User Guide for
Device Fault Manager
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-7816266=
Text Part Number: 78-16266-01
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

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

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

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

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

CCIP, CCSP, the Cisco Arrow logo, the Cisco Powered Network mark, Cisco Unity, Follow Me Browsing, FormShare, 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 Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, IP Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratum, 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 U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

User Guide for Device Fault Manager
Copyright © 2000-2004 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’ website: 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 Expo>>

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.
How Will I Use DFM for Day-to-Day Operations? 1-7
  What Is Alerts and Activities? 1-8
  What Is Device Management? 1-8
  What Is Notification Services? 1-9
  What Is Fault History? 1-10
  What Is Configuration? 1-11

How Does DFM Work? 1-11
  Users Perform Device Management and Configuration 1-11
  DFM Performs Ongoing Monitoring, Analysis, and Notification 1-13
  Users Respond to Notifications and Alerts 1-15

CHAPTER 2
Getting Started with DFM 2-1
  Working with DFM Windows 2-1
    Using Help 2-3
    Understanding the Dates and Times Displayed 2-3
  Using Tabular Displays 2-4
    Paging and Sorting Tabular Displays 2-5
    Viewing Data from Tabular Displays with Over 2000 Records 2-6
    Exporting Data from Tabular Displays 2-6
    Printing Tabular Displays 2-7
  Selecting Objects and Groups 2-7
    Selecting Objects Organized by Group Management 2-8
    Selecting Objects Organized by Discovery Status 2-11
  Understanding Your User Role 2-12
  Responding to Security Alerts 2-12
  Responding to Messages About Device Limits 2-13
CHAPTER 3

Using the Alerts and Activities Display 3-1
- How to Use the Alerts and Activities Display 3-1
- Starting the Alerts and Activities Display 3-2
  - Understanding the Layout of the Alerts and Activities Display 3-4
- Getting Alert Details 3-6
- Customizing the Alerts and Activities Display 3-10
  - Selecting Views for Alerts and Activities 3-10
  - Filtering Alerts and Activities 3-11
- Getting Event Details 3-11
  - Starting the Alerts and Activities Detail Page 3-12
  - Understanding the Layout of the Alerts and Activities Detail Page 3-14
    - Command Button Area 3-16
  - Viewing Events Associated with an Alert 3-17
  - Viewing Event Properties 3-19
- Getting Device Information (Detailed Device View) 3-20
  - Starting the Detailed Device View 3-20
  - Understanding the Layout of the Detailed Device View 3-23
  - Detailed Device View Examples 3-24
- Suspending Device Monitoring 3-26
  - Suspending/Resuming Devices 3-27
  - Suspending/Resuming a Device Component 3-28
- Acknowledging, Annotating, and Sending E-Mail Notifications of Alerts 3-29
  - Acknowledging an Alert 3-30
  - Annotating an Alert 3-30
  - Sending E-Mail in Response to an Alert 3-31
CHAPTER 4

