



Installation and Setup Guide for Device Fault Manager on Solaris

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-7816268=
Text Part Number: 78-16268-01



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.

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

All other trademarks mentioned in this document or Website 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. (0411R)

Installation and Setup Guide for Device Fault Manager on Solaris

Copyright © 2000-2005 Cisco Systems, Inc.

All rights reserved.

The Software may contain certain software and related user documentation (e.g., Crystal Enterprise Professional, Crystal Reports Professional and/or Crystal Analysis Professional) that are owned by Crystal Decisions, Inc., 895 Emerson Street, Palo Alto, CA 94301 ("Crystal Decisions"). All such software products are the technology of Crystal Decisions. The use of all Crystal Decisions software products is subject to a separate license agreement included with the Software electronically, in written materials, or both. YOU MAY NOT USE THE CRYSTAL DECISIONS SOFTWARE UNLESS AND UNTIL YOU READ, ACKNOWLEDGE AND ACCEPT THE TERMS AND CONDITIONS OF THE CRYSTAL DECISIONS' SOFTWARE LICENSE AGREEMENT. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE CRYSTAL DECISIONS' SOFTWARE LICENSE, YOU MAY RETURN, WITHIN THIRTY (30) DAYS OF PURCHASE, THE MEDIA PACKAGE AND ALL ACCOMPANYING ITEMS (INCLUDING WRITTEN MATERIALS AND BINDERS OR OTHER CONTAINERS) RELATED TO THE CRYSTAL DECISIONS' TECHNOLOGY, TO SMARTS FOR A FULL REFUND; OR YOU MAY WRITE, CRYSTAL WARRANTIES, P.O. BOX 67427, SCOTTS VALLEY, CA 95067, U.S.A.

GNU eTeks PJA Toolkit

Copyright © 2000-2001 Emmanuel PUYBARET/eTeks info@eteks.com. All Rights Reserved.

The eTeks PJA Toolkit is resident on the CD on which the Software was delivered to you. Additional information is available at eTEKS' web site: <http://www.eteks.com>. The eTeks PJA Toolkit program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License (GPL) as published by the Free Software Foundation; version 2 of the License. The full text of the applicable GNU GPL is available for viewing at <http://www.gnu.org/copyleft/gpl.txt>. You may also request a copy of the GPL from the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA. The eTeks PJA Toolkit program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

For a period of three years from the date of your license for the Software, you are entitled to receive under the terms of Sections 1 and 2 of the GPL, for a charge no more than SMARTS' cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code for the GNU eTeks PJA Toolkit provided to you hereunder by requesting such code from SMARTS in writing: Attn: Customer Support, SMARTS, 44 South Broadway, White Plains, New York 10601.

IBM Runtime for AIX

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

HP-UX Runtime Environment for the Java™ 2 Platform

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

DataDirect Technologies

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

NetBSD

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

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

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

RSA Data Security, Inc.

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

AES

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

License Terms:

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

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
 2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
 3. the copyright holder's name is not used to endorse products built using this software without specific written permission.
- ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

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



Preface xi

- Audience xi
- Conventions xi
- Product Documentation xii
- Related Documentation xiv
- Additional Information Online xv
- Obtaining Documentation xvi
 - Cisco.com xvi
 - Ordering Documentation xvi
- Documentation Feedback xvii
- Obtaining Technical Assistance xvii
 - Cisco Technical Support Website xviii
 - Submitting a Service Request xviii
 - Definitions of Service Request Severity xix
- Obtaining Additional Publications and Information xx

CHAPTER 1

Prerequisites 1-1

- Product Overview 1-1
- Installation and Upgrade Paths 1-3
 - Installation Paths 1-3
 - Upgrade Paths 1-5

- Server Requirements and Recommendations 1-8
 - Minimum Server Requirements 1-8
 - Server Recommendations 1-9
 - Solaris Patches 1-10
- Client Requirements 1-11
- Supported NMS Environments for Device Import 1-13
- Supported NMS Integration 1-14
- Supported Devices 1-15
 - Number of Ports/Interfaces that DFM Supports 1-16

CHAPTER 2

Installing and Uninstalling DFM 2-1

- Preparing to Install DFM 2-1
 - Verifying TCP and UDP Ports that DFM Uses 2-2
 - Gathering Information to Provide During Installation 2-3
- Performing a New Installation 2-4
- Reinstalling DFM 2-11
- Uninstalling DFM 2-15
- Installing and Upgrading HPOV-NetView Adapters 2-16
 - Reinstalling the HPOV-NetView Adapters on a Local Host 2-17
 - Installing or Upgrading the HPOV-NetView Adapters on a Remote Host Running CiscoWorks 2-17
 - Installing or Upgrading the HPOV-NetView Adapters on a Remote Host Not Running CiscoWorks 2-18
- Uninstalling the HPOV-NetView Adapters 2-20
 - Uninstalling the HPOV-NetView Adapters from a Remote Host Running CiscoWorks 2-21
 - Uninstalling the HPOV-NetView Adapters from a Remote Host Not Running CiscoWorks 2-22

CHAPTER 3**Upgrading DFM 3-1**

Upgrade Overview 3-1

Local Upgrade 3-2

Procedure for Local Upgrade 3-2

Data that Is Migrated by a Local Upgrade 3-2

Remote Upgrade 3-5

Procedure for Remote Upgrade 3-5

Data that Is Migrated by a Remote Upgrade 3-5

Preparing to Upgrade DFM 3-6

Upgrading to DFM 2.0 3-7

Performing a Local Upgrade 3-8

Performing a Remote Upgrade 3-11

Validating the Upgrade 3-11

Exporting DFM 1.2.x Information to an Upgraded Remote Host 3-12

Post-Upgrade Steps 3-13

CHAPTER 4**Getting Started 4-1**

Configuration Roadmap 4-1

Using the CiscoWorks Home Page 4-3

Registering Applications with the CiscoWorks Home Page 4-3

Understanding and Configuring Security 4-4

Managing Device Credentials 4-5

Performing Device Management 4-6

Importing Devices to the Device and Credentials Repository 4-6

Adding Devices to DFM 4-6

Verifying Devices Added to DFM 4-7

Viewing the Device Summary 4-7

Viewing Device Details 4-8

- Viewing Discovery Status 4-9
- Troubleshooting Device Discovery 4-10
- Configuring SNMP Trap Receiving and Forwarding 4-13
 - Updating the SNMP Trap Receiving Port 4-13
 - Enabling Devices to Send Traps to DFM 4-13
 - Enabling Cisco IOS-Based Devices to Send Traps to DFM 4-14
 - Enabling Catalyst Devices to Send SNMP Traps to DFM 4-14
 - Integrating DFM Trap Receiving with Other NMSs or Trap Daemons 4-15
 - Scenarios—DFM Receives SNMP Traps and Forwards Them to an NMS 4-16
 - Scenarios—An NMS Receives SNMP Traps and Forwards Them to DFM 4-17
 - Configuring SNMP Trap Forwarding 4-18
- Viewing Alerts 4-18
- Starting DFM 4-18
- What Next? 4-19

APPENDIX A

Mounting and Unmounting on Solaris A-1

- Mounting a Local CD-ROM Drive A-1
- Mounting a Remote CD-ROM Drive A-3
- Unmounting a CD-ROM Drive A-5
 - Unmounting a Local CD-ROM Drive A-5
 - Unmounting a Remote CD-ROM Drive A-6

APPENDIX B

Licensing B-1

- Licensing Overview B-1
- Licensing for a Fresh Installation B-2
 - Registering Your License B-3
- Upgrading Your Evaluation License B-4

Validating Your Upgrade License	B-4
Licensing Reminders	B-5
Evaluation Version: Before Expiry	B-5
Purchased Version: No License File	B-5
Restricted Version: Device Limit Exceeded	B-6

APPENDIX C**How is DFM 2.0 Different from DFM 1.2.x?** C-1

What's New in DFM 2.0?	C-2
Behavior Changes	C-3
User Interface Changes	C-4
Terminology Changes	C-9
Device Group Changes	C-10
Protocol Support Updates	C-11

APPENDIX D**Configuring DFM with Cisco Secure ACS** D-1

CiscoWorks Login Module	D-1
CiscoWorks Server Authentication Roles	D-3
Before You Begin: Integration Notes	D-4
Configuring DFM on Cisco Secure ACS	D-6
Verifying the DFM and Cisco Secure ACS Configuration	D-6

INDEX



Preface

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

Audience

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

Conventions

This document uses the following conventions:

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

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

**Note**

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

**Caution**

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

Product Documentation

**Note**

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

[Table 1](#) describes the product documentation that is available.

Table 1 Product Documentation

Document Title	Available Formats
<i>Release Notes for Device Fault Manager 2.0 on Solaris</i>	<ul style="list-style-type: none"> Printed document that was included with the product. On Cisco.com at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm20/rel_note/index.htm
<i>Installation and Setup Guide for Device Fault Manager on Solaris</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm20/install/index.htm Printed document available by order (part number DOC-7816268=).¹
<i>User Guide for Device Fault Manager</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm20/ug/index.htm Printed document available by order (part number DOC-7816266=).¹
<i>Supported Device Table for DFM 2.0</i>	<ul style="list-style-type: none"> On Cisco.com at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dev_sup/index.htm
Context-sensitive online help	<ul style="list-style-type: none"> Select an option, then click Help.

1. See [Obtaining Documentation](#), page xvi.

Related Documentation


Note

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

[Table 2](#) describes the additional documentation that is available.

Table 2 *Related Documentation*

Document Title	Available Formats
<i>Quick Start Guide for LAN Management Solution 2.5</i>	<ul style="list-style-type: none"> Printed document that was included with the product. On Cisco.com at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/lms/index.htm
<i>Release Notes for CiscoWorks Common Services 3.0 (Includes CiscoView 6.1) on Solaris</i>	<ul style="list-style-type: none"> Printed document that was included with the product. On Cisco.com at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser30/relnotes/cwcs_rns.htm
<i>Installation and Setup Guide for Common Services (Includes CiscoView) on Solaris</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser30/ig_sol/index.htm Printed document available by order (part number DOC-7815885=).¹
<i>User Guide for CiscoWorks Common Services</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser30/usrguide/index.htm Printed document available by order (part number DOC-7816571=).¹

1. See [Obtaining Documentation](#), page xvi.

Additional Information Online

**Note**

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

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

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

**Note**

You cannot download DFM IDUs/service packs using the following Software Center options: Device Update and Scheduled Device Download.

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

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

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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 Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

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

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

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



Note

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

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- 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://cisco.com/univercd/cc/td/doc/pcat/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>

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

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

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

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



Prerequisites

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

- [Product Overview, page 1-1](#)
- [Installation and Upgrade Paths, page 1-3](#)
- [Server Requirements and Recommendations, page 1-8](#)
- [Client Requirements, page 1-11](#)
- [Supported NMS Environments for Device Import, page 1-13](#)
- [Supported NMS Integration, page 1-14](#)
- [Supported Devices, page 1-15](#)

Product Overview

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

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

Installation Option	Installation Option Components
Device Fault Manager 2.0	<p>This option is available when DFM 2.0 has not been installed on the local system. It is normally chosen to install the entire DFM product on the local system, including:</p> <ul style="list-style-type: none"> • DFM—Provides the graphical user interface (GUI) and back-end processes for DFM. • HPOV-NetView adapters for integrating DFM with HP OpenView and NetView, if already installed on the same box.
Device Fault Manager HPOV-NetView adapters	<p>This option is available whether or not DFM 2.0 is already installed on the local system. However, when this option is selected, it will install only the HPOV-NetView adapters, not the entire DFM product.</p> <p>This option is normally chosen to install the adapters on a remote machine running HP OpenView or NetView, to forward traps from these remote network management systems (NMSs) to a local DFM. For information on how to configure and start these adapters, see Installing and Upgrading HPOV-NetView Adapters, page 2-16.</p>

Installation and Upgrade Paths

This section outlines the steps for installing and upgrading DFM 2.0.

Installation Paths

You must install DFM 2.0 on a system with CiscoWorks Common Services 3.0. You can install DFM 2.0 on a system with:

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

**Note**

If you are installing DFM with the contents of a Cisco product bundle, see the quick start guide for the appropriate bundle for the order in which to install each application in the bundle.

- Another NMS, such as NetView or HP OpenView.

Before you install DFM, you should determine whether you will install DFM as a standalone or with other products. For more information, see [Server Requirements and Recommendations, page 1-8](#).

Whether DFM is installed as a standalone or not, you can integrate it with:

- Other CiscoWorks applications from a Cisco product bundle to share a Device and Credentials Repository (DCR). For more information, see [Supported NMS Environments for Device Import, page 1-13](#).
- Another NMS to receive SNMP traps from it. For more information, see [Supported NMS Integration, page 1-14](#).

[Table 1-2](#) lists the basic installation sequence.

Table 1-2 Installation Roadmap

	Description	References
Step 1	Install Common Services.	<i>Installation and Setup Guide for Common Services (Includes CiscoView) on Solaris</i>
Step 2	<p>If you want to install DFM on a system with an NMS (HP OpenView or NetView), install the NMS.</p> <p>Note If the desired NMS is not installed before DFM, you will have to reinstall DFM later (after you install the NMS).</p>	<ul style="list-style-type: none"> For supported versions of NMSs, see Supported NMS Integration, page 1-14 For installation instructions, see vendor documentation
Step 3	<p>If you want to install DFM on a system with the contents of a Cisco product bundle:</p> <ol style="list-style-type: none"> Check the quick start guide for the order of installation. Install any products that should be installed before DFM. 	<i>Quick Start Guide for LAN Management Solution 2.5</i>
Step 4	<p>Install DFM.</p> <p>Note If you are using Access Control Server (ACS) mode for your security, you will be warned that if you configured any custom ACS roles, they will be lost unless you exit the installation and change the AAA security mode to CiscoWorks Local. You should revert to ACS mode when the installation is completed.</p>	Performing a New Installation, page 2-4
Step 5	If HP OpenView or NetView is installed on a remote system <i>and</i> you want DFM to receive SNMP traps from one of them, install the HPOV-NetView adapters on the remote system.	Installing and Upgrading HPOV-NetView Adapters, page 2-16

Table 1-2 Installation Roadmap (continued)

	Description	References
Step 6	If HP OpenView or NetView is installed on the same system as DFM <i>and</i> uses the standard UDP trap port (162), you must configure DFM SNMP trap receiving to use a different UDP port, such as port 9000.	Integrating DFM Trap Receiving with Other NMSs or Trap Daemons, page 4-15.
Step 7	If you want a standalone DFM to access the DCR on a remote system (to share the device list across applications from a Cisco product bundle): <ol style="list-style-type: none"> a. Configure DCR on one system (local or remote) as a master. b. Configure DCR on the other system as a slave. 	<ul style="list-style-type: none"> • Supported NMS Environments for Device Import, page 1-13 • Managing Device Credentials, page 4-5

Upgrade Paths

You must upgrade DFM 2.0 on a system with Common Services 3.0. You can perform a local in-place upgrade from DFM 1.2.x or a remote upgrade. (For more information, see [Upgrading to DFM 2.0, page 3-7.](#))

After the upgrade, whether DFM 2.0 is installed as a standalone or not, you can integrate it with:

- Other CiscoWorks applications from a Cisco product bundle to share a Device and Credentials Repository (DCR). For more information, see [Supported NMS Environments for Device Import, page 1-13.](#)
- Another NMS to receive SNMP traps from it. For more information, see [Supported NMS Integration, page 1-14.](#)

[Table 1-3](#) lists the basic upgrade sequence.

