and password pair when you install adapters.

---

- Step 11** The Setup window appears. In the username field, enter the DFM username. In the password field, enter the DFM password.



---

**Note** You can change your username and password. Refer to the *User Guide for Device Fault Manager*, available from the online help, for more information.

---

- Step 12** Click **Next**. The installation program copies the files to the CiscoWorks default installation directory C:\Program Files\CSCOpX (*NMSROOT*). The Restart window appears.
- Step 13** Remove the DFM CD-ROM from the drive, and store the CD-ROM in a secure, climate-controlled area for safekeeping.
- Step 14** Click **Finish** to reboot the machine.
- Step 15** 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 DFM notification adapters:

```
# NMSROOT\bin\pdcmd.exe -u DfmFileNotifier
# NMSROOT\bin\pdcmd.exe -u DfmTrapNotifier
# NMSROOT\bin\pdcmd.exe -u DfmMailNotifier
```

- For DfmServer:

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

- For DfmBroker:

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

- b. Decide which hosts you want to specify using the --accept option with arguments shown in [Table 2-1](#).



---

**Note** If you specify registration options using pdcmd, you must re-run your command whenever the daemon manager restarts.

---

**Table 2-1 Arguments to the --accept Option**

Argument	Description
<i>host1,host2,...</i>	Allow only <i>host1,host2,...</i> 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).  <b>Note</b> If you specify the clients as hostnames, be sure the hostname is 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 may 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.exe -r DfmBroker -e NMSROOT\objects\smarts\bin\brstart.exe -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.exe -r DfmServer -e NMSROOT\objects\smarts\bin\sm_server.exe -d
DfmBroker -f "--bootstrap=DFM_bootstrap.conf --accept=lucy,ethel --output --name=DFM"
```

- For DFM notification adapters (the following commands are each one line, and will register the adapter processes to automatically start upon reboot):

```
# NMSROOT\bin\pdcmd.exe -r DfmFileNotifier -d DfmServer -e
NMSROOT\objects\smarts\bin\sm_notify.exe -f "--adapter=filelog --output=sm_file_notifier"
```

```
# NMSROOT\bin\pdcmd.exe -r DfmTrapNotifier -d DfmServer -e
NMSROOT\objects\smarts\bin\sm_notify.exe -f "--adapter=trap --output=sm_trap_notifier"
```

```
# NMSROOT\bin\pdcmd.exe -r DfmMailNotifier -d DfmServer -e
NMSROOT\objects\smarts\bin\sm_notify.exe -f "--adapter=mail --output=sm_mail_notifier"
```

If you do not want the daemons to start after a reboot, add the `-n` option to the end of the command, as in this File Notifier Adapter example:

```
# NMSROOT\bin\pdcmd.exe -r DfmFileNotifier -d DfmServer -e
NMSROOT\objects\smarts\bin\sm_notify.exe -f "--adapter=filelog --output=sm_file_notifier"
-n
```

- 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 16** To verify that the DfmServer process is running, log on to the CiscoWorks desktop as the administrator and select **Server Configuration > Administration > Process Management > Process Status**.



---

**Note** If your client does not have the Java plug-in, you will receive a message asking if you want to install it. The plug-in is required for DFM 1.2.

---

- Step 17** If you plan to use remote adapters with Device Fault Manager 1.2, perform these steps:
- Make sure the machine running the DfmBroker is registered with DNS.
  - Install all remote adapters as described in the [“Installing and Upgrading Adapters”](#) section on page 2-38.
- Step 18** To use DFM, select **Device Fault Manager** from the CiscoWorks navigation tree.
- 

If the standard UDP trap port (162) is being used by another NMS, you must configure the SNMP Trap Adapter to use a different UDP port, such as port 9000. Refer to the [“Configuring the SNMP Trap Adapter”](#) section on page 3-3.

If you install another NMS *after* installing DFM, you must:

- Configure DFM to forward traps to the listening port for the NMSs. Refer to the [“Enabling DFM to Send Traps to NMSs”](#) section on page 3-2.
- Make sure the NMSs are configured to receive traps at the port you specify in Step 1. Refer to the appropriate documentation for the NMS.

When HP OpenView or NetView is restarted, CiscoWorks automatically configures the adapters to forward SNMP traps from HP OpenView or NetView to DFM. If you install HP OpenView or NetView later, you will have to either configure the SNMP Trap Adapter to use another port (as described in the [“Configuring the SNMP Trap Adapter”](#) section on page 3-3), or reinstall DFM.

If a local version of Essentials is already installed (or is installed later), CiscoWorks automatically configures the adapters to forward Essentials inventory device information to DFM. To do this with remote versions of HP OpenView, NetView, or Essentials, you must install the remote adapters as described in the [“Installing and Upgrading Adapters”](#) section on page 2-38.

If you had any errors during installation, check the installation log in the root directory on the drive where the operating system is installed. Each installation creates a new log file. (For example, the CiscoWorks installation might create C:\cw2000\_in001.log, the DFM installation might create C:\cw2000\_in002.log, and so forth.) The Technical Assistance Center (TAC) might ask you to send them the installation log.

## Performing a New Installation of DFM 1.2 Updated for Common Services Version 2.2

Follow these steps to perform a new installation of DFM 1.2 Updated for Common Services Version 2.2 on a Windows system.

**Note**

You can also use this procedure to upgrade from DFM 1.2 to DFM 1.2 Updated for Common Services Version 2.2 (as described in the [“Upgrading DFM 1.2 to DFM 1.2 Updated for Common Services Version 2.2”](#) section on page 2-23).

**Step 1** Make sure your system meets these prerequisites:

- Required (or desired) operating system upgrades have been performed, and required service packs are installed.
- All installed applications are supported by CD One, 5th Edition, or Common Services 2.2. Applications not supported by CD One, 5th Edition, or Common Services 2.2, will be disabled when you upgrade CD One.
- CD One, 5th Edition, or Common Services 2.2 has been installed. (Refer to *Installation and Setup Guide for CD One on Windows* or *Installation and Setup Guide for CiscoWorks Common Services (Includes CiscoView) on Windows*.)

- If desired, HP OpenView or NetView has been installed (to use the HPOV-NetView Adapter with a local version of HP OpenView or NetView).




---

**Note** NetView must be installed on the same drive as DFM (for local integration) or on the same drive as the HPOV-NetView Adapter (for remote integration).

---

- If HP OpenView is installed and operational, stop all HP OpenView services (or 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 on 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.

---

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

**Step 5** Click **Next**. The Software License Agreement window appears.




---

**Note** You *may* be asked to validate your DFM image if you are installing DFM using a Maintenance Kit CD (for CiscoWorks LAN Management Solution 2.2). If you are prompted to validate the image, insert a DFM 1.2 (or earlier) CD into one of your system drives. (If autoplay is enabled, a new installation window will open whenever a CD is inserted. Click **Cancel** in each new installation window.) If the DFM image cannot be validated—that is, if you do not have a DFM 1.2 (or earlier) CD—the installation cannot proceed. Contact your Cisco sales representative.

---

**Step 6** To accept the agreement and continue the installation, click **Yes**.

**Step 7** If your system contains installed IDUs that were released *after* DFM 1.2.3 (such as DFM 1.2 IDU 1.2.4), the Enable DFM window opens, displaying the following message:

The installation program has detected a newer version of DFM already on your system. The newer version is disabled. Do you want to enable it?

Click "Yes" to enable the newer version of DFM.

Click "No" to abort the installation.

Do one of the following:

- To enable DFM, click **Yes**. Because continuing the installation would add no new functionality, further DFM installation is not required, and the installation program exits. To re-establish settings that were lost when CiscoWorks Common Services 2.2 was installed (and DFM was disabled), proceed to [Step 15](#) in the "Performing a New Installation of DFM 1.2" section on page 2-2.
- To keep DFM disabled, select **No**. DFM remains disabled, and the installation program exits.

**Step 8** The Setup Type dialog box appears. Select **Typical** to install the complete DFM package, which contains DFM, the DFM incremental device support base package, the HPOV-NetView Adapter, and the RME Adapter. (For more information on installation components, refer to [Table 1-1 on page 1-2](#).)

**Step 9** Click **Next**. The installation program checks dependencies and system requirements.

**Step 10** The System Requirements window appears, displays the results of the requirements check, and advises whether installation can continue. One of the following should then occur:

- If minimum requirements are met, click **Next**.
- If recommended requirements are not met, an error message appears. To continue the installation, click **Next**.

- Step 11** The Summary dialog box displays your selected settings. Click **Next**.
- Step 12** The Setup window appears, displaying installation progress while files are copied.
- If DFM detects another application using port 162, DFM displays the following message:
- ```
WARNING: Installation has detected port 162 in use. DFM is set to use port 9000 for receiving SNMP traps.
```
- If you see this message, after the installation completes, you must configure the SNMP Trap Adapter to use a different UDP port, such as port 9000. (Refer to the [“Configuring the SNMP Trap Adapter”](#) section on page 3-3.)
- Step 13** To finish installing DFM 1.2 Updated for Common Services Version 2.2, follow [Step 10](#) through [Step 18](#) in the [“Performing a New Installation of DFM 1.2”](#) section on page 2-2.
- 

## Upgrading Device Fault Manager

Refer to these sections for procedures on how to perform these upgrades:

- [Upgrading DFM 1.1 to DFM 1.2, page 2-12](#)
- [Upgrading DFM 1.1 to DFM 1.2 Updated for Common Services Version 2.2, page 2-20](#)
- [Upgrading DFM 1.2 to DFM 1.2 Updated for Common Services Version 2.2, page 2-23](#)
- [Exporting Local DFM Information to an Upgraded Remote DFM Host, page 2-24](#)

## Upgrading DFM 1.1 to DFM 1.2

You can upgrade Device Fault Manager 1.1 (installed with or without IDS 1.1.x patches) on local or remote machines. If desired, you can upgrade a remote machine and then export your local DFM information to the upgraded remote machine.

When you upgrade a local version of DFM 1.1 to DFM 1.2, the upgrade program saves and restores the DFM 1.1 seed file, adapter files, repository, and consoles. If desired, you can manually restore the log files from `NMSROOT\objects\smarts\logs`.

**Note**

---

Customized remote consoles are not saved after upgrade.

---

Follow these steps to upgrade a local host to DFM 1.2:

---

**Step 1** Make sure your system meets these prerequisites:

- Required (or desired) operating system upgrades have been performed, and required service packs are installed.
- All installed applications are supported by CD One, 5th Edition. Applications not supported by CD One, 5th Edition will be disabled when you upgrade CD One.
- CD One, 5th Edition has been installed. (Refer to *Installation and Setup Guide for CD One on Windows*.)
- If desired, HP OpenView or NetView has been installed (to use the HPOV-NetView Adapter with a local version of HP OpenView or NetView).

**Note**

---

NetView must be installed on the same drive as DFM (for local integration) or on the same drive as the HPOV-NetView Adapter (for remote integration).

---

- If HP OpenView is installed and operational, all HP OpenView services have been stopped. (If not, 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 on 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.

---

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

**Step 5** Click **Next**. The Setup Type dialog box appears.

**Step 6** Select **Typical** to upgrade the complete DFM package, which contains DFM, the DFM incremental device support base package, the HPOV-NetView Adapter, and the RME Adapter. (For more information on upgrade components, refer to [Table 1-1 on page 1-2.](#))

**Step 7** Click **Next**. The Start Copying Files window appears.

**Step 8** Click **Next**. The installation program checks dependencies and system requirements.

**Step 9** The Requirements Verification dialog box displays the results of the requirements check and advises whether the installation can continue. One of the following should then occur:

- If minimum requirements are met, click **OK**. The Setup screen appears, displaying installation progress while files are copied. The Setup Complete dialog box appears.
- If recommended requirements are not met, an error message appears. To continue the installation, click **OK**.
- If DFM detects another application using port 162, DFM displays the following message:

WARNING: Installation has detected port 162 in use. DFM is set to use port 9000 for receiving SNMP traps.

If you see this message, after the installation completes, you must configure the SNMP Trap Adapter to use a different UDP port, such as port 9000. (Refer to the [“Configuring the SNMP Trap Adapter”](#) section on page 3-3.)

**Step 10** A dialog box appears, asking if you want to connect this instance of DFM with VHM 1.0. Do one of the following:

- If you will be using a remote version of VHM 1.0 with DFM, click **Yes**.

The installation program copies the files to the CiscoWorks default installation directory C:\Program Files\CSCOPx (*NMSROOT*).

Proceed to [Step 13](#).

- If you will not be using a remote version of VHM 1.0 with DFM, click **No**. Proceed to [Step 11](#).



---

**Note** You *must* give the same answer to this question when you install adapters. If you answer **No** and provide a DFM username and password, you *must* provide the same username and password pair when you install adapters.

---

**Step 11** The Setup window appears. In the username field, enter the DFM username. In the password field, enter the DFM password.



---

**Note** You can change your username and password. Refer to the *User Guide for Device Fault Manager*, available from the online help, for more information.

---

**Step 12** Click **Next**. The installation program copies the files to the CiscoWorks default installation directory C:\Program Files\CSCOPx (*NMSROOT*).

**Step 13** A dialog box appears, reminding you to run rediscovery from the Administration Console; this procedure is described in [Step 19](#). Click **OK**. The Restart window appears.

**Step 14** Remove the DFM CD-ROM from the drive, and store the CD-ROM in a secure, climate-controlled area for safekeeping.

**Step 15** Click **Finish** to reboot the machine.



---

**Note** You must reboot the machine to make sure the DFM broker attaches to the correct port (9002).

---

- Step 16** 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 DFM notification adapters:
 