Using Device Management 4-1

Getting Started with Device Management 4-2

Types of Devices and Device Elements that DFM Monitors 4-3

Ports and Interfaces that DFM Manages 4-5

Listing Ports and Interfaces in the DFM Inventory 4-5

Understanding the Device and Credentials Repository 4-8

Events That Trigger DCR and DFM Synchronization 4-9

DCR Masters and Slaves 4-10

Understanding the Device Summary and Device States 4-10

Importing Devices into DFM 4-12

Importing Devices from the DCR 4-12

How DFM Identifies Devices Imported from the DCR 4-12

How DFM Handles Containing and Contained Devices 4-13

Automatically Importing DCR Devices 4-15

Manually Importing DCR Devices Using the Device Selector 4-16

Determining Which Devices Are in DCR But Not in DFM 4-17

Importing Devices from DFM 1.2.x 4-18

Viewing Alias (Duplicate) Devices 4-18

Verifying Device Import Using Discovery Status 4-19

Troubleshooting Device Import Using Discovery 4-20

Exporting Devices 4-24

Editing Device Configuration and Credentials 4-26

Rediscovering and Deleting Devices 4-26

Rediscovering Devices 4-29

Deleting Devices 4-30

Viewing Device Details 4-32

Understanding the Device Details Display 4-33

Modifying SNMP Timeout and Retries 4-34
CHAPTER 5

Using Notification Services 5-1
Understanding Notifications and Subscriptions 5-2
Customizing the Names of DFM Events 5-5
Configuring Event Sets and Notification Groups for Subscriptions 5-6
  Configuring Event Sets 5-7
  Configuring Notification Groups 5-8
Managing SNMP Trap Notifications 5-10
  Adding an SNMP Trap Notification Subscription 5-12
  Editing an SNMP Trap Notification Subscription 5-13
  Suspending an SNMP Trap Notification Subscription 5-14
  Resuming an SNMP Trap Notification Subscription 5-15
  Deleting an SNMP Trap Notification Subscription 5-15
Managing E-Mail Notifications 5-16
  Adding an E-Mail Notification Subscription 5-17
  Editing an E-Mail Notification Subscription 5-19
  Suspending an E-Mail Notification Subscription 5-21
  Resuming an E-Mail Notification Subscription 5-21
  Deleting an E-Mail Notification Subscription 5-22
Managing Syslog Notifications 5-22
  Adding a Syslog Notification Subscription 5-24
  Editing a Syslog Notification Subscription 5-25
  Suspending a Syslog Notification Subscription 5-27
  Resuming a Syslog Notification Subscription 5-27
  Deleting a Syslog Notification Subscription 5-28
CHAPTER 6

Using Fault History 6-1
Getting Started with Fault History 6-1
Starting Fault History 6-3
Starting Fault History from the Alerts and Activities Display 6-3
Generating a 24-Hour Report on All Alerts in the Current View 6-4
Generating a 24-Hour Report on All Events on a Device Component 6-5
Starting Fault History from the DFM Home Page 6-5
Getting All Stored Information on an Alert 6-6
Getting All Stored Fault History on an Event 6-9
Understanding the Fault History: Alerts and Activities Display 6-12
Understanding the Fault History: Events Display 6-14

PART 2

Configuring and Administering DFM

CHAPTER 7

Configuring and Administering DFM (Basic) 7-1
Using DFM Configuration 7-2
Applying Changes 7-4
Performing Scheduling Tasks 7-5
Configuring the Daily Purging Schedule 7-6
Configuring Rediscovery Schedules 7-7
Suspending a Rediscovery Schedule 7-7
Resuming a Rediscovery Schedule 7-8
Adding a Rediscovery Schedule 7-8
Editing a Rediscovery Schedule 7-9
Deleting a Rediscovery Schedule 7-10
Configuring SNMP Trap Receiving and Forwarding 7-10
Enabling Devices to Send Traps to DFM 7-11
Enabling Cisco IOS-Based Devices to Send Traps to DFM 7-11
Enabling Catalyst Devices to Send SNMP Traps to DFM 7-12
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs</td>
</tr>
<tr>
<td>Updating the SNMP Trap Receiving Port</td>
</tr>
<tr>
<td>Configuring SNMP Trap Forwarding</td>
</tr>
<tr>
<td>Configuring a Default SMTP Server</td>
</tr>
</tbody>
</table>

**CHAPTER 8**

**Managing Groups** 8-1

- Understanding DFM Groups 8-1
  - Groups and ACS 8-4
  - Working with System Defined Groups 8-4
  - Common Services System Defined Groups 8-4
  - DFM System Defined Groups 8-6
  - Working with Customizable Groups 8-7
- Using Group Management 8-9
- Editing and Creating Groups 8-11
  - Editing a Group 8-12
  - Creating a Group 8-16
  - Understanding Rules 8-20
  - Finalizing Group Membership 8-26
  - Viewing the Group Summary 8-26
- Viewing Group Details 8-27
- Viewing Membership Details 8-29
- Refreshing Membership 8-30
- Deleting Groups 8-31

**CHAPTER 9**

**Configuring Views for the Alerts and Activities Display** 9-1

- Getting Started with Views 9-1
- Creating a View 9-2
- Activating and Deactivating a View 9-4
Modifying a View  9-5
Deleting a View  9-7

CHAPTER 10

Configuring Polling and Thresholds  10-1
Overview of Polling and Thresholds  10-1
Which Settings Are Applied to Devices, Ports, and Interfaces?  10-2
Which Polling Settings Are Applied?  10-3
Which Threshold Settings Are Applied?  10-3
What Are Customizable Groups?  10-3
Setting Priorities  10-4
How Does DFM Prioritize Groups for Polling and Thresholds?  10-6
Viewing the Overriding Group—Examples  10-9
How Can I Set Parameters for a Device, Interface, or Port?  10-11