Table 1-3 Upgrade Roadmap


	Description	References
Step 1	<p>Upgrade Common Services.</p>  <p>Caution If you are upgrading your operating system from Solaris 2.8 to Solaris 2.9, run the upgrade script on Solaris 2.8 (<i>before</i> migrating your operating system). Otherwise the upgrade script will fail. If you are not upgrading from Solaris 2.8 to Solaris 2.9, you should upgrade your operating system, do so before upgrading Common Services.</p>	<i>Installation and Setup Guide for Common Services (Includes CiscoView) on Solaris</i>
Step 2	<p>If you want to upgrade DFM on a system with an NMS (HP OpenView or NetView), do one of the following:</p> <ul style="list-style-type: none"> • If the NMS is already installed, determine whether to upgrade it and do so if required. • Install the NMS. <p>Note If the NMS is not installed before DFM, you will have to reinstall DFM later (after you upgrade or install the NMS).</p>	<ul style="list-style-type: none"> • For supported versions of NMSs, see Supported NMS Integration, page 1-14 • For installation instructions, see vendor documentation
Step 3	<p>If you want to upgrade DFM on a system with the contents of a Cisco product bundle:</p> <ol style="list-style-type: none"> a. Check the quick start guide for the order of installation. b. Install any products that should be installed before DFM. 	<i>Quick Start Guide for LAN Management Solution 2.5 (Maintenance Kit)</i>

Table 1-3 Upgrade Roadmap (continued)

	Description	References
Step 4	<p>Upgrade DFM.</p> <p>Note If you are performing a remote upgrade, you may want to download the DFM Upgrade Kit from Cisco.com.</p> <p>Note If you are using ACS mode for your security, you will be warned that if you configured any custom ACS roles, they will be lost unless you exit the installation and change the AAA security mode to CiscoWorks Local. You should revert to ACS mode when the installation is completed.</p>	<p>Upgrading to DFM 2.0, page 3-7</p> <p>Remote Upgrade, page 3-5</p> <p>Upgrading to DFM 2.0, page 3-7</p>
Step 5	If HP OpenView or NetView is installed on a remote system <i>and</i> you want DFM to receive SNMP traps from one of them, install or upgrade the HPOV-NetView adapters on the remote system.	<ul style="list-style-type: none"> • Installing and Upgrading HPOV-NetView Adapters, page 2-16 • Integrating DFM Trap Receiving with Other NMSs or Trap Daemons, page 4-15
Step 6	If HP OpenView or NetView is installed on the same system as DFM <i>and</i> uses the standard UDP trap port (162), you must configure DFM SNMP trap receiving to use a different UDP port, such as port 9000.	Integrating DFM Trap Receiving with Other NMSs or Trap Daemons, page 4-15.
Step 7	<p>If you want a standalone DFM to access the DCR on a remote system (to share the device list across applications from a Cisco product bundle):</p> <ol style="list-style-type: none"> Configure DCR on one system (local or remote) as a master. Configure DCR on the other system as a slave. 	<ul style="list-style-type: none"> • Supported NMS Environments for Device Import, page 1-13 • Managing Device Credentials, page 4-5

Server Requirements and Recommendations

This section describes the server requirements and recommendations for Common Services and DFM 2.0.


Note

If you are installing DFM with the contents of a Cisco product bundle, the server requirements might be different. See the quick start guide for the appropriate bundle for additional information.

Minimum Server Requirements

The minimum system requirements for a CiscoWorks server running Common Services 3.0 and Device Fault Manager 2.0 are shown in [Table 1-4](#).

Table 1-4 Server System Minimum Requirements

Requirement Type	Minimum Requirements
System hardware	<ul style="list-style-type: none"> • Sun UltraSPARC IIIi¹ with two 1-GHz CPUs. • 17-inch color monitor. • CD-ROM drive.
System software	Solaris 2.8 or Solaris 2.9. Note DFM supports only US-English and Japanese language versions of Solaris operating systems. Set the default locale to US-English for the US-English version and Japanese for the Japanese version.
Available memory (RAM)	2 GB.
Available disk space	<ul style="list-style-type: none"> • 4 GB on the partition on which you install the product. The default partition is /opt.² • Swap space equal to double the amount of memory (RAM). For example, if your system has 2 GB of RAM, you need 4 GB of swap space.

Table 1-4 Server System Minimum Requirements (continued)

Requirement Type	Minimum Requirements
Additional required software	Common Services must be installed before you install DFM. For installation instructions, see <i>Installation and Setup Guide for Common Services on Solaris</i> .
Additional optional software	To use the desktop on the server system, you need one of the following browsers: <ul style="list-style-type: none"> • Netscape Navigator 7.0—Use Netscape Navigator downloaded from Sun website <i>only</i>. • Mozilla 1.7.

1. DFM supports Sun SPARC Ultra III machines, such as Sun Fire V440.
2. DFM 2.0 is installed in the same directory as Common Services.

**Caution**

Do not use nonstandard Java options through the JAVA_OPTIONS environment variable.

To verify the amount of available disk space in each of the specified partitions and directories, enter:

```
# df -k directory
```

where *directory* is the partition or directory for which you want to check the available disk space.

Server Recommendations

To select or configure a server system that best meets your needs, consider the number of ports and interfaces being managed. (For the maximum number of ports and interfaces, see [Number of Ports/Interfaces that DFM Supports, page 1-16.](#))

**Note**

If you choose to automatically synchronize DFM device inventory with the Common Services Device and Credentials Repository (DCR) and the synchronization causes DFM to exceed the limits, DFM stops adding devices to the managed inventory. (See [Supported NMS Environments for Device Import, page 1-13.](#))

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

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

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

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

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

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

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

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

Solaris Patches

[Table 1-5](#) lists the required and recommended patches for Solaris 2.8 and 2.9. Use the `showrev -p` command to verify that these patches have been applied.

**Note**

The patches listed in [Table 1-5](#) might be made obsolete by new patches.

Table 1-5 **Solaris Patches**

Operating System	Required Server Patches	Required Client Patches	Recommended Server Patches	Recommended Client Patches
Solaris 2.8	111327-05	111626-03	110951-01	110951-05
	110945-08	108652-81	110662-02	110662-12
	110934-16	108921-21	110615-01	110615-11
	110898-09	108940-62	110286-02	108964-06
	109326-14			
	108827-40			
	108528-29			
Solaris 2.9	114224-01	112771-14	113326-01	112808-06
	113580-01	112661-06	112998-03	
	112839-04	113244-05	113713-14	
	112233-12		112964-07	
	114006-01		113575-05	
			112970-07	

Client Requirements

The minimum system requirements for the CiscoWorks client are shown in [Table 1-6](#).

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

Table 1-6 Client System Requirements Summary

Requirement Type	Minimum Requirements
System hardware and software	<ul style="list-style-type: none"> • One of the following client systems: <ul style="list-style-type: none"> – IBM system with at least a 1 GHz Pentium processor running Windows 2000 (Professional and Server) with Service Pack 3¹ or Service Pack 4; Windows XP with Service Pack 1 or Service Pack 2; or Windows Server 2003 Standard or Enterprise Edition. – Sun SPARC Ultra 10 running Solaris 2.8 or Solaris 2.9. <p>DFM supports only US-English and Japanese versions of the Windows Operating System (OS) and the Solaris OS. Set the default locale to US-English for the US-English OS, and Japanese for the Japanese OS.</p> <ul style="list-style-type: none"> • Color monitor with video card set to 24 bits color depth.
Available memory (RAM)	512 MB.
Available disk space	1 GB swap space. Note Swap space should be equal to twice the amount of RAM.
Browser	One of these browsers: <ul style="list-style-type: none"> • On Windows clients: <ul style="list-style-type: none"> – Microsoft Internet Explorer 6.0 with Service Pack 1, Java Virtual Machine (JVM) 5.0.0.3802 and later, and (optional) Java Plug-in version 1.4.2_04. <p>To verify the JVM: From Internet Explorer, select View > Java Console. From Netscape Navigator, select Tools > Server > Java Console.</p> – Netscape Navigator 7.1 for Windows. – Mozilla 1.7.1. • On Solaris clients: <ul style="list-style-type: none"> – Netscape Navigator 7.0 for Solaris 2.8 or 2.9. – Mozilla 1.7 for Solaris 2.8 and 2.9. <p>For Solaris, use Netscape Navigator downloaded from the Sun website only.</p>

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

Supported NMS Environments for Device Import

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

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

- Using DCR, you can import devices from:
 - A local network management system (NMS)—Common Services supports import from NetView and HP OpenView. For supported versions, see [Supported NMS Integration, page 1-14](#).
 - A remote NMS—The same NMSs supported locally are supported remotely.
 - A file—File can be exported from another product and formatted for import to DCR.
- You can configure a DCR server to host a *master* list of all devices and share the list with clients (other instances of DCR in the same management domain that are configured as slaves).

By default, DFM is configured to automatically synchronize its device list with DCR. If the synchronization causes the DFM system to exceed its limits, the device and credentials list will be truncated. (See [Number of Ports/Interfaces that DFM Supports, page 1-16](#).)

Alternatively, you can configure DFM to allow only manual selection of devices in DCR that you want DFM to manage. When you do so, DFM displays a list of devices in DCR, but not in DFM, for you to choose from.

The following scenarios illustrate only a few possible ways to configure DFM and DCR to share device lists and credentials.

Scenario One

In this scenario, DFM and RME are installed on separate systems. On the RME system, DCR is configured as a server (master). On the DFM system, DCR is configured as a client (slave) of the DCR server on the RME system. The DFM system is configured for manual selection devices from DCR.

In this scenario, devices imported to the DCR server on the RME system are also added to the DCR client on the DFM system. Since DFM is not configured to automatically synchronize with DCR, the devices are not added to the DFM inventory. However, these devices are available in DCR and if DFM users want to manage them, they can do so by selecting them.

Scenario Two

In this scenario, DFM and an NMS are installed on the same system. DCR is configured to run bulk import regularly, importing devices from a local NMS. DFM is configured to synchronize with DCR.

In this scenario, DCR regularly imports devices from the local NMS, updating DCR with any new devices. Since DFM is configured to automatically synchronize with DCR, the devices are also added to the DFM inventory.



Note

Synchronization with DCR will stop when DFM reaches its limit. See [Number of Ports/Interfaces that DFM Supports](#), page 1-16.

Supported NMS Integration

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

- DFM listens for traps from managed devices on port 162 (by default). If another NMS on the system with DFM uses port 162:
 - The installation script warns you that this is the case.
 - You must specify a different port for DFM trap receiving after the installation completes. See [Integrating DFM Trap Receiving with Other NMSs or Trap Daemons](#), page 4-15.
- DFM forwards traps to destinations that you specify, as follows:
 - To forward pass-through traps, see [Configuring SNMP Trap Forwarding](#), page 4-18.
 - To forward processed traps, see “Managing SNMP Trap Notifications” in the “Using Notification Services” chapter of *User Guide for Device Fault Manager*.

For more information on pass-through and processed traps, see the appendix “Processed and Pass-through Traps, and Other Unidentified Traps and Events” in *User Guide for Device Fault Manager*.

- DFM provides the HPOV-NetView adapters, which forward traps (sent from managed devices to the NMS) to DFM from remote or local hosts running:
 - HP OpenView 6.4 and 7.0.1
 - NetView 7.1 and 7.1.4

For remote machines without CiscoWorks, the remote adapters are supported on:

- Solaris 2.8 or 2.9
- Windows 2000 Server and Advanced Server with SP4
- Windows Server 2003 Limited and Enterprise Edition

Installing these adapters on remote machines is described in [Installing and Upgrading HPOV-NetView Adapters, page 2-16](#).

**Note**

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

If the standard User Datagram Protocol (UDP) trap port (162) is being used by another NMS, you must configure DFM SNMP trap receiving to use a different UDP port, such as port 9000. See [Configuring SNMP Trap Receiving and Forwarding, page 4-13](#).

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 this URL:

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

For information on how device support compares between DFM 1.2.x and DFM 2.0, see *Release Notes for Device Fault Manager 2.0* at this URL:

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

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

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

Number of Ports/Interfaces that DFM Supports

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

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

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



Installing and Uninstalling DFM

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

- [Preparing to Install DFM, page 2-1](#)
- [Performing a New Installation, page 2-4](#)
- [Reinstalling DFM, page 2-11](#)
- [Uninstalling DFM, page 2-15](#)
- [Installing and Upgrading HPOV-NetView Adapters, page 2-16](#)
- [Uninstalling the HPOV-NetView Adapters, page 2-20](#)

Preparing to Install DFM

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

- Determine whether your existing applications are already using ports that DFM uses. (Existing applications should not use the ports that DFM uses.)
- Gather information that you might need to provide during the DFM installation.

Verifying TCP and UDP Ports that DFM Uses

Before installing DFM, make sure that the ports DFM uses will be used only by applications listed in [Table 2-1](#). For a complete list of ports used by Common Services and other LAN Management Solution (LMS) applications, see the *Quick Start Guide for LAN Management Solution 2.5* on Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/lms/lms25/index.htm.


Note

If an existing NMS uses port 162, for more information, see [Configuring SNMP Trap Receiving and Forwarding](#), page 4-13.

DFM uses the following TCP and UDP ports.

Table 2-1 DFM Ports and Protocols

Protocol	Port Number	Service Name	Direction (of establishment) of Connection
ICMP	—	Ping	Server to Device
UDP	161	Simple Network Management Protocol (SNMP)	Server to Device, Device to Server
	162	SNMP Traps (Standard Port)—Default port number used by DFM for receiving traps	Server to Device, Device to Server
	9000	Used for trap receiving (if port 162 is occupied)	Client to Server

Table 2-1 DFM Ports and Protocols (continued)

Protocol	Port Number	Service Name	Direction (of establishment) of Connection
TCP	49	TACACS+ and ACS	Server to ACS
	9002	DynamID authentication (Used by DFM broker)	Client to Server
	15000	Used by log server	Server internal
	43445	Used by Fault History database engine (dfmFH)	Server internal
	43446	Used by inventory service database engine (DFMInv)	Server internal
	43447	Used by event processing database engine (dfmEPM)	Server internal
	43500-43520	Used by Common Services Transport Mechanism (CSTM) for internal DFM communication	Server internal

Gathering Information to Provide During Installation

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

- DFM database password and a DFM username and password for use by DFM processes—Only required when you perform a custom installation; otherwise, this information is randomly generated.

For more information on creating passwords see the appendix “Password Information” in *Installation and Setup Guide for Common Services on Solaris*.

- License information—If you must supply license information, the installation script prompts you to enter one of the following:
 - Information that you will find printed on the software claim certificate—Product Identification Number (PIN) and Product Authorization Key (PAK).