```
# NMSROOT\bin\pdcmd.exe -u DfmFileNotifier
# NMSROOT\bin\pdcmd.exe -u DfmTrapNotifier
# NMSROOT\bin\pdcmd.exe -u DfmMailNotifier
```
    - For DfmServer:
 

```
# NMSROOT\bin\pdcmd.exe -u DfmServer
```
    - For DfmBroker:
 

```
# NMSROOT\bin\pdcmd.exe -u DfmBroker
```
  - b. Decide which hosts you want to specify using the `--accept` option with arguments shown in [Table 2-2](#).



**Note** If you specify registration options using `pdcmd`, you must re-run your command whenever the daemon manager restarts.

**Table 2-2 Arguments to the `--accept` Option**

| Argument               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>host1,host2,...</i> | Allow only <i>host1,host2,...</i> 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).<br><br><b>Note</b> If you specify the clients as hostnames, be sure the hostname is 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 may 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.exe -r DfmBroker -e NMSROOT\objects\smarts\bin\brstart.exe -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.exe -r DfmServer -e NMSROOT\objects\smarts\bin\sm_server.exe -d
DfmBroker -f "--bootstrap=DFM_bootstrap.conf --accept=lucy,ethel --output --name=DFM"
```

- For DFM notification adapters (the following commands are each one line, and will register the adapter processes to automatically start upon reboot):

```
# NMSROOT\bin\pdcmd.exe -r DfmFileNotifier -d DfmServer -e
NMSROOT\objects\smarts\bin\sm_notify.exe -f "--adapter=filelog --output=sm_file_notifier"
```

```
# NMSROOT\bin\pdcmd.exe -r DfmTrapNotifier -d DfmServer -e
NMSROOT\objects\smarts\bin\sm_notify.exe -f "--adapter=trap --output=sm_trap_notifier"
```

```
# NMSROOT\bin\pdcmd.exe -r DfmMailNotifier -d DfmServer -e
NMSROOT\objects\smarts\bin\sm_notify.exe -f "--adapter=mail --output=sm_mail_notifier"
```

If you do not want the daemons to start after a reboot, add the `-n` option to the end of the command, as in this File Notifier Adapter example:

```
# NMSROOT\bin\pdcmd.exe -r DfmFileNotifier -d DfmServer -e
NMSROOT\objects\smarts\bin\sm_notify.exe -f "--adapter=filelog --output=sm_file_notifier"
-n
```

- d. Make sure that the client names and current IP addresses are registered with DNS if:
  - You are running DHCP and/or
  - You specified the clients with hostnames

**Step 17** To verify that the `DfmServer` process is running, log on to the CiscoWorks desktop as the administrator and select **Server Configuration > Administration > Process Management > Process Status**.




---

**Note** If your client does not have the Java plug-in, you will receive a message asking if you want to install it. The plug-in is required for DFM 1.2.

---

**Step 18** Make sure the DFM broker has attached to the correct port:

- a. Clear the browser cache.
- b. Exit the browser.
- c. Reopen the browser.

**Step 19** Rediscover the devices in your DFM inventory by opening the Administration Console and selecting **Inventory > Inventory Collect All**.




---

**Note** Depending on the number of managed devices, rediscovering the entire DFM inventory could take several hours.

---

- Step 20** If you plan to use remote clients (such as adapters) with Device Fault Manager 1.2, perform these steps:
- Make sure the machine running the DfmBroker is registered with DNS.
  - Upgrade all remote adapters as described in the [“Installing and Upgrading Adapters” section on page 2-38](#). If the adapters are installed on a remote VHM 1.0 machine, they do not need to be upgraded.
  - For remote versions of VHM 1.0, restart the remote VHM server process.
- Step 21** Proceed to the [“Exporting Local DFM Information to an Upgraded Remote DFM Host” section on page 2-24](#).
- 

If the standard UDP trap port (162) is being used by another NMS—such as Cisco Voice Manager, Traffic Director, or Real Time Monitor—you must configure the SNMP Trap Adapter to use a different UDP port, such as port 9000. Refer to the [“Configuring the SNMP Trap Adapter” section on page 3-3](#).

If you install another NMS—such as Cisco Voice Manager, Traffic Director, or Real Time Monitor—*after* installing DFM, you must:

- Configure DFM to forward traps to the listening port for the NMSs. Refer to the [“Enabling DFM to Send Traps to NMSs” section on page 3-2](#).
- Make sure the NMSs are configured to receive traps at the port you specify in Step 1. Refer to the appropriate documentation for the NMS.

When HP OpenView or NetView are restarted, CiscoWorks automatically configures the adapters to forward SNMP traps from HP OpenView and NetView to DFM. If you install HP OpenView or NetView later, you will have to either configure the SNMP Trap Adapter to use another port (as described in the [“Configuring the SNMP Trap Adapter” section on page 3-3](#)), or reinstall DFM.

If a local version of Essentials is already installed (or is installed later), CiscoWorks automatically configures the adapters to forward Essentials inventory device information to DFM. To do this with remote versions of HP OpenView, NetView, or Essentials, you must install the remote adapters as described in the [“Installing and Upgrading Adapters” section on page 2-38](#).

If you had any errors during upgrade, check the installation log in the root directory on the drive where the operating system is installed. Each installation creates a new log file. (For example, the CiscoWorks CD One installation might create C:\cw2000\_in001.log, the DFM installation might create C:\cw2000\_in002.log, and so forth.) The Technical Assistance Center (TAC) might ask you to send them the installation log.

## Upgrading DFM 1.1 to DFM 1.2 Updated for Common Services Version 2.2

When you upgrade a local version of DFM 1.1 to DFM 1.2 Updated for Common Services Version 2.2, the upgrade program saves and restores the DFM 1.1 seed file, adapter files, repository, and consoles. If desired, you can manually restore the log files from *NMSROOT*\objects\smarts\logs. You can also upgrade a remote machine and then export your local DFM information to the upgraded remote machine (see the [“Exporting Local DFM Information to an Upgraded Remote DFM Host”](#) section on page 2-24).



---

**Note**

Customized remote consoles are not saved after the upgrade.

---

Follow these steps to upgrade a local host to DFM 1.2 Updated for Common Services Version 2.2:

---

**Step 1**

Make sure your system meets these prerequisites:

- Required (or desired) operating system upgrades have been performed, and required service packs are installed.
- All installed applications are supported by CD One, 5th Edition, or Common Services 2.2. Applications not supported by CD One, 5th Edition, or Common Services 2.2, will be disabled when you upgrade CD One.
- CD One, 5th Edition, or Common Services 2.2 has been installed. (Refer to *Installation and Setup Guide for CD One on Windows* or *Installation and Setup Guide for CiscoWorks Common Services (Includes CiscoView) on Windows*.)

- If desired, HP OpenView or NetView has been installed (to use the HPOV-NetView Adapter with a local version of HP OpenView or NetView).



---

**Note** NetView must be installed on the same drive as DFM (for local integration) or on the same drive as the HPOV-NetView Adapter (for remote integration).

---

- If HP OpenView is installed and operational, all HP OpenView services have been stopped (if not, 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 on 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.

---

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

**Step 5** Click **Next**.

**Step 6** If you are installing DFM on Common Services Version 2.2, the Software License Agreement window appears. To accept the agreement and continue the installation, click **Yes**.



---

**Note** You *may* be asked to validate your DFM image if you are installing DFM using a Maintenance Kit CD (for CiscoWorks LAN Management Solution 2.2). If you are prompted to validate the image, insert a DFM 1.2 (or earlier) CD into one of your system drives. (If autoplay is enabled, a new installation window will open whenever a CD is inserted. Click **Cancel** in each new installation window.) If the DFM image cannot be validated—that is, if you do not have a DFM 1.2 (or earlier) CD—the installation cannot proceed. Contact your Cisco sales representative.

---

**Step 7** The Setup Type dialog box appears. Select **Typical** to upgrade the complete DFM package, which contains DFM, the DFM incremental device support base package, the HPOV-NetView Adapter, and the RME Adapter. (For more information on upgrade components, refer to [Table 1-1 on page 1-2.](#))

The installation program checks dependencies and system requirements.