Updating Polling Parameters and Thresholds  10-13
Selecting Groups  10-14
Managing Polling Parameters  10-18
Viewing Polling Parameters  10-18
Editing Polling Parameters  10-20
Understanding What Happens When You Apply Changes  10-23
Restoring Factory Setting Polling Parameters  10-23
Device Polling Settings  10-24

Managing Thresholds  10-26
Viewing Thresholds  10-26
Editing Thresholds  10-28
Restoring Factory Settings for Thresholds  10-30
Threshold Categories for Devices, Interfaces, and Ports  10-31
Threshold Definitions  10-34
Backup Interface Support  10-34
Dial-On-Demand Interface Support  10-34
Environment 10-35
Generic Interface/Port Performance 10-35
Interface/Port Flapping 10-38
Processor and Memory 10-38
Reachability 10-39
Threshold Parameter Values and Events 10-40

CHAPTER 11
Administering DFM (Advanced) 11-1
Ports and Protocols that DFM Uses 11-1
Security Considerations 11-3
File Ownership and Protection 11-3
Secure Socket Layer (SSL) 11-3
SNMPv3 11-4
Working with Firewalls 11-4
Device Support 11-5
System Administration 11-5
Registering Additional DFM Servers with the CiscoWorks Home Page 11-6
Configuring Users (ACS and Non-ACS) 11-7
Configuring Users Using CiscoWorks Local Mode 11-8
Configuring Users Using ACS Mode 11-8
Using DFM in ACS Mode 11-9
Creating Self-Signed Security Certificates Yearly 11-12
Backing Up and Restoring DFM Data 11-14
Changing the Password for DFM Databases 11-16
Configuring Logging 11-17
Viewing and Maintaining Log Files 11-18
Starting and Stopping DFM Processes 11-21
Registering and Unregistering DFM Processes 11-24
Example: Specifying Clients That Can Connect to DFM 11-27
Example: Configuring the DFM Server to Use a Privileged Port 11-28
Preface

This manual describes Device Fault Manager (DFM) and provides instructions for using and administering it.

Audience

The audience for this document includes:
- Network administrators and operators who monitor the status of the IP fabric
- System administrators who maintain and configure software systems

Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Item</th>
<th>Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands and keywords</td>
<td><strong>boldface</strong> font</td>
</tr>
<tr>
<td>Variables for which you supply values</td>
<td><em>italic</em> font</td>
</tr>
<tr>
<td>Displayed session and system information</td>
<td><strong>screen</strong> font</td>
</tr>
<tr>
<td>Information you enter</td>
<td><strong>boldface</strong> <strong>screen</strong> font</td>
</tr>
<tr>
<td>Variables you enter</td>
<td><em>italic</em>* <strong>screen</strong> font</td>
</tr>
<tr>
<td>Menu items and button names</td>
<td><strong>boldface</strong> font</td>
</tr>
</tbody>
</table>
Product Documentation

Table 1 describes the product documentation that is available.

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Available Formats</th>
</tr>
</thead>
</table>
| Release Notes for Device Fault Manager on Windows | • Printed document that was included with the product.  
| Release Notes for Device Fault Manager on Solaris | • Printed document that was included with the product.  
### Table 1  Product Documentation (continued)

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Available Formats</th>
</tr>
</thead>
</table>
| Installation and Setup Guide for Device Fault Manager on Windows | • PDF on the product CD-ROM.  
• Printed document available by order (part number DOC-7816267=).1 |
| Installation and Setup Guide for Device Fault Manager on Solaris | • PDF on the product CD-ROM.  
• Printed document available by order (part number DOC-7816268=).1 |
| User Guide for Device Fault Manager                       | • PDF on the product CD-ROM.  
• Printed document available by order (part number DOC-7816266=).1 |
| Context-sensitive online help                             | • Select an option from the navigation tree, then click Help.  
• Click the Help button in the dialog box.  
**Note** Most DFM dialog boxes do not include a Help button. |

1. See the “Obtaining Documentation” section on page xix.
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

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Available Formats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Notes for CiscoWorks Common Services 3.0 on Windows</td>
<td>• Printed document that was included with the product.</td>
</tr>
<tr>
<td>Release Notes for CiscoWorks Common Services 3.0 on Solaris</td>
<td>• Printed document that was included with the product.</td>
</tr>
<tr>
<td>User Guide for CiscoWorks Common Services</td>
<td>• PDF on the product CD-ROM.</td>
</tr>
<tr>
<td></td>
<td>• Printed document available by order (part number DOC-7816571=).¹</td>
</tr>
</tbody>
</table>

1. See the “Obtaining Documentation” section on page xix.
Additional Information Online

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.