- Location of the license file—If you have already obtained a license file, provide the path. If not, be sure to obtain one. You can do so before or after you install DFM; see [Registering Your License, page B-3](#).

**Note**

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

**Note**

If you are installing DFM for evaluation purposes:

- You do not need to supply a license file or a PIN and a PAK.
 - You might be interested in the following information:
 - [Upgrading Your Evaluation License, page B-4](#)
 - [Licensing Reminders, page B-5](#)
-

Performing a New Installation

Use these steps to perform a fresh installation of DFM.

**Note**

If you are upgrading from DFM 1.2 and using these steps to install DFM 2.0 on a fresh system, afterward:

- If you purchased an upgrade license of DFM 2.0, you must run a CLI script to validate the upgrade license. (You will be prompted to do so.)
- You must export data from DFM 1.2 and import it into DFM 2.0.

For more information, see [Chapter 3, “Upgrading DFM.”](#)

- Step 1** Make sure your system meets these prerequisites:
- Required (or desired) operating system upgrades have been performed, and required service packs are installed.
 - Common Services 3.0 has been installed. See *Installation and Setup Guide for CiscoWorks Common Services 3.0 (Includes CiscoView) on Solaris*.
 - If you want a locally installed NMS to send traps to DFM, HP OpenView or NetView has been installed. See [Supported NMS Integration, page 1-14](#).
- Step 2** Close all open or active programs. Do not run other programs during the installation process.
- Step 3** As root, log into the system on which you will install DFM, and mount a local or remote CD-ROM drive. For instructions on mounting the CD-ROM, see [Appendix A, “Mounting and Unmounting on Solaris.”](#)
- Step 4** Start the installation program by entering one of the following:
- To install from a locally mounted CD, enter:

```
# cd /cdrom/cdrom0
# ./setup.sh
```
 - To install from a remotely mounted CD, enter:

```
# cd remotedir
# ./setup.sh
```
- where *remotedir* is the remote location where the CD-ROM is mounted.
- Step 5** Press **y** to accept the agreement, or **n** to quit installation.

(If the following message is not displayed, skip to Step 8.) The following message might appear:

```
To ensure full use of the product features, please select one of the
following:
```

```
(L) If you have a license file for this product,
you will then be prompted for the license file location.
```

```
(P) If you know only the PAK and PIN,
but have not obtained the license file.
```

```
(E) To evaluate the product only.
```

```
You can provide licensing information later if you want to fully
enable the product.
```

Step 6 Enter one of these:

- **L** for license file
- **P** for PAK and PIN
- **E** for evaluation
- **Q** to quit

Step 7 If you are using ACS mode, you will be warned that if you configured any custom ACS roles, they will be lost unless you exit the installation and change the AAA security mode to CiscoWorks Local. Do one of the following:

- If you want to continue the installation (you will lose any ACS custom roles), click **Yes** and proceed to [Step 8](#).
- If you do not want to continue the installation (so you can change your AAA security mode to CiscoWorks Local and save any ACS custom roles), do the following:
 - Click **No**. (You will need to reset your mode to ACS after you have installed DFM, as described in [Step 13](#).) The installation will abort.
 - From the command prompt, run the following command:


```
NMSROOT/bin/perl NMSROOT/bin/ResetLoginModule.pl
```
 - Return to [Step 4](#) to begin the installation process again.

Step 8 The installation program checks for required patches and other dependencies and displays:

- ```
1) "Typical installation. Recommended for all computers."
2) "Custom installation. Select this if you want to customize the
setup options."
```

```
Select one of the installation modes using its number or enter q to
quit [1]
```




---

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

---

**Step 9** The installation program displays the following installation choices (the choices might vary, depending on your configuration):

- 1) Install Device Fault Manager 2.0
- 2) Install Device Fault Manager 2.0 HPOV-NetView adapters

Select one of the items using its number or enter q to quit [1]

**Step 10** Select **1** and press **Return**. This installs the complete DFM package, which contains DFM and the HPOV-NetView adapters. (For more information on installation components, see [Table 1-1 on page 1-2](#).)

The installation program checks dependencies and system requirements:

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

**Note**

Do not be alarmed if you see the following message:

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

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

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

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 DFM to receive SNMP traps on a different UDP port, such as port 9000. (See [Configuring SNMP Trap Receiving and Forwarding, page 4-13](#).)

The installation proceeds without displaying any more questions, and the system prompt appears. The installation program copies the files to the CiscoWorks default installation directory `/opt/CSCOPx` (*NMSROOT*).

- Step 11** If you purchased an upgrade license of DFM 2.0, the following warning message is displayed when the installation completes:

```
WARNING: Please run the program <NMSROOT>/bin/dfmValidateUpgrade.sh
WARNING: to validate that this is an upgrade.
```

If you see this message, you must run the program after the installation completes. (See [Validating the Upgrade, page 3-11](#).)

- Step 12** Unmount and eject the CD-ROM.




---

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

- Step 13** If you exited the installation in order to change your AAA security mode from ACS to CiscoWorks Local (in [Step 7](#)), reset your security role back to ACS. From the Common Services home page, select **Server > Security > AAA Mode Setup**, click **Help**, and follow the instructions.

- Step 14** Specify the clients that are allowed to connect to the DFM server. (DFM provides this fine-grain control as an additional security feature.)

- a.** Unregister the daemons with the daemon manager:

- For DfmServer:

```
NMSROOT/bin/pdcmnd -u DfmServer
```

- For DfmBroker:

```
NMSROOT/bin/pdcmnd -u DfmBroker
```

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

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

| Argument               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <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 hostnames are registered with DNS, especially if you are using DHCP. |
| =any                   | Allow all incoming connections (default).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

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

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

**Note**

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

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

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

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

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

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

**Step 15** To verify that the DfmServer process is running, log into the CiscoWorks home page as the administrator and select **Common Services > Server > Admin > Processes**.

**Step 16** If you plan to use the HPOV-NetView adapters with Device Fault Manager 2.0, make sure the machine running DFM is registered with DNS.

**Step 17** To use DFM, select **Device Fault Manager** from the CiscoWorks home page.

---

If you had any errors, check the installation log, `/var/tmp/ciscoinstall.log`. The Cisco Technical Assistance Center (TAC) might ask you to send them the installation log.

If the standard UDP trap port (162) is being used by another NMS, you must configure DFM SNMP trap receiving to use a different UDP port, such as port 9000. See [Configuring SNMP Trap Receiving and Forwarding, page 4-13](#).

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

To integrate DFM with remote versions of HP OpenView or NetView, you must install the HPOV-NetView adapters as described in [Installing and Upgrading HPOV-NetView Adapters, page 2-16](#).

# Reinstalling DFM

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

- 
- Step 1** Close all open or active programs. Do not run other programs during the reinstallation process.
- Step 2** As root, log into the system on which you will reinstall DFM, and mount a local or remote CD-ROM drive. For instructions on mounting the CD-ROM, see [Appendix A, “Mounting and Unmounting on Solaris.”](#)
- Step 3** Start the installation program by entering one of the following:
- To reinstall from a locally mounted CD, enter:  

```
cd /cdrom/cdrom0
./setup.sh
```
  - To reinstall from a remotely mounted CD, enter:  

```
cd remotedir
./setup.sh
```

where *remotedir* is the remote location where the CD-ROM is mounted.
- Step 4** You are prompted to accept (and view) the license agreement. Press **Return**.
- Step 5** If you are using ACS mode, you will be warned that if you configured any custom ACS roles, they will be lost unless you exit the installation and change the AAA security mode to CiscoWorks Local. Do one of the following:
- If you want to continue the installation (you will lose any ACS custom roles), click **Yes** and proceed to [Step 6](#).
  - If you do not want to continue the installation (so you can change your AAA security mode to CiscoWorks Local and save any ACS custom roles), do the following:
    - Click **No**. (You will need to reset your mode to ACS after you have installed DFM, as described in [Step 11](#).) The installation will abort.
    - From the command prompt, run the following command:  

```
NMSROOT/bin/perl NMSROOT/bin/ResetLoginModule.pl
```
    - Return to [Step 3](#) to begin the reinstallation process again.

**Step 6** The installation program stops CiscoWorks, performs a requirements check and displays the following installation choices:

- 1) "Typical installation. Recommended for all computers."
- 2) "Custom installation. Select this if you want to customize the setup options."

**Step 7** Enter **1** or **2** and press **Return**. The installation program displays the following prompt:

```
INFO: Device Fault Manager 2.0 has been detected on your system, are
you sure you want to reinstall? (y/n) - y
```

**Step 8** Enter **y** and press **Return**.

**Step 9** If you reinstalled *only* the HPOV-NetView adapters, you are prompted to enter the name of the machine running DFM. Enter the name of the host (the default is localhost).




---

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

---

The reinstallation program checks dependencies and system requirements.

- If there is not enough disk space for the reinstallation, the program displays an error message and stops.
- If the minimum recommended requirements are not met, the program displays an error message and continues installing.

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 reinstallation completes, you must configure DFM SNMP trap receiving to use a different UDP port, such as port 9000. (See [Configuring SNMP Trap Receiving and Forwarding, page 4-13.](#))

The reinstallation proceeds without displaying any more questions, and the system prompt appears. The reinstallation program copies the files to the directory where DFM was originally installed.

**Step 10** Unmount and eject the CD-ROM.



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

**Step 11** If you exited the installation in order to change your AAA security mode from ACS to CiscoWorks Local (in [Step 5](#)), reset your security role back to ACS. From the Common Services home page, select **Server > Security > AAA Mode Setup**, click **Help**, and follow the instructions.

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

a. Unregister the daemons with the daemon manager:

- For DfmServer:

```
NMSROOT/bin/pdcmnd -u DfmServer
```

- For DfmBroker:

```
NMSROOT/bin/pdcmnd -u DfmBroker
```

b. Decide which hosts you want to specify using the `--accept` option with arguments shown in [Table 2-3](#).

**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 might result in configurations that forward incoming connections (possibly through software that provides an encrypted tunnel, for example).

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

- For the DFM server (the following command is one line):

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

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

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

- Step 13** To verify that the `DfmServer` process is running, log into the CiscoWorks home page as the administrator and select **Common Services > Server > Admin > Processes**.
- Step 14** To use DFM, select **Device Fault Manager** from the CiscoWorks home page.
- Step 15** If you use remote HPOV-NetView adapters, make sure the machine running DFM is registered with DNS.

If you had any errors, check the installation log, `/var/tmp/ciscoinstall.log`. The Cisco Technical Assistance Center (TAC) might ask you to send them the installation log.

## Uninstalling DFM



### Caution

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

### Step 1

As root, log into the system on which DFM is installed, and enter the following to start the uninstallation program (`NMSROOT` is the DFM installation directory):

```
cd /
NMSROOT/bin/uninstall.sh
```

The following prompt appears (the uninstallation choices might vary, depending on your configuration; see [Table 1-1 on page 1-2](#)):

```
1) CiscoWorks Common Services 3.0
2) CiscoView 6.1
3) Integration Utility 1.6
4) Device Fault Manager 2.0
5) all of the above
```

Select one of the items using its number or enter `q` to quit [`q`]

(Uninstalling DFM also removes DFM IDUs.)

### Step 2

Enter the appropriate number and press **Return**. The following prompt appears:

```
Are you sure you want to uninstall: the name of the selection (y/n)?
[n]
```

### Step 3

Enter **y** and press **Return** to remove your selections. The following prompt appears:

```
Delete the CiscoWorks packages? (y/n) [y]
```

### Step 4

Press **Return**.

Ignore all messages that ask if you want to remove packages. The uninstallation program does not accept input to these questions.

When the uninstallation program finishes, the following message appears:

```
All files were deleted successfully.
```

---

The uninstallation program removes the DFM application and updates the system. To install DFM again, see [Performing a New Installation, page 2-4](#).

If you had any errors, check the uninstallation log, `/var/tmp/ciscouninstall.log`. The Cisco Technical Assistance Center (TAC) might ask you to send them the uninstallation log.

## Installing and Upgrading HPOV-NetView Adapters

When you install DFM on a system with HP OpenView or NetView, the DFM installation script installs the HPOV-NetView adapters. These adapters take the traps that managed devices send to HP OpenView or Netview and forward them to DFM. For information on supported HP OpenView and NetView versions, see [Supported NMS Integration, page 1-14](#).

This section explains how to install or upgrade the HPOV-NetView adapters on a remote host so the adapters can exchange information with DFM on a local host. You can install or upgrade the HPOV-NetView adapters on remote hosts regardless of whether CiscoWorks is present. You can also use these procedures to reinstall the HPOV-NetView adapters.

If you upgrade a local version of DFM 1.2, you must also upgrade remote HPOV-NetView adapters.

**Note**

---

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

---

**Note**

---

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

---

## Reinstalling the HPOV-NetView Adapters on a Local Host

If you install NetView or HP OpenView on the local host *after* you have installed DFM, you should reinstall the HPOV-NetView adapters to configure them appropriately. See [Reinstalling DFM, page 2-11](#).

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

**Step 1** If you want to upgrade a 1.2 version of the HPOV-NetView adapters, remove the adapters as described in the [Uninstalling the HPOV-NetView Adapters from a Remote Host Running CiscoWorks, page 2-21](#).

**Step 2** As root, log into the machine on which you will install or upgrade the HPOV-NetView adapters, and mount a local or remote CD-ROM drive. For instructions on mounting the CD-ROM, see [Appendix A, “Mounting and Unmounting on Solaris.”](#)

**Step 3** Start the installation program by entering one of the following:

- To install from a locally mounted CD, enter:

```
cd /cdrom/cdrom0
./setup.sh
```

- To install from a remotely mounted CD, enter:

```
cd remotedir
./setup.sh
```

where *remotedir* is the remote location where the CD-ROM is mounted.

**Step 4** Enter the following to start the installation program:

```
./setup.sh
```

The installation program stops CiscoWorks, performs a requirements check, and displays the following installation choices (the choices might vary, depending on your configuration; see [Table 1-1 on page 1-2](#)):

- 1) Install Device Fault Manager 2.0
- 2) Install Device Fault Manager 2.0 HPOV-NetView adapters

**Step 5** Enter the appropriate number for the HPOV-NetView adapters and press **Return**. (For more information on installation components, see [Table 1-1 on page 1-2.](#))

The installation program stops HP OpenView or NetView and copies the files to the directory in which CiscoWorks is installed.

**Step 6** Eject the CD-ROM.




---

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

---

**Step 7** Restart HP OpenView or NetView to activate the adapter (using the **ovstart** or **nvstart** command).

---

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

If you had any errors during installation or upgrade, check the installation log, `/var/tmp/ciscoininstall.log`. The Cisco Technical Assistance Center (TAC) might ask you to send them the installation log.

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



### Caution

---

Do not use this script if DFM is installed. If you use the script on a machine containing DFM, you will corrupt the DFM configuration.

---

**Step 1** If you want to upgrade a 1.2 version of the HPOV-NetView adapter, remove the adapter as described in [Uninstalling the HPOV-NetView Adapters from a Remote Host Not Running CiscoWorks, page 2-22.](#)

**Step 2** Verify that you have 17 MB of space for installing the adapter.

**Step 3** Log in as root on the target machine.

**Step 4** Verify that DFM is not installed on this machine:

```
cd /opt/CSCOpX/setup
ls
```



**Caution** If the `dfm.info` file is present, DFM is installed. Do not use this script or you will corrupt the DFM configuration.