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

- If minimum requirements are met, click **Next**.
- If recommended requirements are not met, an error message appears. To continue the installation, click **Next**.

**Step 9** The Summary dialog box displays your selected settings. Click **Next**.

**Step 10** The Setup window appears, displaying installation progress while files are copied.

If DFM detects another application using port 162, DFM displays the following message:

```
WARNING: Installation has detected port 162 in use. DFM is set to use
port 9000 for receiving SNMP traps.
```

**Step 11** To finish upgrading DFM 1.1 to DFM 1.2 Updated for Common Services Version 2.2, follow [Step 10](#) through [Step 21](#) in the “[Upgrading DFM 1.1 to DFM 1.2](#)” section on page 2-12.

---

## Upgrading DFM 1.2 to DFM 1.2 Updated for Common Services Version 2.2

You can upgrade Device Fault Manager 1.2, 1.2.1, or 1.2.2 on local or remote machines. To perform the upgrade, follow the procedure in the “[Performing a New Installation of DFM 1.2 Updated for Common Services Version 2.2](#)” section on page 2-9. You do not need to do any data preservation, nor do you need to upgrade any adapters, when upgrading from DFM 1.2 to DFM 1.2 Updated for Common Services Version 2.2.

Keep the following in mind when deciding whether to upgrade to DFM 1.2 Updated for Common Services Version 2.2:

- Upgrading from DFM 1.2 to DFM 1.2 Updated for Common Services Version 2.2 allows your system to manage devices that were not supported when DFM 1.2 was released, and also provides a number of DFM bug fixes. The devices and bug fixes are listed in the *Release Notes for Device Fault Manager 1.2 Updated for Common Services Version 2.2 on Windows*.
- If you do not plan to upgrade to Common Services 2.2, it may be easier to download and install the latest DFM IDU from:  
[http://www.cisco.com/en/US/products/sw/cscowork/ps2421/prod\\_upgrades\\_and\\_downloads.html](http://www.cisco.com/en/US/products/sw/cscowork/ps2421/prod_upgrades_and_downloads.html).

The IDU includes the same functionality as DFM 1.2 Updated for Common Services Version 2.2, plus additional device support and bug fixes. (If you do upgrade to Common Services 2.2, you can always download and install the DFM IDU after upgrading or re-enabling DFM from the CD.)

- If you upgrade to DFM 1.2 Updated for Common Services Version 2.2, and your system contains installed IDUs that were released *after* DFM 1.2.3, you will not lose any existing device support.

If desired, you can upgrade a remote machine and then export your local DFM information to the upgraded remote machine. See the “[Exporting Local DFM Information to an Upgraded Remote DFM Host](#)” section on page 2-24 for more information.

## Exporting Local DFM Information to an Upgraded Remote DFM Host

This procedure exports your local DFM configuration information and imports it to a remote DFM machine that has been upgraded. This procedure applies to the following scenarios:

- Exporting local DFM 1.1 information to a remote host running DFM 1.2
- Exporting local DFM 1.1 information to a remote host running DFM 1.2 Upgraded for Common Services Version 2.2
- Exporting local DFM 1.2 information to a remote host running DFM 1.2 Updated for Common Services Version 2.2

---

**Step 1** As the local administrator, log on to the local DFM system, and insert the upgrade CD-ROM into the CD-ROM drive. For example, do one of the following:

- On the DFM 1.1 system, insert the DFM 1.2 CD-ROM
- On the DFM 1.1 system, insert the DFM 1.2 Updated for Common Services Version 2.2 CD-ROM
- On the DFM 1.2 system, insert the DFM 1.2 Updated for Common Services Version 2.2 CD-ROM.

The installer window appears, asking you if you want to install DFM.

**Step 2** Click **Cancel**.

**Step 3** From a DOS command prompt, stop the CiscoWorks daemon manager:

```
Z:\> net stop crmdmgtd
```

**Step 4** If desired, export your CD One information. Refer to *Installation and Setup Guide for CD One on Windows*, or *Installation and Setup Guide for CiscoWorks Common Services (Includes CiscoView) on Windows*.

**Step 5** Run the export script, which is on the DFM upgrade CD ROM drive under the disk1 directory, from the top-level directory:

```
Z:\> cd \  
Z:\> perl export_dfm.pl
```

**Step 6** Copy all files and directories in *NMSROOT*\rigel to an identical location on the remote machine.

**Caution**

---

The DFM upgrade *NMSROOT*\rigel\scripts directory contains a file that may not be in the local *NMSROOT*\rigel\scripts directory. This file is called *import\_userinfo.pl*. Therefore, do not do a simple directory copy or you will lose this file.

---

**Caution**

---

Be sure to copy the files to the same directory path (*NMSROOT*\rigel). Copy all files, not just the files and directories under the *dfm* directory, because the import script needs files that are not stored under the *dfm* directory.

---

For example, you could do one of the following:

- Map the source drive to the destination drive, and copy the files.
- Copy the files to disk or tape and transfer the files to the remote machine.

**Step 7** On the local DFM machine, restart the CiscoWorks daemon manager:

```
Z:\> net start crmdmgt
```

**Step 8** On the remote (upgraded) DFM machine, stop the CiscoWorks daemon manager:

```
C:\> net stop crmdmgt
```

**Step 9** If desired, import your CD One information. Refer to *Installation and Setup Guide for CD One on Windows*, or *Installation and Setup Guide for CiscoWorks Common Services (Includes CiscoView) on Windows*.

- Step 10** Run the import script, where *NMSROOT* is the default installation directory (normally C:\Program Files\CSCOPx):

```
C:\> cd NMSROOT\rigel\scripts
C:\> perl import_dfm.pl
```

The import script checks the space requirements, ensures that the daemon manager is stopped, and displays the following prompt:

```
Importing will cause all the files to be overwritten.
Are you sure you want to import (Y/N)?
```

- Step 11** Enter **Y** and press **Return**.
- Step 12** Restart the CiscoWorks daemon manager:

```
C:\> net start crmdmgt
```

- Step 13** Rediscover the devices in your DFM inventory by selecting **Inventory>Inventory Collect All**.
- 

If any errors occurred during the upgrade, check the installation log in the root directory on the drive where the operating system is installed. Each installation creates a new log file. (For example, the CiscoWorks CD One installation might create C:\cw2000\_in001.log, the DFM installation might create C:\cw2000\_in002.log, and so forth.) The Technical Assistance Center (TAC) might ask you to send them the installation log. Also check import log, *NMSROOT*\rigel\manifest\dfm\import\_dfm.log (where *NMSROOT* is the default installation directory, normally C:\Program Files\CSCOPx).

# Reinstalling Device Fault Manager

The following sections describe how to reinstall DFM on the Windows operating system:

- [Reinstalling DFM 1.2, page 2-27](#)
- [Reinstalling DFM 1.2 Updated for Common Services Version 2.2, page 2-33](#)

## Reinstalling DFM 1.2

- 
- 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 on 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** Click **Next** to continue. The Setup Type dialog box appears.
- Step 6** Select **Custom** to select the components to reinstall. The Select Components dialog box appears. (For more information on reinstallation components, refer to [Table 1-1 on page 1-2.](#))

- Step 7** Select the component you want to reinstall and click **Next**. The Start Copying Files window appears.
- Step 8** Click **Next**.
- Step 9** If you reinstalled *only* the HPOV-NetView Adapter or the RME Adapter, you are prompted to enter the name of the machine running the DFM Broker. Enter the name of the host (the default is localhost).



---

**Note** Make sure the machine running the DfmBroker is registered with DNS.

---

- Step 10** Click **Next**.
- Step 11** The Requirements Verification dialog box displays the results of the requirements check and advises whether the reinstallation can continue. One of the following should then occur:
- If minimum requirements are met, click **OK**. The Setup screen appears, displaying reinstallation progress while files are copied. The Setup Complete dialog box appears.
  - If recommended requirements are not met, an error message appears. To continue the reinstallation, click **OK**.

If DFM detects another application using port 162, DFM displays the following message:

```
WARNING: Installation has detected port 162 in use. DFM is set to use
port 9000 for receiving SNMP traps.
```

- Step 12** If you see this message, after the installation completes, you must configure the SNMP Trap Adapter to use a different UDP port, such as port 9000. (Refer to the [“Configuring the SNMP Trap Adapter”](#) section on page 3-3.)

- Step 13** A dialog box appears, asking if you want to connect this instance of DFM with VHM 1.0. Do one of the following:
- If you will be using a remote version of VHM 1.0 with DFM, click **Yes**.  
The reinstallation program copies the files to the directory in which DFM was originally installed. The Restart window appears.  
Proceed to [Step 16](#).
  - If you will not be using a remote version of VHM 1.0 with DFM, click **No**.  
Proceed to [Step 14](#).



---

**Note** You *must* give the same answer to this question when you install adapters. If you answer **No** and provide a DFM username and password, you *must* provide the same username and password

---

- Step 14** The Setup window appears. In the username field, enter the DFM username. In the password field, enter the DFM password.



---

**Note** You can change your username and password. Refer to the *User Guide for Device Fault Manager*, available from the online help, for more information.

---

- Step 15** Click **Next**. The reinstallation program copies the files to the directory in which DFM was originally installed. The Restart window appears.
- Step 16** Remove the DFM CD-ROM from the drive, and store the CD-ROM in a secure, climate-controlled area for safekeeping.
- Step 17** Click **Finish** to reboot the machine.

- Step 18** 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 DFM notification adapters:
 

```
# NMSROOT\bin\pdcmd.exe -u DfmFileNotifier
# NMSROOT\bin\pdcmd.exe -u DfmTrapNotifier
# NMSROOT\bin\pdcmd.exe -u DfmMailNotifier
```
    - For DfmServer:
 

```
# NMSROOT\bin\pdcmd.exe -u DfmServer
```
    - For DfmBroker:
 

```
# NMSROOT\bin\pdcmd.exe -u DfmBroker
```
  - b. Decide which hosts you want to specify using the `--accept` option with arguments shown in [Table 2-3](#).



**Note** If you specify registration options using `pdcmd`, you must re-run your command whenever the daemon manager restarts.