Your application might support incremental device updates (IDUs) or service packs. An IDU/service pack is a software package that enables an application to support new devices. An IDU/service pack might also contain bug fixes. You can download IDUs/service packs and their Readme files by logging into Cisco.com at http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm.

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, select Common Services > Software Center > Software Update.

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

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:

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product
documentation from the Ordering tool:
- 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:


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:

Part 1

Using DFM
Introduction

These topics provide an overview of Device Fault Manager (DFM):

- What Is DFM?, page 1-1
- What’s New in DFM 2.0?, page 1-3
- Is DFM Ready to Use?, page 1-5
- How Will I Use DFM for Day-to-Day Operations?, page 1-7
- How Does DFM Work?, page 1-11

What Is DFM?

DFM offers the following real-time assistance to network operations personnel:

- Monitoring and displaying the operational health of the network
- Analyzing events that occur in these environments and determining when a probable fault has occurred
- Notifying users of alert conditions through an online display and through other notification services

Figure 1-1 shows the series of activities that DFM performs when a user imports a Cisco 3640 router into DFM. The figure also shows how a user can confirm that these activities have occurred.
**What Is DFM?**

DFM performs:
- **Discovery** and adds devices to inventory
- Assigns device components to DFM system-defined groups
- Prepares to poll devices with settings and values of overriding group

**Device Management**
- Device details for the router:
  - Status: Known

**Group Management**
- System defined groups in which the 3640 router components are members:
  - Routers
  - Interface Groups/10-100MB Ethernet
  - Interface Groups/Others

**Polling and Thresholds**
- Overriding group for the router:
  - Polling settings: Routers
  - Threshold Settings: 10-100MB Ethernet
  - Threshold Settings: Others
DFM performs the following tasks after a user imports a device:

- DFM obtains basic information from the Device and Credentials Repository (DCR), which was supplied when the device was added to the DCR.
- DFM discovers the device—You can see the results of this discovery using Device Management.
- DFM assigns the device to system-defined groups—You can see which devices are members of each system-defined group using Group Management; the Membership Details page for any group will display them.
- DFM starts to poll the device—You can see alerts for a device on the Alerts and Activities display when events occur on the device. You can see the polling and threshold group that DFM uses for DFM polling parameters and threshold values for the device on the Polling Parameters Summary and Thresholds Summary pages.

When you first start to use DFM, you may be interested in the answers to the following questions:

- What’s New in DFM 2.0?, page 1-3
- Is DFM Ready to Use?, page 1-5
- How Will I Use DFM for Day-to-Day Operations?, page 1-7
- How Does DFM Work?, page 1-11

What’s New in DFM 2.0?

- **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 Notification MIB, page C-1.

  **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 Notifications.

• **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 the DCR.
Is DFM Ready to Use?

The person or team that installed DFM should have completed the initial configuration before you start working with DFM. The instructions for configuring DFM are included in Installation and Configuration Guide for Device Fault Manager.

To use DFM, you must import devices into the DFM inventory as explained in Importing Devices from the DCR, page 4-12. Make sure that your devices are forwarding traps to DFM on port 162 (if port 162 is occupied, DFM uses port 9000).

Once you have imported devices, DFM is ready to monitor and analyze events, and provide notification of alerts on the Alerts and Activities display. DFM uses the default polling parameters and threshold values, default rediscovery and purging schedules, and default views. You should determine whether the default values are adequate for your use.

Table 1-1 lists tasks that you may attend to, at your discretion, after the initial configuration. The table lists optional configuration tasks and some day-to-day tasks that you may want to address when you first start to use DFM.

- **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.
- **New MIB Support**—DFM supports the CISCO-FRAME-RELAY and CISCO-PAGP MIBs.