**Step 5** From a temporary directory, use `ftp` to copy the ascii file `NMSROOT/htdocs/rdist/dfm/NMS.bin` from the running DFM. In the following commands, `dfm-host` is where DFM 2.0 is installed, and `NMSROOT` is the DFM installation directory (normally `/opt/CSCOpX`):

```
cd /tmp
ftp dfm-host
User (dfm-host:(none)): login
Password: password
ftp> cd NMSROOT/htdocs/rdist/dfm
ftp> get NMS.bin
ftp> quit
```

**Step 6** Run the `NMS.bin` script:

```
sh NMS.bin
```

This message is displayed:

```
This script will install the Device Fault Manager HPOV-NetView Adapter
Package. Do you want to continue? (y/n) [y]
```

**Step 7** Press **Return**. You will see this message:

```
Would you like to install in the default directory? (y/n) [Y]
```

**Step 8** Press **Return** to install the adapter in the default directory, `/opt/DFM`.



**Caution** If you want to install or upgrade the adapter in another directory, you must enter the fully qualified pathname, and a symbolic link is created between that directory and the `/opt` directory. Do not remove the symbolic link.

This message is displayed:

```
Enter name or IP address of the machine running DFM : ?[localhost]
```

**Step 9** Enter the name of the machine running DFM and press **Return**.



---

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

---

This message is displayed:

```
Successful completion.
```

---

You do not need to stop or restart HP OpenView or NetView. CiscoWorks automatically configures the adapters to forward SNMP traps from HP OpenView and NetView to DFM.

If you had any errors during installation, check the installation log, /opt/DFM/ciscoNMSinstall.log. The Cisco Technical Assistance Center (TAC) might ask you to send them the installation log.

## Uninstalling the HPOV-NetView Adapters

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

## Uninstalling the HPOV-NetView Adapters from a Remote Host

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



---

**Caution**

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

---

## Uninstalling the HPOV-NetView Adapters from a Remote Host Running CiscoWorks

---

**Step 1** Log in as root on the target machine.

**Step 2** Run the uninstallation shell script (*NMSROOT* is the DFM installation directory):

```
NMSROOT/bin/uninstall.sh
```

The following prompt appears (depending on your configuration):

```
1) CiscoView
2) Integration Utility
3) CiscoWorks Common Services
4) Device Fault Manager 2.0
5) Device Fault Manager 2.0 HPOV-NetView adapters
4) all of the above
```

**Step 3** Enter the appropriate number for the HPOV-NetView adapters and press **Return**. The following prompt appears:

```
Are you sure you want to uninstall: Device Fault Manager HPOV-NetView
adapters (y/n)? [n]
```

**Step 4** Enter **y** and press **Return**

The following prompt appears:

```
Delete the CiscoWorks packages? (y/n)? [y]
```

**Step 5** Press **Return** to uninstall your selections.

When the uninstallation program finishes, the following message appears:

```
All files were deleted successfully.
```

---

## Uninstalling the HPOV-NetView Adapters from a Remote Host Not Running CiscoWorks

---

**Step 1** Log in as root on the target machine.

**Step 2** Run the uninstallation script:

```
cd /tmp
/opt/DFM/objects/dfm/bin/removeNMS
```

This message is displayed:

```
Calling remove script.
Removing /opt/DFM.
```

---



## Upgrading DFM

---

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

- [Upgrade Overview, page 3-1](#)
- [Preparing to Upgrade DFM, page 3-6](#)
- [Upgrading to DFM 2.0, page 3-7](#)
- [Post-Upgrade Steps, page 3-13](#)

### Upgrade Overview

DFM 2.0 provides a completely new user interface and many new functions. For more information, see [Appendix C, “How is DFM 2.0 Different from DFM 1.2.x?”](#)

You can perform a local in-place upgrade or a remote upgrade from the following:

- DFM 1.2 (with or without patch/IDUs).
- DFM 1.2 Updated for Common Services Version 2.2 (with or without patch/IDUs).

This document refers to these previous versions as *DFM 1.2.x*. This section provides a brief outline of the procedures and the data migration for each type of upgrade.

## Local Upgrade

You perform a local upgrade on the system where DFM 1.2.x is installed.

### Procedure for Local Upgrade

**Table 3-1 Local Upgrade Procedure**

|               | Tasks                                                                                                                                                                    | Reference                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| <b>Step 1</b> | Upgrade from DFM 1.2.x to DFM 2.0.<br><br><b>Note</b> To perform the upgrade, you will install DFM 2.0 from the CD and then manually run a program to upgrade your data. | <a href="#">Performing a Local Upgrade, page 3-8</a> |
| <b>Step 2</b> | Perform post-upgrade steps to complete basic configuration of DFM 2.0.                                                                                                   | <a href="#">Post-Upgrade Steps, page 3-13</a>        |

### Data that Is Migrated by a Local Upgrade

The following data is migrated from DFM 1.2.x to DFM 2.0 when you perform a local upgrade:

- Device list—The migration procedure adds devices to Common Services Device and Credentials Repository and to DFM.
- Device managed state (managed or unmanaged).
- The following notification information:
  - Mail recipient information
  - Mail sender ID
  - SMTP addresses
  - Trap destination addresses
  - Trap destination ports
- Some polling and threshold settings—See [Upgrading Polling Settings, page 3-3](#) and [Upgrading Threshold Settings, page 3-4](#).

No other data is migrated.

## Upgrading Polling Settings

[Table 3-2](#) lists DFM 1.2 polling groups and settings and those in DFM 2.0 that correspond to them. For a device to retain polling settings from DFM 1.2, a corresponding polling group (and settings) must exist in DFM 2.0 and the device must belong to it.

In DFM 2.0, there are several additional polling groups not listed in [Table 3-2](#) (for more information, see *User Guide for Device Fault Manager*). A device might belong to a new polling group in DFM 2.0. For example, a voice gateway is a member of the Routers polling group in DFM 1.2 and the Voice and Telephony polling group in DFM 2.0.

After upgrade, DFM 2.0 applies factory default settings to:

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

The device support table lists the DFM 1.2 and DFM 2.0 groups; refer to [Product Documentation, page xii](#).

**Table 3-2 Comparison of Polling Groups and Settings between DFM 1.2 and DFM 2.0**

| Polling Groups                                          |                                                  | Polling Settings                                                                                                                                                                                                                           |                                                                                                                                                                                                             |
|---------------------------------------------------------|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Devices that were members of these groups in DFM 1.2... | And become members of these groups in DFM 2.0... | Retain the values from these DFM 1.2 polling settings... <sup>1</sup>                                                                                                                                                                      | Reflected in these DFM 2.0 polling settings                                                                                                                                                                 |
| Optical Switches                                        | Optical Networking                               | <ul style="list-style-type: none"> <li>• Connectivity Polling</li> <li>• Environment Polling</li> <li>• Performance Polling - Processor and Memory</li> <li>• Performance Polling - Ports and Interfaces (includes access port)</li> </ul> | <ul style="list-style-type: none"> <li>• Reachability settings</li> <li>• Environment</li> <li>• Processor and memory utilization</li> <li>• Connector port and interface</li> <li>• Access port</li> </ul> |
| Switches                                                | Switches and Hubs                                |                                                                                                                                                                                                                                            |                                                                                                                                                                                                             |
| Routers                                                 | Routers                                          |                                                                                                                                                                                                                                            |                                                                                                                                                                                                             |
| Other Systems                                           | Voice and Telephony                              | Connectivity Polling                                                                                                                                                                                                                       | Reachability settings                                                                                                                                                                                       |

1. For any polling setting that was removed from a polling group in DFM 1.2, DFM 2.0 sets its value to the DFM 2.0 factory default value.

## Upgrading Threshold Settings

Like polling settings, threshold settings are retained when a device (or device component) is a member of a DFM 2.0 threshold group that corresponds to the DFM 1.2 threshold group it was a member of. [Table 3-3](#) lists the corresponding threshold groups and settings.

There are additional threshold groups in DFM 2.0 not listed in [Table 3-3](#) (for more information, see *User Guide for Device Fault Manager*). DFM 2.0 applies factory default threshold values to devices that are members of new DFM 2.0 threshold groups. The device support table lists the DFM 1.2 and DFM 2.0 groups; refer to [Product Documentation](#), page xii.

**Table 3-3 Comparison of Threshold Groups and Settings between DFM 1.2 and DFM 2.0**

| Threshold Groups                                 |                                                               | Threshold Settings/Categories                                                                                                                                                                                                                                       |                                                                                                                         |
|--------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Devices that were members of these in DFM 1.2... | And become members of these groups in DFM 2.0... <sup>1</sup> | Retain the values from these DFM 1.2 threshold settings... <sup>2</sup>                                                                                                                                                                                             | Reflected in these DFM 2.0 threshold categories                                                                         |
| Interface Groups                                 | Interface Groups                                              | For Interface Groups, Access Port Groups, and Trunk Port Groups, the threshold settings in DFM 1.2 correspond closely to the threshold categories in DFM 2.0. For a list of threshold categories for these groups, see <i>User Guide for Device Fault Manager</i> . |                                                                                                                         |
| Access Ports Groups                              | Access Port Groups                                            |                                                                                                                                                                                                                                                                     |                                                                                                                         |
| Trunk Ports Groups                               | Trunk Port Groups                                             |                                                                                                                                                                                                                                                                     |                                                                                                                         |
| Optical Switches                                 | Optical Networking                                            | <ul style="list-style-type: none"> <li>• Connectivity</li> <li>• Environment</li> <li>• Processor and Memory</li> </ul>                                                                                                                                             | <ul style="list-style-type: none"> <li>• Reachability</li> <li>• Environment</li> <li>• Processor and Memory</li> </ul> |
| Routers                                          | Routers                                                       |                                                                                                                                                                                                                                                                     |                                                                                                                         |
| Switches                                         | Switches and Hubs                                             |                                                                                                                                                                                                                                                                     |                                                                                                                         |

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

## Remote Upgrade

You perform a remote upgrade on a system where DFM 1.2.x is not installed.

### Procedure for Remote Upgrade



#### Caution

If you are upgrading your operating system from Solaris 2.8 to Solaris 2.9, run the upgrade script on Solaris 2.8 (*before* migrating your operating system). Otherwise the upgrade script will fail.

**Table 3-4 Remote Upgrade Procedure**

|               | Tasks                                                                                                                          | Reference                                                                                                                                                                   |
|---------------|--------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Upgrade or install DFM 2.0 on the remote system.                                                                               | <ul style="list-style-type: none"> <li>• <a href="#">Performing a Local Upgrade, page 3-8</a></li> <li>• <a href="#">Performing a New Installation, page 2-4</a></li> </ul> |
| <b>Step 2</b> | If you purchased a DFM 2.0 upgrade license, validate the upgrade by providing proof of purchase of DFM 1.2.x.                  | <a href="#">Validating the Upgrade, page 3-11</a>                                                                                                                           |
| <b>Step 3</b> | Export the DFM 1.2.x seed file and import it to DFM 2.0; or<br><br>Use the DFM 2.0 Upgrade Kit to perform your data migration. | <a href="#">Exporting DFM 1.2.x Information to an Upgraded Remote Host, page 3-12</a><br><br><a href="#">Data that Is Migrated by a Remote Upgrade, page 3-5</a>            |
| <b>Step 4</b> | Perform post-upgrade steps to complete basic configuration of DFM 2.0.                                                         | <a href="#">Post-Upgrade Steps, page 3-13</a>                                                                                                                               |

### Data that Is Migrated by a Remote Upgrade

Only the device list is migrated. However, you can use a DFM 2.0 Upgrade Kit to migrate the following additional DFM 1.2.x information:

- Device managed state (managed or unmanaged).
- Some polling and threshold settings (as described in [Data that Is Migrated by a Local Upgrade, page 3-2](#)).

To use the Upgrade Kit, you must have a copy of the DFM 1.2.x DFM.rps (inventory) file. The Upgrade Kit and accompanying Readmes are available from the DFM download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>

## Preparing to Upgrade DFM

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

If you purchased an upgrade license of DFM 2.0, you are required to validate the upgrade by providing one of the following:

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



### Caution

---

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

---

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

- DFM database password and a DFM username and password for use by DFM processes—Only required when you perform a custom installation; otherwise, this information is randomly generated.

For more information on creating passwords, see the appendix “Password Information” in *Installation and Setup Guide for Common Services on Solaris*.

- License information—If you must supply license information, the installation script prompts you for one of the following:
  - Information that you will find printed on the software claim certificate—Product Identification Number (PIN) and Product Authorization Key (PAK).
  - Location of the license file—If you have a license file, provide its location. If not, be sure to obtain one. You can do so before or after you install DFM; see [Registering Your License, page B-3](#).



---

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

---



**Note**

---

If you are installing DFM for evaluation purposes:

- You do not need to supply a license file or PIN and PAK.
  - You might be interested in the following information:
    - [Upgrading Your Evaluation License, page B-4](#)
    - [Licensing Reminders, page B-5](#)
- 

## Upgrading to DFM 2.0

You can upgrade from DFM 1.2.x, with or without patch/IDUs, to DFM 2.0 on local or remote systems. If desired, you can upgrade a remote system and then export your local DFM 1.2.x information to the upgraded remote system. These procedures are described in the following sections:

- [Performing a Local Upgrade, page 3-8](#)
- [Performing a Remote Upgrade, page 3-11](#)

## Performing a Local Upgrade

Follow these steps to upgrade a local host to DFM 2.0.

**Step 1** Make sure your system meets the following prerequisites:

- Required (or desired) operating system upgrades have been performed, and required service packs are installed.



**Caution** If you are upgrading your operating system from Solaris 2.8 to Solaris 2.9, run the upgrade script on Solaris 2.8 (*before* migrating your operating system). Otherwise the upgrade script will fail.

- All installed applications are supported by Common Services 3.0. Applications not supported by Common Services will be disabled when you upgrade CD One.
- Common Services has been installed. (See *Installation and Setup Guide for Common Services (Includes CiscoView) on Solaris.*)
- If you want a locally installed NMS to send traps to DFM, HP OpenView or NetView has been installed. See [Supported NMS Integration, page 1-14](#).

**Step 2** As root, log into the system on which you will upgrade DFM, and do the following:

- a. Mount a local or remote CD-ROM drive. For instructions on mounting the CD-ROM, see [Appendix A, “Mounting and Unmounting on Solaris.”](#)
- b. Close all open or active programs. Do not run other programs during the upgrade process.

**Step 3** Start the installation program by entering one of the following:

- To install from a locally mounted CD drive, enter:

```
cd /cdrom/cdrom0
./setup.sh
```

- To install from a remotely mounted CD drive, enter:

```
cd remotedir
./setup.sh
```

where *remotedir* is the remote location where the CD-ROM is mounted.