**Table 2-3 Arguments to the `--accept` Option**

| Argument               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>host1,host2,...</i> | Allow only <i>host1,host2,...</i> 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).<br><br><b>Note</b> If you specify the clients as hostnames, be sure the hostname is registered with DNS, especially if you are using DHCP. |
| =any                   | Allow all incoming connections (default).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

For example, the following 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 may 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.exe -r DfmBroker -e NMSROOT\objects\smarts\bin\brstart.exe -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.exe -r DfmServer -e NMSROOT\objects\smarts\bin\sm_server.exe -d
DfmBroker -f "--bootstrap=DFM_bootstrap.conf --accept=lucy,ethel --output --name=DFM"
```

- For DFM notification adapters (the following commands are each one line, and will register the adapter processes to automatically start upon reboot):

```
# NMSROOT\bin\pdcmd.exe -r DfmFileNotifier -d DfmServer -e
NMSROOT\objects\smarts\bin\sm_notify.exe -f "--adapter=filelog --output=sm_file_notifier"
```

```
# NMSROOT\bin\pdcmd.exe -r DfmTrapNotifier -d DfmServer -e
NMSROOT\objects\smarts\bin\sm_notify.exe -f "--adapter=trap --output=sm_trap_notifier"
```

```
# NMSROOT\bin\pdcmd.exe -r DfmMailNotifier -d DfmServer -e
NMSROOT\objects\smarts\bin\sm_notify.exe -f "--adapter=mail --output=sm_mail_notifier"
```

If you do not want the daemons to start after a reboot, add the `-n` option to the end of the command, as in this File Notifier Adapter example:

```
# NMSROOT\bin\pdcmd.exe -r DfmFileNotifier -d DfmServer -e
NMSROOT\objects\smarts\bin\sm_notify.exe -f "--adapter=filelog --output=sm_file_notifier"
-n
```

- 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 19** To verify that the `DfmServer` process is running, log on to the CiscoWorks desktop as the administrator and select **Server Configuration > Administration > Process Management > Process Status**.




---

**Note** If your client does not have the Java plug-in, you will receive a message asking if you want to install it. The plug-in is required for DFM 1.2.

---

**Step 20** To use DFM, select **Device Fault Manager** from the CiscoWorks navigation tree.

**Step 21** Rediscover the devices in your DFM inventory by opening the Administration Console and selecting **Inventory > Inventory Collect All**.




---

**Note** Depending on the number of managed devices, rediscovering the entire DFM inventory could take several hours.

---

**Step 22** If you used remote adapters with Device Fault Manager 1.1, perform these steps:

- a. Make sure the machine running the `DfmBroker` is registered with DNS.
  - b. Upgrade all remote adapters as described in the [“Installing and Upgrading Adapters”](#) section on page 2-38.
- 

When HP OpenView or NetView is restarted, CiscoWorks automatically configures the adapters to forward SNMP traps from HP OpenView or NetView to DFM. If you install HP OpenView or NetView later, you will have to either configure the SNMP Trap Adapter to use another port (as described in the [“Configuring the SNMP Trap Adapter”](#) section on page 3-3), or reinstall DFM.

If Essentials is presently (or subsequently) installed locally, CiscoWorks automatically configures the adapters to forward Essentials inventory device information to DFM. To do this with remote versions of HP OpenView, NetView, or Essentials, you must install the remote adapters as described in the “[Installing and Upgrading Adapters](#)” section on page 2-38.

If you had any errors during reinstallation, check the installation log in the root directory on the drive (For example, the CiscoWorks installation might create C:\cw2000\_in001.log, the DFM installation might create C:\cw2000\_in002.log, and so forth.) The Technical Assistance Center (TAC) might ask you to send them the installation log.

## Reinstalling DFM 1.2 Updated for Common Services Version 2.2

- 
- 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 on 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** Click **Next** to continue. The Software License Agreement window appears.
- Step 6** To accept the agreement and continue the reinstallation, click **Yes**.

**Step 7** If your system contains installed IDUs that were released *after* DFM 1.2.3 (such as DFM 1.2 IDU 1.2.4), one of the following will happen:

- If you *did* enable DFM when you first installed it, a window opens displaying the following message:

```
A newer version of DFM is already running on your system.
```

Because the installation would provide no new functionality, the installation program exits, and your existing device support is preserved.

- If you *did not* enable DFM when you first installed it, the Enable DFM window opens, displaying the following message:

```
The installation program has detected a newer version of DFM  
already on your system. The newer version is disabled. Do you want  
to enable it?
```

```
Click "Yes" to enable the newer version of DFM.
```

```
Click "No" to abort the installation.
```

Do one of the following:

- To enable DFM, click **Yes**. Because continuing the installation would add no new functionality, further DFM installation is not required, and the installation program exits. To re-establish settings that were lost when CiscoWorks Common Services 2.2 was installed (and DFM was disabled), proceed to [Step 15](#) in the “[Performing a New Installation of DFM 1.2](#)” section on page 2-2.
- To keep DFM disabled, select **No**. DFM remains disabled, and the installation program exits.

**Step 8** The Setup Type dialog box appears. 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):

```
CiscoWorks Device Fault Manager (reinstall)
Device Fault Manager Incremental Device Support (reinstall)
```

(For more information on reinstallation components, refer to [Table 1-1 on page 1-2.](#))

**Step 9** Select the component you want to reinstall and click **Next**. The installation program checks dependencies and system requirements.

**Step 10** The System Requirements dialog box appears, displays the results of the requirements check, and advises whether the installation can continue. One of the following should then occur:

- If minimum requirements are met, click **Next**.
- If recommended requirements are not met, an error message appears. To continue the reinstallation, click **Next**.

**Step 11** If you reinstalled *only* the HPOV-NetView Adapter or the RME Adapter, you are prompted to enter the name of the machine running the DFM Broker. Enter the name of the host (the default is localhost).



---

**Note** Make sure the machine running the DfmBroker is registered with DNS.

---

**Step 12** Click **Next**.

**Step 13** The Summary dialog box displays your selected settings. Click **Next**.

**Step 14** The Setup window appears, displaying installation progress while files are copied.

If DFM detects another application using port 162, DFM displays the following message:

```
WARNING: Installation has detected port 162 in use. DFM is set to use port 9000 for receiving SNMP traps.
```

If you see this message, after the installation completes, you must configure the SNMP Trap Adapter to use a different UDP port, such as port 9000. (Refer to the [“Configuring the SNMP Trap Adapter”](#) section on page 3-3.)

**Step 15** To finish reinstalling DFM 1.2 Updated for Common Services Version 2.2, follow [Step 13](#) through [Step 22](#) in the [“Reinstalling DFM 1.2”](#) section on page 2-27.

---

# Removing Device Fault Manager

This section explains the steps for removing DFM 1.2 or DFM 1.2 Updated for Common Services Version 2.2 from Windows systems.



---

**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 on to the system on which DFM is installed, and select **Start>Programs>CiscoWorks>Uninstall CiscoWorks** to start the uninstallation process. The Uninstallation window appears, and the system displays these options (the choices may vary, depending on your configuration):