Along with these new features, DFM 2.0 includes other changes that DFM 1.x users will notice. For detailed information on these behavioral differences between DFM 2.0 and DFM 1.x, refer to Installation and Setup Guide for Device Fault Manager.
### Table 1-1  Tasks to Consider when Initially Setting Up DFM

<table>
<thead>
<tr>
<th>Initial Setup Tasks</th>
<th>Explanation</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscribe users to receive e-mail notification of alerts and subscribe hosts to receive DFM-generated SNMP trap, e-mail, and syslog messages.</td>
<td>DFM displays the operational health of the network on the Alerts and Activities display. In addition, you can subscribe users and hosts to receive e-mail, syslog, or SNMP trap notifications, in response to alerts.</td>
<td>How to Use the Alerts and Activities Display, page 3-1  Using Notification Services, page 5-1</td>
</tr>
<tr>
<td>Update polling parameters and threshold values.</td>
<td>DFM provides default values. However, you can update the values based on your experience with and knowledge of the network.</td>
<td>Configuring Polling and Thresholds, page 10-1</td>
</tr>
<tr>
<td>Update device rediscovery schedules.</td>
<td>DFM provides a single default schedule for device rediscovery. You can use that schedule or create additional rediscovery schedules (several can be active at the same time).</td>
<td>Configuring Rediscovery Schedules, page 7-7</td>
</tr>
<tr>
<td>Add Alerts and Activities views.</td>
<td>Alerts and Activities views control which groups of devices are the focus of the Alerts and Activities display. DFM provides two default view (All Alerts and Suspended Devices). You can add more views.</td>
<td>Configuring Views for the Alerts and Activities Display, page 9-1</td>
</tr>
<tr>
<td>Update the daily purging schedule.</td>
<td>By default, DFM purges the database at midnight. You can modify the schedule.</td>
<td>Configuring the Daily Purging Schedule, page 7-6</td>
</tr>
<tr>
<td>Configure DFM to forward traps to a Network Management System (NMS).</td>
<td>DFM can forward traps to other NMSs, such as HP OpenView and NetView.</td>
<td>Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs, page 7-12</td>
</tr>
</tbody>
</table>
How Will I Use DFM for Day-to-Day Operations?

These topics briefly describe the DFM functions and how they are used, often on a daily basis:

Note

Your login determines the operations you can perform. For more information, refer to Understanding Your User Role, page 2-12.

- **Alerts and Activities**—To monitor the network and assess its health.
- **Fault History**—To monitor the network and assess its health.
- **Device Management**—To keep the inventory of devices that DFM monitors current.
- **Notification Services**—To ensure that the right users and systems receive e-mail, syslog or SNMP traps in response to alerts on selected devices.
- **Configuration**—To change polling and threshold settings, and perform system administration.

To make the most effective use of DFM on a day-to-day basis, users need to understand the impact of operations on configuration and administration tasks. An overview is provided in Performing Scheduling Tasks, page 7-5.

The DFM functions that support day-to-day operations are further described in the following topics:

- **What Is Alerts and Activities?**, page 1-8
- **What Is Device Management?**, page 1-8
- **What Is Notification Services?**, page 1-9
- **What Is Fault History?**, page 1-10
- **What Is Configuration?**, page 1-11
What Is Alerts and Activities?

The Alerts and Activities display provides a consolidated real-time view of the operational status of your network. When a fault occurs in your network, DFM generates an event (or events). Events are rolled up into alerts, one alert for each device with a fault. You can also use Notification Services to change an event name to something that is more meaningful to you.

When an alert occurs on an element in your active view (a logical group of devices), it is displayed on your Alerts and Activities display. You, or a user with the necessary privileges, can customize your view to include only those device groups that are important to you.

From the Alerts and Activities display you can also:

- Drill down into an alert to see what events caused the alert, and add alert annotations for other users to read.
- Drill down into specific events for MIB attribute values.
- Open a Detailed Device View (DDV) to examine device components and suspend or resume monitoring them.
- Use tools such as CiscoView, User Tracking (if Campus Manager is installed), and Fault History.

You can see which components of the device are in the DFM manageable inventory as follows: After you locate the device on the Alerts and Activities display, you can click it and open a DDV. The DDV displays the manageable components of the device. From the DDV, a user with the necessary privileges can suspend monitoring of a device component and, afterward, resume monitoring of the device component again. Suspended devices are moved to the Suspended Devices view. To launch a DDV for devices that currently have no alerts, use Device Management > Device Details.

What Is Device Management?

Device Management involves keeping the inventory of devices that DFM monitors up-to-date. Before devices can be in the DFM inventory, they must be added to the Device and Credentials Repository (DCR). The DCR is a centralized device repository for sharing device information across CiscoWorks. DCR devices can be automatically added to DFM using automatic synchronization, or
you can add them selectively by deactivating automatic synchronization and moving them individually. Synchronization is controlled using the Device Selector; by default, DFM uses automatic synchronization.