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

**Step 4** If you are using ACS mode, you will be warned that if you configured any custom ACS roles, they will be lost unless you exit the upgrade and change the AAA security mode to CiscoWorks Local. Do one of the following:

- If you want to continue the upgrade (you will lose any ACS custom roles), click **Yes** and proceed to [Step 5](#).
- If you do not want to continue the upgrade (so you can change your AAA security mode to CiscoWorks Local and save any ACS custom roles), do the following:
  - Click **No**. (You will need to reset your mode to ACS after you have installed DFM, as described in [Step 8](#).) The installation will abort.
  - From the command prompt, run the following command:
 

```
NMSROOT/bin/perl NMSROOT/bin/ResetLoginModule.pl
```
  - Return to [Step 3](#) to begin the upgrade process again.

**Step 5** The installation program displays the following installation choices (the choices may vary, depending on your configuration; see [Table 1-1 on page 1-2](#)):

- 1) Install Device Fault Manager 2.0
- 2) Install Device Fault Manager 2.0 HPOV-NetView adapters

**Step 6** Select **1** and press **Return**. This installs the complete DFM package, which contains DFM and the HPOV-NetView adapters. (For more information on installation components, see [Table 1-1 on page 1-2](#).)

The installation program checks dependencies and system requirements:

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



**Note**

Do not be alarmed if you see the following message:

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

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

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

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 DFM SNMP trap receiving to use a different UDP port, such as port 9000. (See [Configuring SNMP Trap Receiving and Forwarding, page 4-13.](#))

The upgrade proceeds without displaying any more questions. The upgrade program:

- Copies the files to the CiscoWorks default installation directory `/opt/CSCOPx (NMSROOT)`.
- Exports data (see [Data that Is Migrated by a Local Upgrade, page 3-2.](#))

The system prompt appears.

**Step 7** Unmount and eject the CD-ROM.




---

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

---

**Step 8** If you exited the upgrade in order to change your AAA security mode from ACS to CiscoWorks Local (in [Step 4](#)), reset your security role back to ACS. From the Common Services home page, select **Server > Security > AAA Mode Setup**, click **Help**, and follow the instructions.

**Step 9** Upgrade DFM 1.2.x data to DFM 2.0 using the following command:

```
perl NMSROOT/bin/DFM12x-DFM20-upgrade.pl
```

where NMSROOT is the default installation directory, normally `/opt/CSCOPx`.

The script automatically does all of the following:

1. Imports the seedfile generated from DFM 1.2.x into DCR.
2. Imports devices from DCR into DFM 2.0 and monitors device import status.




---

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

---

3. Applies the manage/unmanage state of the devices/device components obtained from DFM 1.2.x during the upgrade.
4. Applies new polling and threshold settings to the devices.

**Step 10** To check the status of device discovery and to complete your configuration of DFM, see [Post-Upgrade Steps, page 3-13](#).

---

## Performing a Remote Upgrade

Perform these steps after DFM 2.0 is installed on a remote system:

- If you purchased an upgrade license of DFM 2.0, you must validate the upgrade. See [Validating the Upgrade, page 3-11](#).
- Export DFM 1.2.x information to DFM 2.0. See [Exporting DFM 1.2.x Information to an Upgraded Remote Host, page 3-12](#).

## Validating the Upgrade

If you purchased an upgrade license of DFM 2.0, you must validate the upgrade on the system where DFM 2.0 is installed using the following commands:

```
cd NMSROOT/bin
./dfmValidateUpgrade.sh
```

where *NMSROOT* is the default installation directory, normally */opt/CSCOpX*. The following prompt is displayed:

```
This utility will validate your proof of purchase of the product and
allows you to obtain an upgrade license.
Please select the source for upgrade validation from the following:
1. Validate from a CD (old version).
2. Validate from a remote server (old version).
Please enter option [1 / 2]:
```

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

```
Please insert the previous versions of DFM CD into the CDROM drive and
provide the absolute path to the CD drive:
/cdrom/cdrom0
Validation succeeded.
```

For example, if you enter 2:

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



#### Note

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

- DFM is licensed for evaluation only and operates in *nag* mode for no more than 90 days before ceasing operation. (See [Evaluation Version: Before Expiry](#), page B-5.)
- You must contact your Cisco representative to purchase a fully licensed version of DFM. (See [Upgrading Your Evaluation License](#), page B-4.)

## Exporting DFM 1.2.x Information to an Upgraded Remote Host

This procedure exports your local DFM 1.2.x device list and imports it to a remote system that has been upgraded to DFM 2.0.

**Step 1** As root, log in to the local DFM 1.2.x system.

**Step 2** Export the device inventory to a seed file using the following command:

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

where *NMSROOT* is the default installation directory (normally /opt/CSCOPx).

**Step 3** Copy the seed file to the remote system.

**Step 4** Log in to the remote DFM 2.0 system as root.

**Step 5** Import the inventory into DFM 2.0 using the following command:

```
NMSROOT/bin/dfmimport fn=completePath/seedfile.txct
```

where *NMSROOT* is the default installation directory (normally */opt/CSCOpX*) and *completePath/seedfile.txt* is the complete path to the seed file and the seed file name.

The script will initiate device discovery.

---

**Note**

If an error occurs because the CiscoWorks daemon manager is not running, start it by typing the following command:

```
/etc/init.d/dmgttd start
```

---

## Post-Upgrade Steps

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

- Familiarize yourself with new device management procedures; see [Performing Device Management, page 4-6](#).
- Verify discovery status; see [Verifying Devices Added to DFM, page 4-7](#).
- Complete basic configuration steps; see [Configuring SNMP Trap Receiving and Forwarding, page 4-13](#).
- Start using DFM to monitor the network; see [Viewing Alerts, page 4-18](#) and [What Next?, page 4-19](#).

If you plan to use HPOV-NetView adapters on a remote system with Device Fault Manager 2.0 on a local system, perform these steps:

1. Make sure the system running DFM is registered with DNS.
2. Upgrade all remote adapters as described in [Installing and Upgrading HPOV-NetView Adapters, page 2-16](#).

**Note**

---

If the standard UDP trap port (162) is being used by another NMS, such as Cisco Voice Manager, you must configure DFM SNMP trap receiving to use a different UDP port, such as port 9000. See [Integrating DFM Trap Receiving with Other NMSs or Trap Daemons](#), page 4-15.

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

1. Configure DFM to forward traps to the listening port for the NMS. See [Configuring SNMP Trap Forwarding](#), page 4-18.
2. Make sure the NMS is configured to receive traps at the port you specified in Step 1. See the appropriate documentation for the NMS.

If a local version of HP OpenView or NetView is already installed (or is installed later), CiscoWorks automatically configures the adapters to forward SNMP traps to DFM. To configure remote versions of HP OpenView and NetView to forward SNMP traps to DFM, you must install the HPOV-NetView adapters on the remote systems as described in [Installing and Upgrading HPOV-NetView Adapters](#), page 2-16.

---



## Getting Started

---

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

## Configuration Roadmap

[Table 4-1](#) lists the basic tasks for setting up DFM.

**Table 4-1**      **Configuration Roadmap**

| Task                                  | Steps                                                                                      | References                                                                                                                                                                                             |
|---------------------------------------|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add devices to DFM managed inventory. | 1. Add devices and credentials to Common Services Device and Credentials Repository (DCR). | <ul style="list-style-type: none"><li>• <a href="#">Managing Device Credentials, page 4-5</a></li><li>• <a href="#">Importing Devices to the Device and Credentials Repository, page 4-6</a></li></ul> |
|                                       | 2. Verify that devices were discovered (and troubleshoot problems, if necessary).          | <ul style="list-style-type: none"><li>• <a href="#">Verifying Devices Added to DFM, page 4-7</a></li><li>• <a href="#">Troubleshooting Device Discovery, page 4-10</a></li></ul>                       |

**Table 4-1** Configuration Roadmap (continued)

| Task                                     | Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                               | References                                                                                                                                                                                                                                                                                                              |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure Trap Receiving                 | <p><b>3.</b> Determine which of the following approaches to SNMP trap receiving to take and perform the appropriate steps:</p> <ul style="list-style-type: none"> <li>• Send SNMP traps directly to DFM: <ul style="list-style-type: none"> <li><b>a.</b> Update DFM trap receiving port if necessary.</li> <li><b>b.</b> Enable devices to send traps to DFM.</li> </ul> </li> <li>• Integrate DFM SNMP trap receiving with other NMSs or trap daemons.</li> </ul> | <p>—</p> <p>—</p> <ul style="list-style-type: none"> <li>• <a href="#">Updating the SNMP Trap Receiving Port, page 4-13</a></li> <li>• <a href="#">Enabling Devices to Send Traps to DFM, page 4-13</a></li> <li>• <a href="#">Integrating DFM Trap Receiving with Other NMSs or Trap Daemons, page 4-15</a></li> </ul> |
| (Optional) Configure DFM Trap Forwarding | <p><b>4.</b> Configure DFM to forward traps.</p>                                                                                                                                                                                                                                                                                                                                                                                                                    | <p><a href="#">Configuring SNMP Trap Forwarding, page 4-18</a></p>                                                                                                                                                                                                                                                      |

After you complete the tasks in [Table 4-1](#):

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

# Using the CiscoWorks Home Page

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

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

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

**Note**

---

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

---

## Registering Applications with the CiscoWorks Home Page

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

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

**Note**

---

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

---

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

## Understanding and Configuring Security

DFM supports the following security-related mechanisms:

- **SNMPv3 protocol (Authentication/No-Privacy option)**—DFM supports the authentication/no-privacy option between the server and the device.
- **Security on the CiscoWorks server**—You can configure the following aspects of security for the server on which DFM resides:
  - **Secure Socket Layer (SSL)**—DFM can use SSL protocol between the server and the browser. You can enable and disable SSL for the server. If you enable SSL, you should set up a self-signed security certificate to enable SSL communication.
  - **Local security or Cisco Secure ACS**—Access to tasks within DFM is controlled either by local security, provided by Common Services, or by Cisco Security ACS. Local security is enabled on the server by default. DFM supports integration with Cisco Secure ACS. For more information, see [Configuring DFM on Cisco Secure ACS, page D-6](#).

**Note**

---

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

---

## Managing Device Credentials

DCR is a common repository of devices and their credentials for use by individual applications. DFM takes its device list and credentials from DCR. DCR enables DFM to synchronize with or select from a device list that:

- Is shared by other CiscoWorks applications that are installed locally. This is the default.
- Can be shared by remote CiscoWorks applications if the remote CiscoWorks server has been configured to use the same master instance of DCR.

**Note**

---

To set up DCRs in a configuration with a master and slaves, see *User Guide for Common Services*. See also *User Guide for Device Fault Manager* for details about DFM integration with DCR.

---

- Can synchronize with Network Management Systems (NMSs) installed locally or remotely.

You will use DCR to:

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

To perform these tasks, see *User Guide for CiscoWorks Common Services*. For scenarios for DFM, see [Performing Device Management, page 4-6](#).

# Performing Device Management

There are two distinct sets of device management tasks:

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

## Importing Devices to the Device and Credentials Repository

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



### Note

You can import devices from a previous version of DFM by following the instructions in [Exporting DFM 1.2.x Information to an Upgraded Remote Host, page 3-12](#).

## Adding Devices to DFM



### Note

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

- 
- Step 1** On the DFM home page, select **Device Management > Device Selector**.
- Step 2** To manually select devices to add to DFM:
- a. Deselect the Synchronize with Device Credentials Repository check box. (By default, the check box is selected.)
  - b. After new devices have been added to DCR, click **Ctrl** and select devices from the Devices not in Device Fault Manager list.

- c. Click the > **Add** >> button.
- d. Click **OK**.

**Step 3** To automatically add devices to DFM:

- a. Select the Synchronize with Device Credentials Repository check box.
  - b. Click **OK**.
- 

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

## Verifying Devices Added to DFM

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

- A brief summary—See [Viewing the Device Summary, page 4-7](#).
- Details for devices in a particular device state—See [Viewing Device Details, page 4-8](#).
- Discovery status of all devices—See [Viewing Discovery Status, page 4-9](#).

If you find that problems have occurred during device discovery, see [Troubleshooting Device Discovery, page 4-10](#).

## Viewing the Device Summary

---

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

---

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

- **Known**—The device has been successfully imported and is fully managed by DFM.
- **Learning**—DFM is discovering the device. This is the beginning state, when the device is first added or is being rediscovered.

- **Questioned**—DFM cannot manage the device. See [Troubleshooting Device Discovery, page 4-10](#).
- **Pending**—The device is being deleted. DFM is waiting for confirmation from all of its data collectors before purging the device and its details.
- **Unknown**—DFM does not support the device.

For a list of devices in a particular device state, see [Viewing Device Details, page 4-8](#). For a list of all devices, see [Viewing Discovery Status, page 4-9](#).

## Viewing Device Details

- Step 1** On the DFM home page, select **Device Management > Device Details**. The Device Report page opens. In the Device Selector pane, a device group for each current device state is displayed.
- Step 2** Select a device group or devices from a group and click **View**. The Device Details report opens in a new window and displays the following information.

| Column          | Description                                                                                                                                                                                                                                                                         |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device Name     | IP address or DNS name for the device.                                                                                                                                                                                                                                              |
| IP Address      | IP address for the device.                                                                                                                                                                                                                                                          |
| Status          | The device state: Known, Learning, Questioned, Pending, or Unknown.<br><br>For device state definitions, see <a href="#">Viewing the Device Summary, page 4-7</a> .<br><br>If devices are not in the Known state, see <a href="#">Troubleshooting Device Discovery, page 4-10</a> . |
| Device Type     | The device type; for example, Content Networking, Routers, Switches and Hubs, and so on. For more information, see <i>User Guide for Device Fault Manager</i> .                                                                                                                     |
| First Added     | Date and time the device was first added to DFM.                                                                                                                                                                                                                                    |
| Last Discovered | Date and time of most recent discovery.                                                                                                                                                                                                                                             |

## Viewing Discovery Status

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

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

The View Discovery Status table displays the following information:

| Column          | Description                                                                                                                                                                                                                                                                         |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device Name     | IP address or DNS name for the device.                                                                                                                                                                                                                                              |
| Status          | <p>Device state—Known, Learning, Questioned, Pending, or Unknown.</p> <p>For device state definitions, see <a href="#">Viewing the Device Summary, page 4-7</a>.</p> <p>If devices are not in the Known state, see <a href="#">Troubleshooting Device Discovery, page 4-10</a>.</p> |
| DFM Processing  | <p>Processing status—One of the following:</p> <ul style="list-style-type: none"> <li>Active—DFM is managing the device.</li> <li>Suspended—DFM is not managing the device.</li> <li>N/A—DFM cannot manage the device; the device state is Questioned.</li> </ul>                   |
| Last Discovered | Date and time of most recent discovery.                                                                                                                                                                                                                                             |

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

## Troubleshooting Device Discovery

Try the following to troubleshoot device discovery:

- If a device is not responding, confirm all device credentials and reread the device. See [Changing Device Credentials, page 4-10](#).
- Increase SNMP timeout settings if device rediscovery times out for several devices. See [Modifying SNMP Timeout and Retries, page 4-10](#).
- View device error information on the Edit Device Configuration page. See [Rediscovering a Device, page 4-11](#).
- Verify that the device is operational during the import and that it supports MIB II.
- Check the reason for devices in the Questioned state. See [Understanding Device Discovery Messages, page 4-12](#).