```
CiscoWorks Common Services
CiscoView
Device Fault Manager
```

- Step 2** Deselect everything except **Device Fault Manager** and click **Next**. A dialog box listing the components selected for removal appears. (Removing DFM also removes DFM incremental device support. For more information on uninstallation components, refer to [Table 1-1 on page 1-2](#).)
- Step 3** Click **Next**. Messages appear, showing the progress of the uninstallation, and the uninstallation completes.
-

# Installing and Upgrading Adapters

Several software adapters link DFM with its environment. For the purposes of installation, this section classifies these adapters as local or remote, depending on whether or not they are installed on the same host as DFM. Detailed information on the adapters is provided in the *User Guide for Device Fault Manager* (available from online help).

## Types of Adapters: Local and Remote

Local adapters are installed for forwarding traps or synchronizing information with NMSs running on the DFM host; remote adapters do the same, but on remote hosts not running DFM.

### Local Adapters

When you install DFM locally, all adapters are installed. The local adapters include:

- **File Notifier Adapter**—Logs alarms detected by the DFM server and forwards them to a file. A file is the only valid recipient for this adapter. This adapter is normally used to create a historical file containing all alarms generated by DFM.
- **Trap Notifier Adapter**—Converts DFM alarms into SNMP trap messages and forwards the traps to recipients. You can specify recipients, such as NMSs or other domain managers, using an IP address or a system name. This adapter is normally used to send DFM alarms to another application for additional processing or display.
- **Mail Notifier Adapter**—Using SMTP, send mail notifications to recipients. As with the Trap Notifier Adapter, you can specify recipients—in this case, an email address. This adapter is normally used to generate asynchronous email notifications (for example, to an page or an email address) when one or more alarm conditions occur.
- **SNMP Trap Adapter**—Listens on a user-specified port for traps sent to DFM from managed devices, and forwards traps to specified destinations. This adapter provides a generic method for integrating DFM with other NMS applications. The SNMP Trap Adapter is normally used to allow DFM to

coexist with another trap-receiving application (such as an NMS) on the same server; have an NMS forward traps to DFM for processing; or have DFM listen for traps on devices and forward the traps to an NMS that does not support trap forwarding. Basic steps for configuring this adapter are provided in [Chapter 3, “Getting Started.”](#)

- HPOV-NetView Adapter—Forwards traps that managed devices send to a local HP OpenView or NetView NMS to DFM. This adapter is normally used when you want DFM to monitor faults on devices managed by a local version of HP OpenView or NetView. (For information on supported HP OpenView and NetView versions, refer to the [“Supported NMS Integration”](#) section on [page 1-21.](#))
- RME Adapter—Synchronizes the list of managed devices in a local Essentials inventory with a DFM inventory. This adapter is normally used when you want DFM to monitor faults on devices managed by a local version of Essentials. (For information on supported Essentials versions, refer to the [“Supported NMS Environments for Device Import”](#) section on [page 1-21.](#))

## Remote Adapters

In addition to using the following adapters locally, you can install them remotely (on hosts not running DFM) to exchange remote device information with DFM:

- RME Adapter—Synchronizes the list of managed devices in a remote Essentials inventory with a local DFM inventory. This adapter is normally used when you want a local DFM to monitor faults on devices managed by a remote version of Essentials. (For information on supported Essentials versions, refer to the [“Supported NMS Environments for Device Import”](#) section on [page 1-21.](#))
- HPOV-NetView Adapter—Forwards traps that managed devices send to a remote HP OpenView or NetView NMS to DFM. This adapter is normally used when you want a local DFM to monitor faults on devices managed by a remote version of HP OpenView or NetView. (For information on supported HP OpenView and NetView versions, refer to the [“Supported NMS Integration”](#) section on [page 1-21.](#))

**Note**

---

NetView must be installed on the same drive as DFM (for local integration) or on the same drive as the HPOV-NetView Adapter (for remote integration).

---

## Configuring and Starting Adapters

Table 2-4 summarizes which adapters you must configure, whether you can use the GUI or command line to configure the adapter, and whether you must manually start the adapter. Additional information on configuring and starting adapters is provided in the *User Guide for Device Fault Manager* (available from online help).



### Note

Whenever you configure any adapter using the command line, you must manually stop and restart the adapter. Adapters configured with the DFM administration menus do not need to be stopped and restarted.

**Table 2-4** Configuring and Starting Adapters

| Adapter Type and Name        | Must Be Configured Before Use | Can Be Configured Using...                   |     | Automatically Starts with CiscoWorks                                           |
|------------------------------|-------------------------------|----------------------------------------------|-----|--------------------------------------------------------------------------------|
|                              |                               | GUI                                          | CLI |                                                                                |
| <b>Notification Adapters</b> |                               |                                              |     |                                                                                |
| File Notifier                | Yes                           | Yes                                          | Yes | No                                                                             |
| Trap Notifier                | Yes                           | Yes                                          | Yes | No                                                                             |
| Mail Notifier                | Yes                           | Yes                                          | Yes | No                                                                             |
| <b>Event Adapters</b>        |                               |                                              |     |                                                                                |
| HPOV-NetView                 | No                            | No                                           | Yes | Yes, if HP OpenView or NetView is installed on the same machine as the adapter |
| <b>Special Adapters</b>      |                               |                                              |     |                                                                                |
| SNMP Trap                    | Yes                           | Yes                                          | Yes | Yes                                                                            |
| RME Adapter                  | No                            | N/A, but can be <i>started</i> using the GUI | N/A | Yes, if Essentials is installed on the same machine as the adapter             |

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

This section describes how to install or upgrade the HPOV-NetView Adapter on a remote host so the adapter can exchange information with DFM on a local host. You can install or upgrade the HPOV-NetView Adapter on remote hosts regardless of whether CiscoWorks is present. You can also use this procedure to reinstall the HPOV-NetView Adapter on a machine running CiscoWorks; reinstallation of the HPOV-NetView Adapter is supported only on machines running CiscoWorks.

If you upgrade a local version of DFM 1.1, you must also upgrade all remote adapters. You do not need to upgrade DFM 1.2 adapters if you are upgrading to DFM 1.2 Updated for Common Services Version 2.2.

**Note**

---

NetView must be installed on the same drive as DFM (for local integration) or on the same drive as the HPOV-NetView Adapter (for remote integration).

---

**Note**

---

To upgrade a remote HPOV-NetView Adapter, you must first remove the old adapter and then install the new version.

---

**Note**

---

If the DFM broker is moved—for example, if DFM is moved to a different machine, or you want to use a different instance of DFM—you must reinstall the remote adapters.

---

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

Use this procedure to do the following:

- Install a new HPOV-NetView Adapter on a remote host running CiscoWorks, or
- Upgrade a DFM 1.1 version of the HPOV-NetView Adapter on a remote host running CiscoWorks

You do not need to upgrade DFM 1.2 adapters if you are upgrading to DFM 1.2 Updated for Common Services Version 2.2.

---

**Step 1** If you want to upgrade a DFM 1.1 version of the HPOV-NetView Adapter, remove the adapter as described in the [“Removing the HPOV-NetView Adapter from a Remote Host Running CiscoWorks”](#) section on page 2-49.

**Step 2** As the local administrator, log on to the machine on which you will install the HPOV-NetView Adapter, and insert the DFM CD-ROM into the CD-ROM drive. The installer window appears, asking you if you want to install DFM. (Alternatively, you can install the adapter using DFM 1.2 Patch/IDU 1.2.7 or later, and proceed to [Step 3](#).)




---

**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.

---




---

**Note** To use the HPOV-NetView Adapter with NetView, be sure to install the adapter on the same drive as NetView.

---

**Step 3** Click **Install**. The Welcome window appears.

**Step 4** Click **Next**.

**Step 5** If you are upgrading your DFM 1.1 adapter to DFM 1.2 Updated for Common Services Version 2.2, the Software License Agreement window appears. To accept the agreement and continue the installation, click **Yes**.

**Step 6** The Setup Type dialog box appears. Select **Custom** to select a component to install and click **Next**. The Select Components dialog box appears.

- Step 7** Select **Device Fault Manager HPOV-NetView adapters** and click **Next**. HP OpenView and NetView are stopped. The installation program checks dependencies and system requirements.
- Step 8** Click **Next**. HP OpenView and NetView are stopped. The Requirements Verification dialog box displays the results of the requirements check and advises whether installation can continue.
- Step 9** When prompted, enter the machine name or IP address of the machine on which the DfmBroker is running (this is normally the machine that is running DFM).



---

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

---

- Step 10** A dialog box appears, asking if you want to connect this instance of DFM with VHM 1.0.



---

**Note** You *must* give the same answer to this question that you gave when installing DFM. If you answered **No** to this question when installing DFM, you *must* provide the same username and password pair that you provided for DFM.

---

Do one of the following:

- If you will be using a remote version of VHM 1.0 with DFM, click **Yes**.  
HP OpenView and NetView are stopped. The Requirements Verification dialog box displays the results of the requirements check and advises whether installation can continue.  
Proceed to [Step 12](#).
  - If you will not be using a remote version of VHM 1.0 with DFM, click **No**.  
Proceed to [Step 11](#).
- Step 11** The Setup window appears. In the username field, enter the DFM username. In the password field, enter the DFM password.



---

**Note** You can change your username and password. Refer to the *User Guide for Device Fault Manager*, available from the online help, for more information.

---

- Step 12** Click **OK**. The installation program copies the files to the directory in which CD One was installed.
- Step 13** Remove the DFM CD-ROM from the drive.

## Installing or Upgrading the HPOV-NetView Adapter on a Remote Host Not Running CiscoWorks

Use this procedure to do the following:

- Install a new HPOV-NetView Adapter on a remote host that is not running CiscoWorks, or
- Upgrade a DFM 1.1 version of the HPOV-NetView Adapter on a remote host that is not running CiscoWorks

If you try to run the DFMadapter.exe script on a host that is running CiscoWorks or DFM, you will receive an error message and the installation will abort.

You do not need to upgrade DFM 1.2 adapters if you are upgrading from DFM 1.2 to DFM 1.2 Updated for Common Services Version 2.2.



### Note

The DFMadapter.exe script does not support reinstallation.

- Step 1** Verify that you have 31 MB of space for installing the adapter.
- Step 2** If you want to upgrade a 1.1 version of the HPOV-NetView Adapter, remove the adapter as described in the [“Removing the HPOV-NetView Adapter from a Remote Host Not Running CiscoWorks”](#) section on page 2-50.
- Step 3** From a temporary directory, use ftp to copy the binary file *NMSROOT\htdocs\rdist\dfm\DFMadapter.exe* from the running DFM. In the following commands, *dfm-host* is where DFM is installed, and *NMSROOT* is the DFM installation directory (normally C:\Program Files\CSCOpX):