The DCR is the front-end for adding devices to and exporting devices from CiscoWorks, and modifying device credentials. DFM provides a user interface for performing the following operations on devices in the DFM inventory:

- Viewing device details
- Rediscovering devices
- Suspending and resuming DFM device management
- Deleting devices (local delete), when manual DCR synchronization is being used

The following scenario describes the process for managing devices:

1. Devices are added from the DCR to the DFM inventory.
2. DFM gets basic information from the DCR.
3. DFM discovers a device and adds its manageable elements to its inventory, placing the device and its elements into the appropriate DFM system-defined groups. (The user can click View Discovery Status to see the status of the device import.)
4. By default, DFM performs rediscovery on a weekly basis. A user can update the default discovery schedule or add discovery schedules.

**What Is Notification Services?**

In addition to watching network conditions as they change on the Alerts and Activities display, you can use notification services to automatically notify users and other systems when specific changes occur on selected devices. To do so, you create subscriptions for e-mail notifications, DFM-generated SNMP trap notifications, or syslog notifications. You can also change event names to names that are more meaningful to you, and these names will be reflected in the DFM displays and notifications.
DFM subscriptions comprise:

- Alerts and/or events. For events, the subscription can contain an event set, which lists the specific events in which you are interested.
- A notification group, which lists the devices (or device groups) and alert/event severity levels in which you are interested.

You can add, modify, and delete subscriptions at any time as your need to disseminate the status and severity of alarm and event changes.

**What Is Fault History?**

Fault History provides the history of DFM events and alerts. The stored history includes alert information and annotations (informational text entered by DFM users), and event information and properties (component name and MIB attributes).

You can start Fault History in the following ways:

- From the DFM Alerts and Activities Display page. From here, you can generate a Fault History display with information about alerts and events from the last 24 hours.
- From the DFM home page by selecting **Device Fault Manager > Fault History**. This method provides historical information about all alerts and events in the Fault History database. The Fault History database keeps information for the alerts and events that occurred within the last 31 days.
- From the CiscoWorks home page by selecting **Device Troubleshooting > Device Center**. From here, you can select a single device and generate a 24-hour or 31-day display.

You can use Fault History to generate customized tabular displays of specific alerts, specific events, event dates, and event severity.
What Is Configuration?

The Configuration pages provide a centralized location for all DFM configuration tasks. Configuration tasks are divided into two categories: Polling and Thresholds, and Other Configurations.

- The Polling and Thresholds category contains the functions that you can use to adjust polling and threshold settings on devices, ports, and interfaces.
- The Other Configurations category includes system administration tasks, such as configuring rediscovery schedules, logging levels, views for the Alerts and Activities display, trap forwarding and receiving; and selecting an SMTP server. In addition, you can perform group management from Other Configurations.

How Does DFM Work?

These topics provide a simplified view of DFM user tasks and DFM processing:

- Users Perform Device Management and Configuration, page 1-11
- DFM Performs Ongoing Monitoring, Analysis, and Notification, page 1-13
- Users Respond to Notifications and Alerts, page 1-15

Users Perform Device Management and Configuration

Users supply the information that tells DFM what to monitor. Figure 1-2 shows a user importing devices, and performing optional configuration tasks to optimize DFM.
How Does DFM Work?

Create the DFM Inventory
- Configure devices to forward traps to DFM.
- Import devices.

Manage the Information (Alerts and Traps)
- Manage polling and threshold settings.
- Create e-mail, SNMP trap, and syslog notification subscriptions.
- Configure SNMP trap forwarding to another NMS.
- Customize the Alerts and Activities display.

Maintain the Data
- Schedule database purging.
- Configure the Rediscovery Schedule.
- Adjust polling parameters.
- Adjust thresholds.

You must import devices and, as your network changes, you must add and delete them accordingly. DFM performs periodic rediscovery, refreshing the inventory of known devices and device components.

Note
DFM monitors supported devices only. To see the device support table for DFM, go to http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dev_sup/index.htm.
You can decide how to manage the information about alerts, events, and traps that DFM produces. For example, you can:

- Create views, enabling users to monitor specific groups of devices on the Alerts and Activities display.
- Create subscriptions to send e-mail to users, or syslog and generated SNMP trap notification to systems.
- Determine where to forward traps by configuring the port to which DFM forwards them.