After troubleshooting your problem, check the device status. See [Viewing Discovery Status, page 4-11](#).

### Changing Device Credentials

You change device credentials using Common Services DCR.

### Modifying SNMP Timeout and Retries

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

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

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

- 
- Step 1** Select **Device Management > SNMP Config**. The SNMP Configuration page appears.
  - Step 2** Select a new SNMP Timeout setting. The default is 4 seconds.

- Step 3** Select a new Number of Retries setting. The default is 3 retries.
- Step 4** Click **Apply**. Click **Yes** to confirm.
- 

## Rediscovering a Device

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

---

- Step 1** Select **Device Management > Rediscover/Delete**. The Rediscover/Delete Devices page appears.
- Step 2** Select the devices or group(s) you want to rediscover.
- Step 3** Click **Rediscover**.
- Rediscovery is started. To view rediscovery status, select **Device Management > View Discovery Status**.
- 

## Viewing Discovery Status

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

## Understanding Device Discovery Messages

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

**Table 4-2** Import Error Messages

| Message                                              | Meaning                                                                                                                                                    | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNMP Timeout                                         | The device is in the Questioned state because the SNMP read-only community string for the device is incorrect.                                             | See <a href="#">Changing Device Credentials, page 4-10</a> to enter the correct read community string for the device.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Others: Missing IP Address or Data Collector Timeout | The device is in the Questioned state because of some other reason. It could be that DNS resolution for the device failed or the data collector timed out. | <p>Click the device on the Rediscover/Delete Devices page. The error message displays the exact problem.</p> <ul style="list-style-type: none"> <li>• If the IP address is missing: <ul style="list-style-type: none"> <li>– Readd the device with the correct IP address.</li> <li>or</li> <li>– Make sure that DFM can resolve the device name: try adding the domain name as part of the device name.</li> </ul> </li> <li>• If the data collector times out, restart the daemon manager to get all data collectors in sync.</li> </ul> |

# Configuring SNMP Trap Receiving and Forwarding

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

- An NMS
- A trap daemon

To send traps directly to DFM, perform the tasks in [Enabling Devices to Send Traps to DFM, page 4-13](#). To integrate SNMP trap receiving with an NMS or a trap daemon, follow the instructions in [Integrating DFM Trap Receiving with Other NMSs or Trap Daemons, page 4-15](#).

## Updating the SNMP Trap Receiving Port

By default, DFM receives SNMP traps on port 162. If you need to change the port (for example, to port 9000), you can do so.

- 
- Step 1** On the Configuration tab of the DFM home page, select **Other Configurations > SNMP Trap Receiving**.
  - Step 2** Enter the port number in the Receiving Port entry box.
  - Step 3** Click **Apply**.
- 

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

## Enabling Devices to Send Traps to DFM

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

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

- [Enabling Cisco IOS-Based Devices to Send Traps to DFM, page 4-14](#)
- [Enabling Catalyst Devices to Send SNMP Traps to DFM, page 4-14](#)

## Enabling Cisco IOS-Based Devices to Send Traps to DFM

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

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

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

For more information, see the appropriate command reference guide.

- 
- Step 1** Log in to Cisco.com.
  - Step 2** Select **Products & Solutions > Cisco IOS Software**.
  - Step 3** Select the Cisco IOS Software release version used by your Cisco IOS-based devices.
  - Step 4** Select **Technical Documentation** and select the appropriate command reference guide.
- 

## Enabling Catalyst Devices to Send SNMP Traps to DFM

For devices running Catalyst software, provide the following commands:

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

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

For more information, see the appropriate command reference guide.

- 
- Step 1** Log in to Cisco.com.
- Step 2** Select **Products & Solutions > Switches**.
- Step 3** Select the appropriate Cisco Catalyst series switch.
- Step 4** Select **Technical Documentation** and select the appropriate command reference guide.
- 

## Integrating DFM Trap Receiving with Other NMSs or Trap Daemons

You might need to complete one or more of the following steps to integrate trap receiving with other network management systems (NMSs) or trap daemons:

- Add the host where DFM is running to the list of trap destinations in your network devices. See [Enabling Devices to Send Traps to DFM, page 4-13](#). Specify port 162 as the destination trap port.  
  
If another NMS is already listening for traps on the standard UDP trap port (162), you must configure DFM to use another port, such as port 9000. See [Updating the SNMP Trap Receiving Port, page 4-13](#).
- If your network devices are already sending traps to another management application, configure that application to forward traps to DFM. See appropriate documentation for the management application.

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

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

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

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

| With DFM installed on...                     | You can configure DFM to...                   |                                                                                                     | Advantages                                                                                                                                                                                                                                                                  |
|----------------------------------------------|-----------------------------------------------|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                              | Receive traps on this port and...             | Forward traps to an NMS on this port                                                                |                                                                                                                                                                                                                                                                             |
| A host with an NMS                           | 162 (standard listening port and DFM default) | 9000 (nonstandard listening port)<br><b>Note</b> You must configure the NMS to listen on this port. | <ul style="list-style-type: none"> <li>DFM provides a reliable trap reception and forwarding mechanism.</li> <li>Devices do not need to be reconfigured to send traps to another host or port.</li> <li>DFM and the NMS run on the same host.</li> </ul>                    |
|                                              | 9000                                          | 162                                                                                                 | <ul style="list-style-type: none"> <li>DFM provides a reliable trap reception and forwarding mechanism.</li> <li>No reconfiguration of the NMS is required; it continues to listen for traps on default port 162.</li> <li>DFM and the NMS run on the same host.</li> </ul> |
| A host and an NMS installed on a remote host | 162                                           | 162 (on the remote host)                                                                            | <ul style="list-style-type: none"> <li>DFM provides a reliable trap reception and forwarding mechanism.</li> <li>NMS continues to receive traps on port 162.</li> <li>Network devices continue to send traps to port 162.</li> </ul>                                        |

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

Table 4-4 lists configurations in which an NMS receives SNMP traps and forwards the traps to DFM. In these configurations, the HPOV-NetView adapters forward SNMP traps to DFM; the adapters must be installed properly. For more information, see [Installing and Upgrading HPOV-NetView Adapters](#), page 2-16.

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

| With DFM installed on...                     | And the NMS receiving traps on this port ...                                                           | Configure DFM to receive traps (forwarded from the NMS) on this port... | Advantages                                                                                                                                                                                                                                                              |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A host with an NMS                           | 162 (standard listening port)                                                                          | 9000 (nonstandard listening port)                                       | <ul style="list-style-type: none"> <li>• No reconfiguration of the NMS is required.</li> <li>• No reconfiguration of network devices is required.</li> <li>• DFM and the NMS run on the same host.</li> <li>• DFM does not receive traps dropped by the NMS.</li> </ul> |
| A host and an NMS installed on a remote host | 162 (on the remote host)<br><b>Note</b> You must install the HPOV-NetView adapters on the remote host. | 162                                                                     | <ul style="list-style-type: none"> <li>• No reconfiguration of the NMS is required.</li> <li>• No reconfiguration of network devices is required.</li> <li>• DFM does not receive traps dropped by the NMS.</li> </ul>                                                  |

## Configuring SNMP Trap Forwarding

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

- 
- Step 1** On the Configuration tab of the DFM home page, select **Other Configurations > SNMP Trap Forwarding**.
- Step 2** For each host, enter:
- An IP address or DNS name for the hostname.
  - A port number on which the host can receive traps.
- Step 3** Click the **Apply** button.
- 

## Viewing Alerts

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

## Starting DFM

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

**Note**

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

- Device Management
- Notification Services

- Fault History
- Configuration

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

**Note**

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

## What Next?

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

[Table 4-5](#) summarizes how to continue setting up DFM.

**Table 4-5**      **Setting Up DFM**

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

**Table 4-5**      **Setting Up DFM (continued)**

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

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



# Mounting and Unmounting on Solaris

---

This appendix describes how to mount the DFM CD-ROM on a Solaris system. It includes general information only. For more detailed instructions, consult your Sun documentation.

You can install DFM from a CD-ROM mounted on the DFM server system or from a CD-ROM mounted on a remote Solaris system.

This appendix contains:

- [Mounting a Local CD-ROM Drive, page A-1](#)
- [Mounting a Remote CD-ROM Drive, page A-3](#)
- [Unmounting a CD-ROM Drive, page A-5](#)

## Mounting a Local CD-ROM Drive

Insert the DFM CD-ROM into the CD-ROM drive and do the following:

- 
- Step 1** Become the superuser by entering the command **su** and the root password at the command prompt, or log in as root. The command prompt changes to the pound sign (#).
- Step 2** If the `/cdrom` directory does not already exist, enter the following command to create it:
- ```
# mkdir /cdrom
```

Step 3 Mount the CD-ROM drive.



Note The vold process manages the CD-ROM device and performs the mounting. The CD-ROM might automatically mount onto the /cdrom/cdrom0 directory.

If you are running File Manager, a separate File Manager window displays the contents of the CD-ROM. From the File Manager, double-click setup.sh. The Action: Run box appears. Click **OK** to continue installation.

Step 4 If the /cdrom/cdrom0 directory is empty because the CD-ROM was not mounted, or if File Manager did not open a window displaying the contents of the CD-ROM, verify that the vold daemon is running by entering:

```
# ps -ef | grep vold | grep -v grep
```

Step 5 If the vold daemon is running, the system displays the vold process identification number. If the system does not display anything, restart the daemon by entering:

```
# /usr/sbin/vold &
```

Step 6 If the vold daemon is running but did not mount the CD-ROM, stop the vold daemon and then restart it. To stop the vold process, you must know the process identification number. If you do not know the process identification number, you can get it by entering:

```
# ps -ef | grep vold | grep -v grep
```

Step 7 Stop the vold process by entering:

```
# kill -15 process_ID_number
```

Step 8 Restart the vold process by entering:

```
# /usr/sbin/vold &
```

Step 9 If you have problems using the vold daemon, enter the following command to mount the CD-ROM:

```
# mount -F hsfs -r ro /dev/dsk/cxydz0sz /cdrom/cdrom0
```

where *x* is the CD-ROM drive controller number, *y* is the CD-ROM drive SCSI ID number, and *z* is the slice of the partition on which the CD-ROM is located.

You have now mounted the CD-ROM drive. For instructions on installation, see [Chapter 2, “Installing and Uninstalling DFM.”](#) For instructions on performing an upgrade, see [Chapter 3, “Upgrading DFM.”](#)

Mounting a Remote CD-ROM Drive

Insert the DFM CD-ROM into the CD-ROM drive of the remote machine and perform Steps 1 through 12 only on the remote machine.

Step 1 Become the superuser by entering the command `su` and the root password at the command prompt, or log in as root. The command prompt changes to the pound sign (#).

Step 2 If the `/cdrom` directory does not already exist, enter:

```
# mkdir /cdrom
```

Step 3 Mount the CD-ROM drive.



Note The `vold` daemon process manages the CD-ROM device and performs the mounting. The CD-ROM might automatically mount onto the `/cdrom/cdrom0` directory.

If you are running File Manager, a separate File Manager window displays the contents of the CD-ROM. From the File Manager, double-click `setup.sh`. The Action: Run box appears. Click **OK** to continue installation.

Step 4 If the `/cdrom/cdrom0` directory is empty because the CD-ROM was not mounted, or if File Manager did not open a window displaying the contents of the CD-ROM, verify that the `vold` daemon is running by entering:

```
# ps -ef | grep vold | grep -v grep
```

Step 5 If the `vold` daemon is running, the system displays `/usr/sbin/vold`. If the system does not display anything, restart the daemon by entering:

```
# /usr/sbin/vold &
```

Step 6 If the vold daemon is running but did not mount the CD-ROM, stop the vold daemon and then restart it. To stop the vold process, you must know the process identification number. If you do not know the process identification number, you can get it by entering:

```
# ps -ef | grep vold | grep -v grep
```

Step 7 Stop the vold process by entering:

```
# kill -15 process_ID_number
```

Step 8 Restart the vold process by entering:

```
# /usr/sbin/vold &
```

Step 9 If you have problems using the vold daemon, enter the following to mount the CD-ROM:

```
# mount -F hsfs -r ro /dev/dsk/cxydz /cdrom/cdrom0
```

where *x* is the CD-ROM drive controller number, *y* is the CD-ROM drive SCSI ID number, and *z* is the slice of the partition on which the CD-ROM is located.

Step 10 Use a text editor to create an /etc/dfs/dfstab file, if one does not exist.

Step 11 Add the following line to the /etc/dfs/dfstab file:

```
share -F nfs -o ro /cdrom/cdrom0
```

Step 12 Make sure your remote machine is enabled as an NFS server by entering:

```
# ps -ef | grep nfs | grep -v grep
```

The output of this command shows whether the /usr/lib/nfs/nfsd and /usr/lib/nfs/mountd daemons are running. If they are not running, enable your machine as an NFS server by entering:

```
# /etc/init.d/nfs.server start
```

If your machine is enabled as an NFS server, enter one of the following:

```
# share
```

or

```
# shareall
```

Step 13 Go to the machine on which you want to install DFM.

- Step 14** Log on as superuser by entering the command `su` and the root password, or log on as root.
- Step 15** Create a `/cdrom` directory, if one does not already exist, by entering:
- ```
mkdir -p /cdrom/cwcs
```
- Step 16** To mount the CD-ROM drive, enter:
- ```
# /usr/sbin/mount -r remote_machine_name:/cdrom/cdrom0 /cdrom/cwcs
```
-

You have now mounted the CD-ROM drive. For instructions on installation, see [Chapter 2, “Installing and Uninstalling DFM.”](#) For instructions on performing an upgrade, see [Chapter 3, “Upgrading DFM.”](#)

Unmounting a CD-ROM Drive

After you complete the DFM installation, you must unmount the CD-ROM drive.

Unmounting a Local CD-ROM Drive

To unmount a local CD-ROM drive:

- Step 1** As root, enter:
- ```
cd
umount /cdrom/cdrom0
eject
```
- Step 2** Remove the CD-ROM and store it in a safe place.
-

## Unmounting a Remote CD-ROM Drive

To unmount a remote CD-ROM drive:

---

- Step 1** As root, enter the following on the local machine:
- ```
# umount /cdrom/cwcs
```
- Step 2** As root, enter the following on the remote machine:
- ```
umount /cdrom/cdrom0
```
- Step 3** Remove the CD-ROM and store it in a safe place.
-



# Licensing

---

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

- [Licensing Overview, page B-1](#)
- [Licensing for a Fresh Installation, page B-2](#)
- [Upgrading Your Evaluation License, page B-4](#)
- [Validating Your Upgrade License, page B-4](#)
- [Licensing Reminders, page B-5](#)

## Licensing Overview

Installation ensures that you possess a registered and a licensed copy of DFM 2.0. The installation script asks the first application installed on Common Services 3.0 to enter licensing information. The following licensing information is shipped with the product, printed on the software claim certificate.

| Field                               | Description                                                                                                                                                                                                                                                                                |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Product Identification Number (PIN) | <p>PIN identifies the type of installation, which may be one of the following:</p> <ul style="list-style-type: none"> <li>• Evaluation installation—For an evaluation copy, licensing details are not required.</li> <li>• Fresh installation.</li> <li>• Upgrade installation.</li> </ul> |
| Product Authorization Key (PAK)     | <p>PAK is used to register DFM 2.0 on Cisco.com and contains resource limitations. A license file is sent to you after you register the PAK on Cisco.com.</p>                                                                                                                              |

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

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

**Note**

You can obtain a license file before or after you install DFM. (See [Registering Your License, page B-3.](#))

## Licensing for a Fresh Installation

The installation script asks the first application installed on Common Services 3.0 for the PIN, PAK, and license file location details.