```
# cd \Temp
# ftp dfm-host
User (dfm-host:(none)): login
Password: password
ftp> cd NMSROOT\htdocs\rdist\dfm
ftp> get DFMadapter.exe
ftp> quit
```

- Step 4** Double-click **DFMadapter.exe**. The Choose Destination Location window appears.
- Step 5** In the Select Destination Folder field, select **C:\DFM** and click **Next**. The Setup Window appears.
- Step 6** Enter the machine name or IP address of the machine on which the DfmBroker is running (normally the machine that is running DFM).



---

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

---

- Step 7** A dialog box appears, asking if you want to connect this instance of DFM with VHM 1.0.



---

**Note** You *must* give the same answer to this question that you gave when installing DFM. If you answered **No** to this question when installing DFM, you *must* provide the same username and password pair that you provided for DFM.

---

Do one of the following:

- If you will be using a remote version of VHM 1.0 with DFM, click **Yes**.  
The adapter is installed (or upgraded), and HP OpenView and NetView are stopped.  
Proceed to [Step 10](#).
- If you will not be using a remote version of VHM 1.0 with DFM, click **No**.  
Proceed to [Step 8](#).

- Step 8** The Setup window appears. In the username field, enter the DFM username. In the password field, enter the DFM password.



---

**Note** You can change your username and password. Refer to the *User Guide for Device Fault Manager*, available from the online help, for more information.

---

- Step 9** Click **Next**. The adapter is installed (or upgraded), and HP OpenView and NetView are stopped.

- Step 10** Click **Finish**. The Restarting Windows dialog box appears.
- Step 11** Select **Yes** to confirm that you want to reboot, and click **OK**.
- Step 12** Restart HP OpenView or NetView to activate the adapter (using the `ovstart` or `nvstart` command).
- 

CiscoWorks automatically configures the remote adapters to forward SNMP traps from HP OpenView and NetView to DFM.

## Installing or Upgrading the RME Adapter on a Remote Host

This section describes how to install or upgrade the RME Adapter on a remote host so the adapter can exchange information with DFM on a local host. You can also use this procedure to reinstall the RME Adapter.

## Installing or Upgrading the RME Adapter on a Remote DFM Host

Use this procedure to do the following:

- Install a new RME Adapter on a remote host running CiscoWorks, or
- Upgrade a DFM 1.1 version of the RME Adapter on a remote host running CiscoWorks

You do not need to upgrade DFM 1.2 adapters if you are upgrading from DFM 1.2 to DFM 1.2 Updated for Common Services Version 2.2.



### Note

If the DFM broker is moved—for example, if DFM is moved to a different machine, or you want to use a different instance of DFM—you must reinstall the remote adapters.

---

- 
- Step 1** As the local administrator, log on to the machine on which you will install the HPOV-NetView Adapter, and insert the DFM CD-ROM into the CD-ROM drive. (Alternatively, you can install the adapter using DFM 1.2 Patch/IDU 1.2.7 or later.) 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.

---

- Step 2** Click **Install**. The Welcome window appears.
- Step 3** Click **Next**.
- Step 4** If you are upgrading your DFM 1.1 adapter to DFM 1.2 Updated for Common Services Version 2.2, the Software License Agreement window appears. To accept the agreement and continue the installation, click **Yes**.
- Step 5** The Setup Type dialog box appears. Select **Custom** to select a component to install and click **Next**. The Select Components dialog box appears.
- Step 6** Select **Device Fault Manager RME Adapter** and click **Next**. The Start Copying Files dialog box appears.
- Step 7** Click **Next**. The Requirements Verification dialog box displays the results of the requirements check and advises whether installation can continue.
- Step 8** Click **OK**. The installation program copies the files to the CiscoWorks default installation directory C:\Program Files\CSCOPx (*NMSROOT*). The Enter Information window appears, asking you for the name of the machine running the DFM Broker.
- Step 9** Enter the machine name or IP address of the machine on which the DfmBroker is running (this is normally the machine that is running DFM).



---

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

---

**Step 10** A dialog box appears, asking if you want to connect this instance of DFM with VHM 1.0.



---

**Note** You *must* give the same answer to this question that you gave when installing DFM. If you answered **No** to this question when installing DFM, you *must* provide the same username and password pair that you provided for DFM.

---

Do one of the following:

- If you will be using a remote version of VHM 1.0 with DFM, click **Yes**.  
The Restart Windows dialog box appears.  
Proceed to [Step 13](#).
- If you will not be using a remote version of VHM 1.0 with DFM, click **No**.  
Proceed to [Step 11](#).

**Step 11** The Setup window appears. In the username field, enter the DFM username. In the password field, enter the DFM password.



---

**Note** You can change your username and password. Refer to the *User Guide for Device Fault Manager*, available from the online help, for more information.

---

**Step 12** Click **Next**. The Restart Windows dialog box appears.

**Step 13** Select **Yes** and click **OK** to reboot the machine.

**Step 14** Remove the DFM CD-ROM from the drive.

---

After Essentials is installed, CiscoWorks automatically configures the remote adapters to forward Essentials inventory device information to DFM.

If you had any errors during installation (or upgrade), check the installation log in the root directory on the drive. (For example, the CiscoWorks installation might create C:\cw2000\_in001.log, the DFM installation might create C:\cw2000\_in002.log, and so forth.) The Technical Assistance Center (TAC) might ask you to send them the installation log.

# Removing Adapters

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

## Removing the HPOV-NetView Adapter from a Remote Host

You can remove the HPOV-NetView Adapter from remote host machines with or without installed CiscoWorks products.

**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.

## Removing the HPOV-NetView Adapter from a Remote Host Running CiscoWorks

Use this procedure to remove the HPOV-NetView Adapter from a remote host that is running CiscoWorks.

- 
- Step 1** As the local administrator, log on to the system on which the remote HPOV-NetView Adapter is 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 Adapter. Messages appear, showing the progress of the uninstallation, 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 installation might create C:\cw2000\_in001.log, the DFM installation might create C:\cw2000\_in002.log, and so forth.) The Technical Assistance Center (TAC) might ask you to send them the installation log.

## Removing the HPOV-NetView Adapter from a Remote Host Not Running CiscoWorks

Use this procedure to remove the HPOV-NetView Adapter from a remote host that does not contain CiscoWorks. If you try to run the `DFMadapter.exe` on a host that is running CiscoWorks or DFM, you will receive an error message and the uninstallation will abort.

- 
- Step 1** From a temporary directory, use ftp to copy the `NMSROOT\htdocs\rdist\dfm\DFMadapter.exe` binary file from the running DFM. In the following commands, *dfm-host* is where DFM is installed, and *NMSROOT* is the DFM installation directory (normally C:\Program Files\CSCOpX):
- ```
# cd \Temp
# ftp dfm-host
User (dfm-host:(none)): login
Password: password
ftp> cd NMSROOT\htdocs\rdist\dfm
ftp> get DFMadapter.exe
ftp> quit
```
- Step 2** Double-click `DFMadapter.exe`. The Confirm File Deletion window appears.
- Step 3** Click **OK**. The adapter is removed, and HP OpenView and NetView are stopped and restarted. The Setup window appears.
- Step 4** Click **Finish**.
-

## Removing the RME Adapter from a Remote Host

This section describes how to remove the RME Adapter from a remote host.

**Caution**

---

You must use the CiscoWorks uninstallation program to remove the RME Adapter 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 on to the system on which the RME Adapter is 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 RME adapter**.
- Step 3** Click **Next**. The Uninstallation window lists the components selected for removal.
- Step 4** Click **Next** to begin removing the RME Adapter. Messages appear, showing the progress of the uninstallation, and the uninstallation completes.
- 

If you had any errors during installation, check the installation log in the root directory on the drive. (For example, the CiscoWorks installation might create C:\cw2000\_in001.log, the DFM installation might create C:\cw2000\_in002.log, and so forth.) The Technical Assistance Center (TAC) might ask you to send them the installation log.





## Getting Started

---

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



### Note

---

Within DFM are three consoles: the Monitoring Console, the Administration Console, and the Polling and Thresholds Console. The consoles are described in detail in the *User Guide for Device Fault Manager* (available from online help).

---

To start using DFM, you will want to perform most of the steps in these sections:

- [Enabling Devices to Send Traps to DFM, page 3-2](#)
- [Enabling DFM to Send Traps to NMSs, page 3-2](#)
- [Preparing a Seed File, page 3-8](#)
- [Accessing Device Fault Manager, page 3-10](#)
- [Importing Devices from a Seed File, page 3-11](#)
- [Opening the DFM Administration Console, page 3-12](#)
- [Opening the DFM Polling and Thresholds Console, page 3-12](#)
- [Checking Default Settings, page 3-13](#)

- [Accessing the Device Inventory, page 3-13](#)
- [Probing the DFM Inventory, page 3-14](#)
- [Opening the DFM Monitoring Console, page 3-16](#)
- [Closing the DFM Monitoring Console, page 3-17](#)

## Enabling Devices to Send Traps to DFM

Make sure your devices are enabled to send traps to DFM by using the command line or GUI interface appropriate for your device. For example, if you are using Essentials, you can use the NetConfig application.

- For information on enabling traps on IOS-based devices, use the `snmp-server enable traps` command. Refer to the appropriate command reference guide on [cisco.com](http://www.cisco.com):  
<http://www.cisco.com/univercd/cc/td/doc/product/software/index.htm>
- For information on enabling traps on Catalyst devices (which use the Catalyst operating system), use the `set snmp trap` command. Refer to the appropriate command reference guide on [cisco.com](http://www.cisco.com):  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/index.htm>

## Enabling DFM to Send Traps to NMSs

If you want DFM to integrate with other NMSs, you must enable trap forwarding in DFM by performing the tasks outlined in these sections:

1. [Configuring the SNMP Trap Adapter, page 3-3](#)
2. [Integrating the SNMP Trap Adapter with Other Trap Daemons, page 3-5](#)

For more information on configuring adapters, refer to the *User Guide for Device Fault Manager* (available from online help).

## Configuring the SNMP Trap Adapter

The SNMP Trap Adapter listens for traps (from managed devices) on a user-specified port and forwards the traps to specified destinations, providing a generic method for integrating with other NMS applications. If another NMS is already listening for traps on the standard UDP trap port (162), you must configure this adapter to use another port, such as port 9000.

You can use the DFM administration menus to configure the SNMP Trap Adapter to both receive and forward SNMP traps.

### Using the GUI to Configure the SNMP Trap Adapter to Receive Traps

To configure which port will be monitored for SNMP traps DFM receives from other NMSs:

- 
- Step 1** Make sure the devices and/or NMSs that are forwarding traps to DFM are configured to send them to the port defined in the adapter configuration file.  
If another NMS is already listening for traps on the standard UDP trap port (162), you must configure this adapter to use another port, such as port 9000.
  - Step 2** Select **Device Fault Manager > Administration > Trap Configuration > Trap Receiving**.
  - Step 3** In the Listening Port field, enter the port number of the local host where the DFM server is running.
  - Step 4** Select the Restart DFM Server check box if you want to restart the server when you click **OK**. (You must restart the DFM server for your changes to take effect.)
  - Step 5** Click **OK**.
-

This procedure does the following:

- Enables/disables the process and registers/unregisters the process with CiscoWorks. When the process is unregistered, you will no longer see it using **Server Configuration > Administration > Process Management**.
- Updates the SNMP Trap Adapter configuration file `NMSROOT\objects\smarts\conf\trapd\trapd.conf`.
- Saves SNMP Trap Adapter log information in the DFM domain manager log file `NMSROOT\objects\smarts\logs\DFM.log`

If you did not select the Restart DFM Server check box, you must do so manually to apply your changes. Use **Server Configuration > Administration > Process Management**. To further configure the adapter—for example, to specify how nonprintable characters are formatted—use the command line as described in the *User Guide for Device Fault Manager* (available from online help).

You may also need to complete one or more of the following steps:

- If your network devices are already sending traps to another management application, configure that application to forward traps to DFM.
- If your devices are already configured to send traps to port 162, and no other management application is using port 162, then you can configure DFM to listen on port 162 instead of port 9000.
- If your network devices are already sending traps to another NMS, but that NMS cannot forward traps, you should:
  - Configure the devices to send traps to DFM.