For instance, when DFM 2.0 is installed over Common Services 3.0, the installer verifies whether or not the system already has the PIN, PAK, and license file details. The details are available if the information was entered earlier using another CiscoWorks application.

If the details are not available, then during the DFM 2.0 installation, the installer requests the PIN and PAK or the license file location.

For an evaluation copy of DFM 2.0, licensing details are not required. When prompted for licensing information, enter **E** (for evaluation).



---

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

---

## Registering Your License

To register your license:

- 
- Step 1** Register the PAK with Cisco.com to get the license file:
- Use this site if you are a registered user of Cisco.com:  
<http://www.cisco.com/go/license>.
  - Use this site if you are *not* a registered user of Cisco.com:  
<http://www.cisco.com/go/license/public>.



---

**Note** The PAK is printed on the software claim certificate.

---

The license file will be e-mailed to you.

- Step 2** Copy the license file to the CiscoWorks Common Services server with read permission for casuser.
- Step 3** Enter the license file location from the CiscoWorks home page. (Select **Common Services > Server > Admin > Licensing**. For more information, see Common Services online help.)
-

# Upgrading Your Evaluation License

You can upgrade your evaluation license to a registered and licensed copy of DFM 2.0.

- 
- Step 1** Contact your Cisco representative about obtaining a PAK.
- Step 2** After obtaining a PAK, follow the instructions in [Registering Your License, page B-3](#). The evaluation copy will be converted to a registered copy of DFM 2.0.
- 

# Validating Your Upgrade License

Proof of Purchase (POP) is required to validate an upgrade license of DFM 2.0. If you purchased an upgrade license, at the end of the DFM installation, you are prompted to run a CLI script to validate the upgrade license. The script in turn prompts you to do one of the following:

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

To run the script, see [Validating the Upgrade, page 3-11](#).

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

# Licensing Reminders

DFM provides reminders in the following circumstances:

- [Evaluation Version: Before Expiry](#), page B-5
- [Purchased Version: No License File](#), page B-5
- [Restricted Version: Device Limit Exceeded](#), page B-6

## Evaluation Version: Before Expiry

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

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

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

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

## Purchased Version: No License File

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

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

DFM 2.0 is fully functional. However, you will continue to receive the alert until you register your license.

## Restricted Version: Device Limit Exceeded

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

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

DFM 2.0 remains functional, but will shortly stop adding devices to managed inventory.



## How is DFM 2.0 Different from DFM 1.2.x?

---

The differences between DFM 2.0 and DFM 1.2 are listed in the following sections:

- [What's New in DFM 2.0?, page C-2](#)
- [Behavior Changes, page C-3](#)
- [User Interface Changes, page C-4](#)
- [Terminology Changes, page C-9](#)
- [Device Group Changes, page C-10](#)
- [Protocol Support Updates, page C-11](#)

# What's New in DFM 2.0?

DFM 2.0 provides a completely new user interface and many new features:

- **Alerts and Activities Display**—DFM 2.0 introduces the Alerts and Activities display, which provides real-time information about the operational status of your network. You can bring up a display and leave it running, providing an ongoing monitoring tool that signals you when something needs attention. When a fault occurs in your network, DFM generates an event or events that are rolled up into an alert. If the alert occurs on an element in your active view (a logical grouping of device groups), it is shown on your Alerts and Activities display.
- **Fault History**—Fault History is installed when you install DFM 2.0. Fault History is integrated with:
  - DFM Alerts and Activities display—You can launch a Fault History report from Alerts and Activities.
  - Common Services Device Center—You can launch a Fault History report for a device that you are troubleshooting in the Device Center.

DFM 2.0 also introduces Search by Group; in addition to searching Fault History by device and by alert or event ID, you can search by device group.

- **Customizable event names**—This feature enables you to change event names to names that are more meaningful to you. These customized names are reflected in both the Alerts and Activities display and any Fault History reports you generate.

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




---

**Note** The SNMP Trap Notifier MIB is no longer used.

---

- **Easier notification configuration**—You can fully configure e-mail notification and trap notification from the DFM user interface without the need to modify the configuration on the management server.
- **SYSLOG notification**—DFM 2.0 adds SYSLOG notification.

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

## Behavior Changes

### Discovery

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

- After you upgrade to DFM 2.0, you will see an increase in the number of ports and interfaces that are managed for the following devices:
  - Cisco MDS 9000 Series Multilayer Switches
  - Cisco SN 5400 Series Storage Routers
  - Cisco Catalyst 2950 Series Switches (2950-ST-24-LRE, 2955C-12, 2955S-12, 2955T-12)
  - Cisco Catalyst 3550 Series Switches (3550-24-PWR-SMI and -EMI)
  - Cisco Catalyst 3750 Series Switches (3750-stack)

DFM 1.2.x did not create ports and interfaces for these devices because they do not support IF-MIB. DFM 2.0 creates ports and interfaces for them whether they support IF-MIB or not.

#### **Additional MIB Support**

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

## **User Interface Changes**

The DFM 2.0 user interface is quite different from that of DFM 1.2.x. To help you access the applications you need to use, [Table C-1](#) lists the click-by-click navigation paths you would use to access functions in DFM 1.2.x. Then it provides the comparable navigation paths to use in DFM 2.0.

Table C-1 DFM 1.2 Navigation Compared to DFM 2.0 Navigation

| DFM 1.2.x                                                                   | DFM 2.0                                                                                                                                                                                  | DFM 2.0 Description                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Device Fault Manager &gt; Administration &gt; Administration Console</b> | <b>Device Fault Manager &gt; Alerts and Activities</b><br><br>(From the Alerts and Activities display, click a device to open a Detailed Device View.)                                   | From the Detailed Device View, you can: <ul style="list-style-type: none"> <li>• View device detail information</li> <li>• Manage and unmanage devices</li> <li>• Acknowledge alerts</li> <li>• Annotate events</li> </ul>                                                                             |
|                                                                             | (From the CiscoWorks home page) <b>Common Services &gt; Device and Credentials &gt; Device Management</b><br><br><b>Device Fault Manager &gt; Device Management &gt; Device Selector</b> | Device management, such as add, import, and delete.<br><br><b>Note</b> In DFM 2.0, you import devices into a Device and Credentials Repository (DCR) that is shared by CiscoWorks applications. You select devices from the DCR (or automatically synchronize devices with the DCR) for DFM to manage. |
|                                                                             | <b>Device Fault Manager &gt; Device Management &gt; Device Details</b>                                                                                                                   | View device inventory.                                                                                                                                                                                                                                                                                 |
|                                                                             | <b>Device Fault Manager &gt; Configuration &gt; Polling and Thresholds</b>                                                                                                               | Configure polling parameters and manage thresholds.                                                                                                                                                                                                                                                    |
|                                                                             | <b>Device Fault Manager &gt; Configuration &gt; Polling and Thresholds &gt; Operations</b>                                                                                               | Reconfigure DFM to use updated polling parameters and threshold values.                                                                                                                                                                                                                                |

Table C-1 DFM 1.2 Navigation Compared to DFM 2.0 Navigation (continued)

| DFM 1.2.x                                                                                       | DFM 2.0                                                                                                                                     | DFM 2.0 Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Device Fault Manager &gt; Monitoring Console</b>                                             | <b>Device Fault Manager &gt; Alerts and Activities</b>                                                                                      | <p>Alarm display from which you can:</p> <ul style="list-style-type: none"> <li>• Launch tools, such as Fault History and Common Services Device Center</li> <li>• Export data to a PDF file or a comma-separated-values file</li> <li>• Print data</li> </ul> <p>You can also change the display to show the information that interests you most, as follows:</p> <ul style="list-style-type: none"> <li>• Select and create views or groups of device groups; use a view that contains the device groups of interest to you.</li> <li>• Filter the display to show alerts based on their severity, status, and originating device.</li> </ul> |
| <b>Device Fault Manager &gt; Administration &gt; Device Discovery &gt; Change Probe</b>         | <b>Device Fault Manager &gt; Device Management &gt; Device Selector</b><br><br><b>Note</b> The change probe process is obsolete in DFM 2.0. | <p>Select devices manually or configure DFM to automatically synchronize device inventory with Device and Credentials Repository (DCR).</p> <p><b>Note</b> Applications on different servers can use the same master DCR. For more information, see <i>User Guide for CiscoWorks Common Services</i>.</p>                                                                                                                                                                                                                                                                                                                                       |
| <b>Device Fault Manager &gt; Administration &gt; Device Discovery &gt; Rediscovery Schedule</b> | <b>Device Fault Manager &gt; Configuration &gt; Other Configurations &gt; Rediscovery Schedule</b>                                          | <ul style="list-style-type: none"> <li>• Edit the default rediscovery schedule.</li> <li>• Create additional rediscovery schedules.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

Table C-1 DFM 1.2 Navigation Compared to DFM 2.0 Navigation (continued)

| DFM 1.2.x                                                                    | DFM 2.0                                                                              | DFM 2.0 Description                                                                                                                                                                                        |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device Fault Manager > Administration > Trap Configuration > Trap Receiving  | Device Fault Manager > Configuration > Other Configurations > SNMP Trap Receiving    | Change the port number that DFM uses to listen for SNMP traps.<br><br><b>Note</b> Although the SNMP trap adapter file used in DFM 1.2 is still present in the DFM 2.0 filesystem, DFM 2.0 does not use it. |
| Device Fault Manager > Administration > Trap Configuration > Trap Forwarding | Device Fault Manager > Configuration > Other Configurations > SNMP Trap Forwarding   | Configure hostnames and port numbers for trap forwarding.<br><br><b>Note</b> Although the SNMP trap adapter file used in DFM 1.2 is still present in the DFM 2.0 filesystem, DFM 2.0 does not use it.      |
| Device Fault Manager > Administration > Fault Notification > File Notifier   | —                                                                                    | If you need to log events to a file, contact the Technical Assistance Center for the workaround for CSCsa83426.                                                                                            |
| Device Fault Manager > Administration > Fault Notification > Mail Notifier   | Device Fault Manager > Notification Services > E-Mail Notification                   | Configure e-mail notifications for alarms.<br><br><b>Note</b> Although the mail notifier file used in DFM 1.2 is still present in the DFM 2.0 filesystem, DFM 2.0 does not use it.                         |
| Device Fault Manager > Administration > Fault Notification > Trap Notifier   | Device Fault Manager > Notification Services > Trap Notification                     | Configure trap notifications for alarms.<br><br><b>Note</b> Although the trap notifier file used in DFM 1.2 is still present in the DFM 2.0 filesystem, DFM 2.0 does not use it.                           |
| Device Fault Manager > Administration > Fault History Database Sizing        | Device Fault Manager > Configuration > Other Configurations > Daily Purging Schedule | Trim the Fault History database.<br><br><b>Note</b> DFM 2.0 keeps 31 days of history and trims the database daily at the time you specify.                                                                 |

Table C-1 DFM 1.2 Navigation Compared to DFM 2.0 Navigation (continued)

| DFM 1.2.x                                                                                                                                                          | DFM 2.0                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | DFM 2.0 Description                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| <p><b>Device Fault Manager &gt; Fault History:</b></p> <ul style="list-style-type: none"> <li>• Search by Devices</li> <li>• Search by Fault Conditions</li> </ul> | <p><b>Device Fault Manager &gt; Fault History:</b></p> <ul style="list-style-type: none"> <li>• Alert Filtering               <ul style="list-style-type: none"> <li>– Search Alarm ID</li> <li>– Search by Device</li> <li>– Search by Group</li> </ul> </li> <li>• Event Filtering               <ul style="list-style-type: none"> <li>– Search by Event ID</li> <li>– Search by Device</li> <li>– Search Alert ID</li> <li>– Search by Group</li> </ul> </li> </ul> | <p>Generate a 31-day Fault History report based on search criteria.</p>              |
|                                                                                                                                                                    | <p><b>Device Fault Manager &gt; Alerts and Activities &gt; Tools &gt; Fault History</b></p>                                                                                                                                                                                                                                                                                                                                                                             | <p>Generate a 24-hour Fault History report for all alerts in your current view.</p>  |
|                                                                                                                                                                    | <p><b>Device Fault Manager &gt; Alerts and Activities</b></p> <p>Click an alert ID. The Alerts and Activities Detail display appears. In the Tools column next to the device component of interest, select <b>Fault History</b>.</p>                                                                                                                                                                                                                                    | <p>Generate a 24-hour Fault History report for all events on a device component.</p> |

# Terminology Changes

Terminology has changed since DFM 1.2 as follows:

- *Symptom* is replaced by *event*. Events are rolled up into *alerts*.
- *Compound* is not used and there is no replacement. A compound differs from an alert; there could be multiple compounds on a single device, whereas an alert is a roll-up of all events for a device.
- Levels of device certification (*validated*, *certified*, *template*, *undiscovered*, *uncertified*) are replaced by new device states:
  - *Known*—The device is successfully imported and fully managed by DFM. (Corresponds to *validated* and *certified*).
  - *Learning*—DFM is discovering the device. This is the initial state, when the device is first added to DFM or is being rediscovered.
  - *Questioned*—DFM cannot manage the device. (Can sometimes correspond to *undiscovered*.)
  - *Pending*—The device is being deleted. DFM is waiting for confirmation from all of its data collectors before purging the device and its details.
  - *Unknown*—The device is not supported by DFM. (Corresponds to *unsupported* and *uncertified*).
- *Manage* is replaced by *Activate*; *unmanage* is replaced by *suspend*.
- When a DFM 1.2 fault was *acknowledged*, it was removed from the Alarm Log. In DFM 2.0, when an event is *acknowledged*, it remains in the Alerts and Activities display.
- DFM 1.2 assigned devices to groups based on *matching criteria*. DFM 2.0 assigns devices to groups based on *group rules*.
- DFM 2.0 eliminates the term *device class* and introduces *device type*.
- DFM 1.2 displayed managed elements organized by *device class*—for example: *Bridge*, *Host*, *Hub*, *MSFC*, *Probe*, *Router*, *RSM*, *Switch*. DFM 2.0 displays devices organized by *device group*:
  - Inventory device groups are organized by device state.
  - Polling and Threshold groups are organized by device type; for example, Routers, Switches and Hubs, and Voice and Telephony. (For more information, see *User Guide for Device Fault Manager*.)

# Device Group Changes

In DFM 1.2, you could browse the device inventory by selecting a device class. In DFM 2.0, you can examine device groups.