  - Configure DFM to forward the traps to the other NMS.

## Using the GUI to Configure the SNMP Trap Adapter to Forward Traps

To have DFM send received traps to other NMSs:

- 
- Step 1** Select **Device Fault Manager > Administration > Trap Configuration > Trap Forwarding**.
- Step 2** In the Forwarding field, select **ON** or **OFF** to enable or disable trap forwarding.
- Step 3** If you want to add a recipient, in the Add Recipient field, enter the hostname and port number of the machine you want to forward traps to.

- Step 4** If you want to remove a recipient, select the recipient from the Remove Recipient field.
- Step 5** Click **OK**.
- Step 6** If you want to add or remove any other recipients, repeat the appropriate steps and click **OK**. Repeat these steps until you have added or removed all recipients.
- Step 7** Select the Restart DFM Server check box if you want to restart the server when you click **OK**. (You must restart the DFM server for your changes to take effect.)
- 

This procedure does the following:

- Enables/disables the process and registers/unregisters the process with CiscoWorks. When the process is unregistered, you will no longer see it using **Server Configuration > Administration > Process Management**.
- Updates the SNMP Trap Adapter configuration file *NMSROOT\objects\smarts\conf\trapd\trapd.conf*.
- Saves SNMP Trap Adapter log information in the DFM domain manager log file *NMSROOT\objects\smarts\logs\DFM.log*

If you did not select the Restart DFM Server check box, you must do so manually to apply your changes. Use **Server Configuration > Administration > Process Management**. To further configure the adapter—for example, to specify how nonprintable characters are formatted—use the command line as described in the *User Guide for Device Fault Manager* (available from online help).

## Integrating the SNMP Trap Adapter with Other Trap Daemons

The SNMP Trap Adapter can receive traps on any port and forward them to a list of devices and ports. This flexibility enables it to easily work with other trap processing applications. The following sections describe possible scenarios for integrating the SNMP Trap Adapter with an existing network management system (NMS) platform.

You may need to complete one or more of the following steps to configure the trap notifier adapter:

- Add the host where DFM is running to the list of trap destinations in your network devices. Specify port 9000 as the destination trap port.
- If your network devices are already sending traps to another management application, configure that application to forward traps to DFM.
- If your devices are already configured to send traps to port 162, and no other management application is using port 162, then you can configure DFM to listen on port 162 instead of port 9000.

## Scenario One

DFM and another NMS are installed on the same host. DFM can be configured to listen for traps on default port 162 and forward them to the NMS, which listens on a nonstandard port, such as port 9000.

The advantages of this approach:

- SNMP Trap Adapter provides a reliable trap reception, storage, 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.

## Scenario Two

DFM and the NMS run on separate hosts. Network devices send traps to port 162 of the host where DFM is running. DFM receives the traps and forwards them to the NMS.

The advantages of this approach:

- SNMP Trap Adapter provides a reliable trap reception, storage, and forwarding mechanism.
- NMS continues to receive traps on port 162.
- Network devices continue to send traps to port 162.

## Scenario Three

DFM and the NMS are installed on the same host. The SNMP Trap Adapter listens for traps on port 9000 and forwards them to the NMS on port 162.

The advantages of this approach:

- SNMP Trap Adapter provides a reliable trap reception, storage, and forwarding mechanism.
- No reconfiguration of the NMS is required; it continues to listen for traps on the default port 162.
- DFM and the NMS run on the same host.

## Scenario Four

DFM and the NMS run on the same host. The NMS receives traps on port 162 and forwards them to the SNMP Trap Adapter, which listens for traps on a nonstandard port such as port 9000.

The advantages of this approach:

- No reconfiguration of the NMS is required.
- No reconfiguration of network devices is required.
- DFM and the NMS run on the same host.
- The SNMP Trap Adapter does not receive traps dropped by the NMS.

## Scenario Five

DFM and the NMS run on separate hosts. The NMS receives traps on the default port of 162 and forwards them to port 162 on the host where DFM is running.

The advantages of this approach:

- No reconfiguration of the NMS is required.
- No reconfiguration of network devices is required.
- The SNMP Trap Adapter does not receive traps dropped by the NMS.

## Preparing a Seed File

When DFM is installed as a standalone product, the device inventory of the network must be imported into DFM from a text file called a seed file. The file can be created with any text editor. Subsequent updates to groups of managed devices can also be performed by way of a seed file. Individual devices can be added using the Add Agent option listed on the Inventory menu of the Administration Console.

A seed file lists top-level network devices such as hosts, routers, switches, and hubs. After the seed file is imported into DFM, DFM automatically discovers the internal structure of the devices. For example, you need only provide the name or IP address of one interface in a router; DFM discovers the rest of the interfaces. In the case of a switch, you need only provide the name or IP address of the switch's SNMP agent. DFM automatically determines the switch's configuration and how it connects to other devices listed in the DFM inventory.

The seed file must be stored on the host on which the domain manager runs. It is recommended that you store it under its default path name, *NMSROOT*\objects\smarts\conf\seedfile.

## Format of a Seed File

A seed file consists of lines with one or two columns. Separate the columns with any combination of spaces and tab characters. The first column names the network device. You can specify either a name or an IP address. You can intermix the two formats freely within a single seed file.

The second column defines the read community string. It is meaningful only if an SNMP agent is accessible at the default SNMP port (UDP port 161) at the name or address given in the first column. If you omit this column, DFM uses a default value; the initial default value is public. If many of your devices use a single alternative read community string, you can change DFM's default (see the [“Changing the Default Read Community String”](#) section on page 3-11 for additional information). To make your seed file more readable, you can include blank and comment lines. A comment line is one that begins with a # sign.

The following offers a brief example of a seed file:

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

The default read community string (public, unless changed) is used for the devices at IP address 192.168.1.200 and at name host1.example.com, because an alternate string is not specified. The read community string for access-router-1 is private, and the read community string for 192.168.2.100 is public, regardless of the default community string.

## How To Determine What to Put in a Seed File

The seed file must list all of the network devices that DFM is to manage. Creating the seed file can be a substantial task if it is done manually. However, the necessary information is usually available from existing computer-accessible sources. This section lists a variety of sources where this information might be found:

- If you are using CiscoWorks with Essentials on another host but do not want to use it to perform automatic updates, you can dump the hardware inventory to a text file. That text file can be converted into a seed file. Similar operations may be possible with other network management platforms.
- If you are using HP OpenView or NetView, you can obtain this information from the ovsnmp.conf file. This configuration file is maintained by the xmmsnmpconf configuration utility. By default, for example, the ovsnmp.conf is located in \usr\OV\conf.
- If you store backup router or switch configuration files at a central location, you can construct a seed file from them.
- Domain name resolution files, such as hosts.txt or zone files, are often a useful source. Note that, at sites with multiple administrative authorities who choose different read community strings, the hosts listed in a given zone file often share an administrative authority and hence a read community string. TACACS configuration files may be useful for similar reasons.

- Large sites usually maintain hardware inventories in a database or at least in some computer-readable form. These inventories often contain the necessary information.
- Some sites run network *sniffer* tools to keep track of active IP addresses. The lists of addresses they generate can form the basis for a seed file.

## Choosing a Router Address for the Seed File: Special Considerations

As noted earlier, only a single name or IP address is necessary for a router. However, if a router is configured to allow SNMP access only on select interfaces, at least one of those interfaces must be listed in the seed file. While only one name or IP address is needed for a given network device, more than one can be listed. DFM automatically determines that the names or addresses actually belong to a single device. In complex network configurations, this capability enables DFM to reach the device using an alternate address if the primary address is inaccessible (due to a failure) during DFM's initial probe of the device. (Once DFM has probed the device successfully, it knows all its IP addresses, and will automatically try them all to route around failures and reach the device.)

## Accessing Device Fault Manager

To access DFM, select one of the following:

- **Device Fault Manager > Monitoring Console** to open the DFM Monitoring Console and check DFM polling and analysis results. For more information, refer to the *User Guide for Device Fault Manager* (available from online help).
- **Device Fault Manager > Administration > Administration Console** to open the Administration Console. For more information, refer to the [“Opening the DFM Polling and Thresholds Console”](#) section on page 3-12.
- From the Administration Console, select **Edit > Polling and Thresholds** to open the Polling and Thresholds Console to browse and fine tune the device inventory of your network. For more information, refer to the [“Opening the DFM Polling and Thresholds Console”](#) section on page 3-12.

# Importing Devices from a Seed File

When DFM is installed as a standalone product, a seed file—or a list of managed devices—must be imported into DFM to initiate inventory discovery.

To import a seed file:

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



---

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

---

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

## Changing the Default Read Community String

DFM uses public as its default read community string to access the SNMP agents of managed devices. You can change the default read community string if the read community string for SNMP agents in your network is different.

- 
- Step 1** Click the domain manager icon.
  - Step 2** Select the Inventory tab in the right panel of the Administration Console.
  - Step 3** Specify a different read community string in the Default Read Community String field.
  - Step 4** Click **Apply** to make the new string take effect.
-

# Opening the DFM Administration Console

To open the Monitoring Console, select **Device Fault Manager > Administration > Administration Console**.

The Administration Console displays an inventory tree that lists system classes and VLANs. Systems include devices such as switches, hubs, bridges, routers, router switch modules, probes, and hosts.

When an instance (managed element) of a class is selected in the left panel, DFM displays the properties of the instance under three tabs:

- Attributes lists the attributes and their values for the selected instance.

**Note**

---

If a line appears in place of an attribute value, the value is derived by polling an external device that is currently unavailable to the domain manager.

---

- Events lists the events that can occur in or affect the instance. Active events are colored according to their type. Double-clicking an event displays the Notification Properties dialog box for the event. For more information regarding the Notification Properties dialog box, see the *User Guide for Device Fault Manager* (available from the online help).
- Group lists the Polling and Threshold groups the instance is a member of and the settings from those groups that apply to the instance.

# Opening the DFM Polling and Thresholds Console

From the Administration Console, select **Edit > Polling and Thresholds** to open the Polling and Thresholds Console.

The Polling and Thresholds Console enables you to display the settings and configurations of the managed devices. It also enables you to display the current device inventory.

Settings are the polling parameters and notification thresholds that are applied to the managed devices of the network. Configuration groups, in turn, are collections of settings that are applied to specified groups of managed devices (hosts and routers, for example).

- 
- Step 1** Click the domain icon that is displayed in the left-hand panel of the window to display the configuration groups of the domain.
  - Step 2** Select and click on a configuration group to display the settings of that group. At this point, you can also display the description, priorities, and matching criteria for the group.
  - Step 3** Review the default information for the domain groups.
- 

For additional information on the Polling and Thresholds Console, see the *User Guide for Device Fault Manager* (available from online help).

## Checking Default Settings

When it is installed, DFM includes default values for all of the configurations and settings used by the application. The default values, however, can be modified to meet the requirements of your environment. For additional information about modifying the configurations and settings, see the *User Guide for Device Fault Manager* (available from online help).

## Accessing the Device Inventory

To access the device inventory of your network, click the domain manager icon displayed in the left panel of the Administration Console to expand the inventory tree.

This inventory tree view enables you to traverse the device inventory that DFM imported from the Essentials database. The view displays the domain manager, its classes, a selected managed element (instance), and that element's relationships to other elements.

For each object you select in the inventory view, a corresponding property sheet appears. The property sheet displays the current value of the element's attributes, its events (highlighting the active ones), and its configuration settings.

In the inventory view:

- Click the plus sign to expand individual objects.
- Click the plus sign next to the domain manager to view the classes (types) of elements it manages.
- Click the plus sign next to a class to view its instances.
- Click an instance to view its properties.
- Click the plus sign next to an instance to view its relations.
- Click the plus sign next to a relation to view the classes of the related objects.
- Click the plus sign next to each class to view the actual related instances.
- Double-click an instance to create a new, separate window that displays an inventory browser starting with the selected object.

For more information on viewing analysis results and other operator tasks, consult the *User Guide for Device Fault Manager* (available from online help).

## Probing the DFM Inventory

After Device Fault Manager is installed, the DFM inventory is regularly probed. These topics provide information on how this is done:

- [Synchronizing the DFM Inventory with the Essentials Inventory, page 3-14](#)
- [Rediscovering Devices in the Entire DFM Inventory, page 3-15](#)

## Synchronizing the DFM Inventory with the Essentials Inventory

When Essentials is installed, DFM (specifically, the DfmChangeProbe process) automatically queries the Essentials database, and sends device information to the DFM repository. DFM then probes the devices to analyze their properties and status.

During normal operation, the DfmChangeProbe process monitors messages that are broadcast by the Essentials inventory collector, and forwards inventory additions and updates to the DFM repository.

To check the status of the DfmChangeProbe process, when necessary, select **Server Configuration > Administration > Process Management > Process Status**.

To disable (or enable) the DfmChangeProbe process, select **Device Fault Manager > Administration > Device Discovery > ChangeProbe**. For more information, see the *User Guide for Device Fault Manager* (available from online help).

**Note**

---

If you delete a device from the DFM inventory, the device is not deleted from the Essentials database. Therefore, when the DfmChangeProbe process again performs a query of the full Essentials database (after a restart of the system, for example), the deleted device is again added to the DFM repository.

---

## Rediscovering Devices in the Entire DFM Inventory

In addition to the initial inventory probe, DFM includes a scheduled probe of the entire inventory. The scheduled probe is a batch process that is controlled by CiscoWorks. By default, the probe of the entire inventory is scheduled to run once a week, on Saturday night or Sunday morning. After the probe of the entire inventory, the DFM inventory is also synchronized with the Essentials inventory, and DFM is directed to rediscover the managed devices.

To check the status of a scheduled probe of the inventory, when necessary, select **Server Configuration > Administration > Job Management**.

To change the date, time, and duration of inventory collection, use the Rediscovery Schedule option:

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

If the Rediscovery Schedule job is stopped by the CiscoWorks Job Manager, you must remove the job and then schedule discovery again.

To remove the job:

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

For more information on rediscovering devices in the DFM inventory, refer to the *User Guide for Device Fault Manager* (available from online help).

## Opening the DFM Monitoring Console

To open the Monitoring Console, select **Device Fault Manager > Monitoring Console**.

The Monitoring Console displays the results of DFM's polling and analysis of the managed devices. The Console automatically receives and displays notifications in the Alarm Log view.



### Note

---

When you open a Monitoring Console using the CiscoWorks navigation tree, by default the Monitoring Console does *not* display the Inventory Browser. If you want to open a Monitoring Console that displays the Inventory Browser, either (1) open a Monitoring Console using the Administration Console's toolbar button, or (2) open a Monitoring Console from any running console in a session using **File > New > Monitoring Console**.

---

As exceptional conditions occur across the network, notifications begin to appear in the Alarm Log view of the Monitoring Console. In the Alarm Log view, information presented for the notifications includes class (or type) of managed element, name of managed element, name of notified event, certainty of diagnosis, number of times the event occurred, last change (of state), first notification (the time the event was first detected), and the name of the domain manager.

To view possible causes or events used in the analysis, double-click the notification in the Alarm Log. This displays the Notification Properties window.

The Notification Properties window displays the selected event notification, the name of the device associated with the notification, the general properties of that device, and any associated component notifications. Thus, it provides you with the information that you need to resolve the problem.

For additional information on the Monitoring Console, see the *User Guide for Device Fault Manager* (available from online help).

## Closing the DFM Monitoring Console

Three methods exist to close the Monitoring Console (none affect the domain manager):

- Select **File>Close**.

The Close command closes an individual Console and the session continues. When you close the last Monitoring Console, you end the DFM session.

- Select **File>Exit**.

The Exit command closes all consoles that are part of the session, and the session ends.

- Close your Web browser.



---

**Note**

When you log out of CiscoWorks, the Monitoring Console remains displayed for continuous viewing. To close the Console, you must explicitly close it or the Web browser.

---





---

## Symbols

\$NMSROOT [2-4](#), [2-5](#), [2-15](#)

---

## A

### adapters

configuring [2-40](#)

installing [1-2](#), [1-13](#), [2-38 to 2-48](#)

local [2-38](#)

remote [2-39](#)

starting [2-40](#)

upgrading [2-38 to 2-48](#)

### adapters, local

configuring and starting [2-40](#)

File Notifier adapter [2-38](#)

HPOV-NetView adapter [2-39](#)

installing [2-40](#)

Mail Notifier adapter [2-38](#)

RME adapter [2-39](#)

SNMP Trap adapter [1-21](#), [2-38](#), [3-2 to 3-7](#)

Trap Notifier adapter [2-38](#)

### adapters, remote

configuring and starting [2-40](#)

HPOV-NetView adapter [1-22](#), [2-39](#)

installing [2-41 to 2-48](#)

removing [2-49 to 2-51](#)

RME adapter [2-39](#)

upgrading [2-32](#), [2-38 to 2-48](#)

Administration Console [3-10](#), [3-13](#)

Attributes tab [3-12](#)

Events tab [3-12](#)

Group tab [3-12](#)

layout [3-12](#)

audience for this document [ix](#)

---

## B

bundles, DFM and [1-15](#)

---

## C

### cautions

significance of [x](#)

CD One, supported versions [1-14](#)

Cisco.com, accessing [xiv](#)

client requirements [1-19](#)

Common Services, supported versions [1-14](#)

## console

- Administration Console [3-10](#)
  - Attributes tab [3-12](#)
  - Events tab [3-12](#)
  - Group tab [3-12](#)
  - layout [3-12](#)
- Monitoring Console [3-10, 3-16, 3-17](#)
- Polling and Thresholds Console [3-10, 3-12](#)

**D**

## default

- installation directory [2-4, 2-5, 2-15](#)
- settings [3-13](#)

devices, supported [1-22](#)device traps, enabling [3-2, 3-2 to 3-7](#)

## DFM

- accessing [3-10](#)
- installing [2-2 to 2-12](#)
  - installing DFM 1.2 [2-2 to 2-9](#)
  - installing DFM 1.2 Updated for Common Services Version 2.2 [2-9 to 2-12](#)
- inventory and Essentials
  - inventory [3-14 to 3-16](#)
- reinstalling [2-27 to 2-36](#)
  - reinstalling DFM 1.2 [2-27 to 2-33](#)
  - reinstalling DFM 1.2 Updated for Common Services Version 2.2 [2-33 to 2-36](#)
- removing [2-37](#)

## DFM (continued)

- upgrading [2-12 to 2-26](#)
  - upgrading DFM 1.1 to DFM 1.2 [2-12 to 2-20](#)
  - upgrading DFM 1.1 to DFM 1.2 Updated for Common Services Version 2.2 [2-20 to 2-22](#)
  - upgrading DFM 1.2 [2-23](#)

## DfmBroker

- limiting access [2-5, 2-16, 2-30](#)
- port change after upgrade [2-16, 2-18](#)
- specifying new DFM [2-41, 2-46](#)
- specifying remote HPOV-NetView adapter [2-43, 2-45](#)
- specifying remote RME adapter [2-47](#)

## documentation

- feedback, submitting electronically [xv](#)
- obtaining [xiv](#)
  - CD-ROM [xiv](#)
  - Cisco.com [xiv](#)
  - ordering [xv](#)
- other Cisco publications and information [xviii](#)
- product [x to xii](#)

**F**File Notifier adapter [2-38](#)

---

**H**help [xvi](#)Cisco.com [xvi](#)TAC [xvi](#)Escalation Center [xviii](#)website [xvii](#)

HP OpenView

supported versions [1-21](#)HPOV-NetView adapter [1-13](#)local [2-39](#)remote [1-22, 2-39, 2-42 to 2-46](#)

---

**I**importing devices [3-11](#)

installation

default directory [2-4, 2-5, 2-15](#)paths [1-13](#)preparation [1-13](#)roadmap [1-3 to 1-13](#)

installing

adapters [2-38 to 2-48](#)DFM [2-2 to 2-12](#)installing DFM 1.2 [2-2 to 2-9](#)installing DFM 1.2 Updated for Common  
Services Version 2.2 [2-9 to 2-12](#)DFM with a bundle [1-15](#)remote adapters [2-39](#)integrating with other trap daemons [3-5](#)

inventory

accessing [3-13](#)rediscovering devices [3-14 to 3-16](#)scheduling probes [3-14 to 3-16](#)inventory browser layout [3-12](#)

---

**L**

logs

DFM installation [2-9, 2-20, 2-26](#)DFM reinstallation [2-33](#)HPOV-NetView remote adapter  
uninstallation [2-50](#)RME remote adapter installation [2-48](#)RME remote adapter uninstallation [2-51](#)

---

**M**Mail Notifier adapter [2-38](#)Monitoring Console [3-10](#)closing [3-17](#)opening [3-16](#)

---

**N**NetView versions [1-21](#)NMS integration, supported [1-21](#)NMSROOT [2-4, 2-5, 2-15](#)

---

**O**

OpenView (HP) versions [1-21](#)  
overview  
    DFM [1-2](#)  
    installation and upgrade [1-3 to 1-13](#)  
    product [1-2](#)  
    upgrade [1-5, 1-8](#)

---

**P**

Polling and Thresholds Console [3-10](#)  
ports  
    DfmBroker, after upgrade [2-16, 2-18](#)  
    maximum supported [1-14](#)  
    occupied [1-22, 2-8, 2-19](#)  
    supported [1-14](#)  
preparing to install DFM [1-13](#)  
    client requirements [1-19](#)  
    installation paths [1-13](#)  
    server requirements and  
        recommendations [1-14](#)  
    supported devices [1-22](#)  
    supported NMS integration [1-21](#)  
    supported NMSs for device import [1-21](#)  
probes, scheduling [3-14 to 3-16](#)

---

**R**

recommendations  
    client [1-19](#)  
    ports, supported [1-14](#)  
    server [1-16, 1-17](#)  
rediscovery, scheduling [3-14 to 3-16](#)  
reinstalling  
    DFM [2-27 to 2-36](#)  
        DFM 1.2 Updated for Common Services  
        Version 2.2 [2-33 to 2-36](#)  
        reinstalling DFM 1.2 [2-27 to 2-33](#)  
removing  
    DFM [2-37](#)  
    remote adapters [2-49 to 2-51](#)  
Resource Manager Essentials  
    inventory and DFM [3-14 to 3-16](#)  
    supported versions [1-14](#)  
RME adapter [1-13, 1-21](#)  
    local [2-39](#)  
    remote [2-39, 2-46 to 2-48, 2-51](#)

---

**S**

security  
    new installation [2-5](#)  
    reinstallation [2-30](#)  
    upgrade [2-16](#)

seed file

- contents [3-9](#)
- format [3-8](#)
- importing devices from [3-11](#)
- preparing [3-8](#)

server

- limiting access [2-5, 2-16, 2-30](#)
- requirements [1-14](#)

SNMP Trap adapter [1-21, 2-38, 3-3 to 3-7](#)

- and occupied ports [3-3](#)
- configuring [3-3 to 3-5](#)
- integration with other trap daemons [3-5](#)

supported

- client environments [1-19](#)
- devices [1-22](#)
- Essentials versions [1-21](#)
- HP OpenView versions [1-21](#)
- NetView versions [1-21](#)
- NMS integration [1-21](#)
- ports, number of [1-14](#)
- server environments [1-16, 1-17](#)

supported devices [1-22](#)

---

## T

TAC (Technical Assistance Center) [xvi](#)

- Escalation Center [xviii](#)
- website [xvii](#)

technical support [xvi](#)

- Cisco.com [xvi](#)
- TAC [xvi](#)
  - Escalation Center [xviii](#)
  - website [xvii](#)

Trap Notifier adapter [2-38](#)

traps

- and remote hosts [2-38 to 2-39](#)
- changing port [1-22](#)
- converting DFM notifications to SNMP traps [2-38](#)
- enabling devices to send to DFM [3-2](#)
- forwarding from DFM [3-2 to 3-5](#)
- receiving by DFM [3-3 to 3-4](#)

typographical conventions used in this document [ix to x](#)

---

## U

uninstalling DFM [2-37](#)

upgrading

- and DFM broker port [2-18](#)
- and occupied ports [2-19](#)
- and remote adapters [2-19](#)
- DFM [2-12 to 2-26](#)
  - upgrading DFM 1.1 to DFM 1.2 [2-12 to 2-20](#)
  - upgrading DFM 1.1 to DFM 1.2 Updated for Common Services Version 2.2 [2-20 to 2-22](#)
  - upgrading DFM 1.2 [2-23](#)

upgrading (continued)

exporting DFM information to upgraded  
remote DFM host [2-24 to 2-26](#)

restored files [2-20](#)