**Table C-2**      **Device Group Changes**

| <b>DFM 1.2 Device Classes</b> | <b>DFM 2.0 Device Groups</b>                                                                                                                                                                          |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bridge                        | Wireless                                                                                                                                                                                              |
| Host                          | Cisco Interfaces and Modules<br>Content Networking<br>Network Management<br>Voice and Telephony                                                                                                       |
| Hub                           | Switches and Hubs                                                                                                                                                                                     |
| MSFC                          | Cisco Interfaces and Modules                                                                                                                                                                          |
| Probe                         | Cisco Interfaces and Modules<br>Network Management                                                                                                                                                    |
| Router                        | Broadband Cable<br>Cisco Interfaces and Modules<br>Content Networking<br>Routers<br>Security and VPN<br>Switches and Hubs<br>Universal Gateways and Access Servers<br>Voice and Telephony<br>Wireless |
| RSFC                          | Cisco Interfaces and Modules                                                                                                                                                                          |
| RSM                           | Cisco Interfaces and Modules                                                                                                                                                                          |

**Table C-2** Device Group Changes (continued)

| DFM 1.2 Device Classes | DFM 2.0 Device Groups                                                                                                                                                  |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch                 | Content Networking<br>DSL and Long Reach Ethernet (LRE)<br>Optical Networking<br>Routers<br>Storage Networking<br>Switches and Hubs<br>Wireless<br>Voice and Telephony |
| Terminal Server        | Universal Gateways and Access Servers                                                                                                                                  |

## Protocol Support Updates

**Table C-3** Protocols

| Protocol | DFM 1.2.x                                                                                                                                      | DFM 2.0                                                                                                                                                                                                                                                                                                                                                                          |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSL      | Not SSL-compliant                                                                                                                              | Uses SSL protocol between the server and the browser. You enable and disable SSL for the server. See <i>User Guide for Common Services</i> .                                                                                                                                                                                                                                     |
| SNMP     | <ul style="list-style-type: none"> <li>Supports SNMPv1 and SNMPv2 for polling and receiving traps</li> <li>Forwards traps as SNMPv2</li> </ul> | <ul style="list-style-type: none"> <li>Supports SNMPv1 and SNMPv2 for polling and receiving traps.</li> <li>Forwards traps as SNMPv2.</li> <li>Partially supports SNMPv3:             <ul style="list-style-type: none"> <li>Uses SNMPv3 protocol between the server and the device.</li> <li>Supports the Authentication No Privacy (AuthNoPriv) option.</li> </ul> </li> </ul> |





# Configuring DFM with Cisco Secure ACS

---

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

- [CiscoWorks Login Module, page D-1](#)
- [CiscoWorks Server Authentication Roles, page D-3](#)
- [Before You Begin: Integration Notes, page D-4](#)
- [Configuring DFM on Cisco Secure ACS, page D-6](#)
- [Verifying the DFM and Cisco Secure ACS Configuration, page D-6](#)

## CiscoWorks Login Module

Common Services provides security mechanisms for authenticating users of CiscoWorks applications. You can configure the CiscoWorks login module to use one of the following modes of user authentication and authorization:

- **Non-ACS**—In this mode, the CiscoWorks server provides authentication and authorization services.
- **ACS**—In this mode, a Cisco Secure Access Control Server (ACS) provides authentication and authorization services. To use this mode, you must have a Cisco Secure ACS installed on your network. The supported versions of Cisco Secure ACS for Windows are 3.2, 3.2.3 and 3.3.2.

If you are using ACS 3.2.3, we recommend that you install the Admin HTTPS PSIRT patch:

1. Go to <http://www.cisco.com/kobayashi/sw-center/ciscosecure/cs-accs.shtml>
2. Click the Download Cisco Secure ACS Software (Windows) link. You will find the link to the Admin HTTPS PSIRT patch in the table.

**Note**

---

You can integrate DFM with Cisco Secure ACS only if they are installed on separate systems because DFM must be configured as an AAA client for Cisco Secure ACS.

---

In ACS mode, *fallback* is provided for authentication only. (Fallback options allow you to access CiscoWorks if the login module fails, or you accidentally lock yourself or others out.) If authentication with ACS fails, CiscoWorks does the following:

1. Tries authentication using non-ACS mode (CiscoWorks local mode).
2. If non-ACS authentication is successful, presents you with a dialog box with instructions to change the login mode to CiscoWorks local. (You can do so only if you have permission to perform that operation in non-ACS mode.)

**Note**

---

You will not be allowed to log in if authentication fails in non-ACS mode.

---

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

# CiscoWorks Server Authentication Roles

In ACS mode, by default the CiscoWorks server provides the five roles listed here, from least privileged to most privileged:

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

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

- **Approver**—A user with this role has the privilege to approve all DFM tasks and can also perform all the Help Desk tasks.

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

- **Network Operator**—A user with this role has the privilege to perform all tasks that involve collecting data from the network. The user can also perform all Approver tasks. The user does not have write access on the network.

For example, this user can configure logging parameters.



---

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

---

- **Network Administrator**—A user with this role has the privilege to change the network. The user can also perform Network Operator tasks.

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

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

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



---

**Note** If you use Cisco Secure ACS to modify these roles, removing tasks or reassigning tasks from one role to another, the Permission Report will not reflect your changes.

---

You can modify roles on Cisco Secure ACS.

- 
- Step 1** Select **Shared Profile Components > Device Fault Manager**.
- Step 2** Click the DFM role that you want to modify.
- Step 3** Select the DFM tasks that suit your business workflow and needs.
- Step 4** Click **Submit**.
- 

**Note**

If desired, you can also create new roles on Cisco Secure ACS.

---

## Before You Begin: Integration Notes

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

- CiscoWorks server and Cisco Secure ACS integration should be performed only *after* installing all LAN Management Solution (LMS) applications.
- If you have installed your application after configuring the CiscoWorks Login Module to ACS mode, then the application users are not granted any permissions; however, the application is registered to Cisco Secure ACS. On the Cisco Secure ACS server, you must assign the appropriate permissions to the application.

See [Configuring DFM on Cisco Secure ACS, page D-6](#).

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

**Note**

This is applicable if you are using Cisco Secure ACS version 3.2.3 or earlier.

---

- You must create roles in Cisco Secure ACS for each LMS application that is running on the CiscoWorks server.  
For example: you must create roles in Cisco Secure ACS for DFM. These roles are not shared by any other LMS application.
- The roles that you create in Cisco Secure ACS are shared across all CiscoWorks servers that are configured to the same Cisco Secure ACS.  
For example: You have configured 10 CiscoWorks servers with a Cisco Secure ACS, and you have created a role in Cisco Secure ACS for DFM (say, *DFMSU*). This role is shared by DFM applications running on all 10 CiscoWorks servers.
- A user can have different access privileges for different LMS applications.  
For example: A user, *CWSU*, can have the following privileges:
  - System Administrator for Common Services
  - Approver for RME
  - Network Operator for Campus Manager
  - Network Administrator for DFM
  - Help Desk for Internet Performance Monitor (IPM)
- On CiscoWorks, you must configure the following:
  - Set AAA Mode to ACS—You will need to supply the following information obtained from Cisco Secure ACS to complete this task: IP address or hostname, port, admin username and password, and shared secret key.
  - Setup System Identity Setup username.
- On Cisco Secure ACS, you must configure a user with the same username as the CiscoWorks server System Identity Setup user. For DFM, that user must have Network Administrator privileges on Cisco Secure ACS.

See the chapter “Configuring the Server” in *User Guide for CiscoWorks Common Services* for details on configuring the CiscoWorks server in ACS mode.

# Configuring DFM on Cisco Secure ACS

After you complete setting the CiscoWorks server to ACS mode with Cisco Secure ACS, perform the following tasks on Cisco Secure ACS:

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

**Note**

---

If you integrated CiscoWorks Common Services with Cisco Secure ACS *before* installing DFM, you must configure ACS mode again and register all applications with ACS. See Common Services online help.

---

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

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

3. Assign the appropriate DFM privileges to the user or group.

For DFM, you must ensure that a user with the same name as the CiscoWorks server System Identity Setup user is configured on Cisco Secure ACS and has Network Administrator privileges.

## Verifying the DFM and Cisco Secure ACS Configuration

After performing the tasks in [Configuring DFM on Cisco Secure ACS, page D-6](#), verify the configuration as follows:

1. Log in to CiscoWorks with the username defined in Cisco Secure ACS.
2. Try to perform tasks, to ensure that you can perform only those tasks that you are entitled to perform based on your privileges on Cisco Secure ACS.

For example: If your privilege is Help Desk, then:

- You should be able to view the device summary.
  - You should not be able to select devices for DFM to manage.
3. Based on the Network Device setting for the user or group on Cisco Secure ACS, you can view only certain devices on the CiscoWorks server.

**Note**

---

For a list of DFM displays that perform device-based filtering, see DFM-specific online help in Cisco Secure ACS.

---





## INDEX

---

## A

### ACS

- configuring [4-4, D-1 to D-7](#)
- new installation and [1-4, 2-6, 2-8](#)
- port [2-3](#)
- reinstallation and [2-11, 2-13, 3-9, 3-10](#)
- upgrade and [1-7, 3-9, 3-10](#)

### adapters

- files, no longer used [C-7](#)
- installing [1-2, 2-16 to 2-20](#)
- removing [2-20](#)
- upgrading [2-16 to 2-20](#)

### audience for this document [xi](#)

### authentication

- ACS mode [D-1](#)
- non-ACS mode [D-1](#)

---

## B

### bundles, DFM and [1-3](#)

---

## C

### cautions

- significance of [xii](#)

### Cisco Secure ACS [D-1](#)

- DFM integration with [D-1](#)
- supported versions [D-1](#)

### client requirements [1-11](#)

### configuring DFM (minimum setup)

- further configuration tasks [4-19](#)
- SNMP trap receiving and forwarding, configuring
  - trap receiving port, updating [4-13](#)
  - traps, enabling devices to send [4-13](#)

---

## D

### default

- installation directory [2-7, 3-10](#)

### device

- discovery [C-3](#)
  - rediscovery schedule [4-11](#)
  - troubleshooting [4-12](#)
- states, defined [C-9](#)

## Device and Credentials Repository

- configuring [4-5](#)
- overview [1-13](#)
- using [4-6](#)

## devices, managing

- adding to DFM [4-6](#)
- importing
  - to DCR [4-6](#)
  - troubleshooting import [4-10](#)

devices, supported [1-15](#)

## DFM

- installing [2-4 to 2-10](#)
- reinstalling [2-11 to 2-15](#)
- uninstalling [2-15 to 2-16](#)
- upgrading [3-7 to 3-13](#)

## DFM 2.0 updates

- additional MIB support [C-4](#)
- discovery behavior [C-3](#)
- navigation paths [C-4](#)

## DfmBroker

- limiting access [2-8, 2-13](#)
- specifying new DFM [2-16](#)
- specifying remote HPOV-NetView adapter [2-20](#)

## discovery

- error messages [4-12](#)

## DNS

- registering hostnames with [2-10, 2-12, 2-14, 2-20](#)
- resolution [4-12](#)

documentation [xii](#)

- additional online [xv](#)
- audience for this [xi](#)
- typographical conventions in [xi](#)

---

**E**

## error messages

- device import [4-12](#)

---

**H**

## help

- online documentation [xv](#)

HP OpenView versions [1-14](#)

## HPOV-NetView adapter

- remote [2-20](#)

---

**I**

## importing devices

- troubleshooting [4-10](#)

## installation

- default directory [2-7, 3-10](#)
- paths [1-8](#)

## installing

- adapters [2-16 to 2-20](#)
- DFM [2-4 to 2-10](#)
- DFM with a bundle [1-3](#)

---

**L**

## license

- evaluation, upgrading **B-4**
- Product Authorization Key **B-2**
- Product Identification Number **B-2**
- registering **B-3**

## logs

- DFM installation **2-10**
- DFM reinstallation **2-15**
- DFM uninstallation **2-16**
- HPOV-NetView remote adapter  
installation **2-18, 2-20**

---

**M**

## MIBs

- CISCO-FRAME-RELAY-MIB **C-4**
- CISCO-PAGP-MIB **C-4**
- IF-MIB **C-4**
- OLD-CISCO-CHASSIS-MIB **C-3**

## mounting and unmounting Solaris

## mounting

- a local CD-ROM drive **A-1**
- a remote CD-ROM drive **A-3**

## unmounting

- a local CD-ROM drive **A-5**
- a remote CD-ROM drive **A-6**

---

**N**NetView versions **1-14**NMS integration, supported **1-14**

---

**O**OpenView (HP) versions **1-14**

## overview

- DFM **1-1**
- product **1-1**

---

**P**patches recommended **1-10**

## ports

- forwarding **4-16**
- listening **4-16**
- occupied **2-10**

## preparing to install DFM

- client requirements **1-11**
- installation paths **1-8**
- server requirements and  
recommendations **1-8**
- Solaris patches **1-10**
- supported devices **1-15**
- supported NMS integration **1-14**

## Product

- Authorization Key **B-2**
- Identification Number **B-2**

---

**Q**

Questioned device state, troubleshooting [4-12](#)

---

**R**

recommendations

client [1-11](#)

server [1-8](#)

recommended patches [1-10](#)

reinstalling DFM [2-11 to 2-15](#)

removing

remote adapters [2-20](#)

roles

modifying in Cisco Secure ACS [D-4](#)

---

**S**

security

Cisco Secure ACS [D-4](#)

CiscoWorks

login module [D-1](#)

roles [D-3](#)

configuring [4-4](#)

new installation [2-8](#)

reinstallation [2-13](#)

SSL compliance [C-11](#)

server

limiting access [2-8, 2-13](#)

requirements [1-8 to 1-9](#)

SNMP

AuthNoPriv [C-11](#)

configuring

retries [4-10](#)

timeout [4-10](#)

supported versions [C-11](#)

timeout [4-12](#)

SNMP trap receiving and forwarding,  
configuring

trap receiving port, updating [4-13](#)

traps, enabling devices to send [4-13](#)

Solaris

mounting

a local CD-ROM drive [A-1](#)

a remote CD-ROM drive [A-3](#)

patches [1-10](#)

unmounting

a local CD-ROM drive [A-5](#)

a remote CD-ROM drive [A-6](#)

SSL compliance [C-11](#)

supported

Cisco Secure ACS versions [D-1](#)

client environments [1-11](#)

devices [1-15](#)

HP OpenView versions [1-15](#)

supported (continued)

NetView versions [1-15](#)

NMS integration [1-14](#)

server environments [1-8](#)

SNMP versions [C-11](#)

---

## T

timeout

Data Collector [4-12](#)

SNMP [4-12](#)

    configuring [4-10](#)

traps

    changing port [1-15](#)

troubleshooting

    device import [4-10](#)

        device credentials, changing [4-10](#)

        devices, rediscovering [4-11](#)

        discovery status, viewing [4-11](#)

        SNMP timeout and retries, modifying [4-10](#)

typographical conventions in this document [xi](#)

---

## U

uninstalling

    adapters [2-20](#)

    DFM [2-15 to 2-16](#)

unmounting

    a local CD-ROM drive [A-5](#)

    a remote CD-ROM drive [A-6](#)

upgrading

    DFM [3-7 to 3-13](#)

    exporting DFM 1.2 information [3-12](#)

users

    authentication [D-3](#)

    roles [D-4](#)

    System Identity Setup User [D-4](#)