You can also control how often DFM gathers data. DFM receives traps in real time, but you can change the frequency with which DFM performs the following tasks:

- Polling—You can change the default polling parameters for device groups, altering the polling interval, timeout, and number of retries.
- Rediscovery—You can suspend the default rediscovery schedule and add different rediscovery schedules to fit your circumstances.

**DFM Performs Ongoing Monitoring, Analysis, and Notification**

DFM continuously gathers information from devices and device components, analyzing and prioritizing events, and raising alerts.
DFM generates alerts based on the following activities:

- **Polling**—During polling, DFM identifies conditions that warrant generating an event, such as device unreachable or interface down.

- **Managing thresholds**—After polling, DFM compares the data it collected against threshold values for the devices. If threshold values exceed or do not meet limits, DFM generates the appropriate event.

- **Receiving SNMP traps**—DFM listens for traps on the default port or the port that you have configured for SNMP trap receiving. DFM will process the traps from known, supported devices.
As DFM generates alerts and alert conditions change, DFM determines when to send e-mail or syslog notifications to subscribers and when to generate SNMP traps to send to other systems.

For additional information, see the following topics:

- MIBs Polled, page A-1
- Processed and Pass-Through Traps, and Unidentified Traps and Events, page B-1
- Events Processed, page D-1
- Polling—SNMP and ICMP, page E-1
- How DFM Calculates Repeated Restarts and Flapping, page F-1

**Users Respond to Notifications and Alerts**

Most users will monitor the condition of DFM by using the Alerts and Activities display; others will respond to e-mail. External hosts will receive generated SNMP traps or syslog notifications. **Figure 1-4** shows how you can respond using Alerts and Activities.
How Does DFM Work?

**Figure 1-4 Users Respond to Alerts**

- Select a device
  - Detailed Device View
    - View device element and component information
    - Suspend or resume device element monitoring

- Select an alert
  - Alerts and Activities Detail
    - Suspend or resume device monitoring
    - Annotate an alert
    - Send impromptu e-mail notification
    - Launch Fault History to get historical information

- Select Fault History
  - Fault History
    - View Fault History for past 24 hours

- Monitor and respond using Alerts and Activities
  - Select an event and view details, using available tools for more information
  - Launch Device Center to use other troubleshooting details
  - Launch CiscoView to view chassis details
  - Launch other tools (depends on your configuration)
Getting Started with DFM

These topics help you to work with and understand the Device Fault Manager (DFM) user interface:

- Working with DFM Windows, page 2-1
- Using Tabular Displays, page 2-4
- Selecting Objects and Groups, page 2-7
- Understanding Your User Role, page 2-12
- Responding to Security Alerts, page 2-12
- Responding to Messages About Device Limits, page 2-13

Working with DFM Windows

This topic focuses on questions you may have when you first start to work with the DFM user interface:

- What is the purpose of the CiscoWorks Home Page?, page 2-2
- What is the purpose of the DFM Home Page?, page 2-2
- Why are multiple windows open?, page 2-2
- Why do I see the error “The page cannot be displayed”?, page 2-2
- When I press the Enter key, why doesn’t DFM complete the current task?, page 2-2
- Where is the help button?, page 2-3
What is the purpose of the CiscoWorks Home Page?
The CiscoWorks home page is a portal that provides access to local and remote CiscoWorks applications. You can add or remove applications from the home page, as desired. The applications launched from the CiscoWorks home page normally have a common look and feel for ease of use.

What is the purpose of the DFM Home Page?
The DFM home page opens when you click a Device Fault Manager link on the CiscoWorks home page. The DFM home page is the portal for all DFM-related tasks: starting an Alerts and Activities display, running Fault History reports, managing devices in the DFM inventory, configuring notifications, and performing system configuration on DFM.

Why are multiple windows open?
For ease of use, DFM opens separate windows for each application, and sometimes for functions within applications. Opening multiple browser windows allows you to:

- Refer to information from one display to complete a task in another window
- Rapidly compare information on different displays.

When DFM opens a new browser window, it does not close previously opened windows. You can close browser windows when you are done with them.

Note
If you close the CiscoWorks window while displaying Alerts and Activities in the Device Fault Manager browser windows, links in those windows will continue to function. In contrast, if you log out of CiscoWorks, links from those windows will return errors and you will need to log in to CiscoWorks again.

Why do I see the error “The page cannot be displayed”?
DFM displays often include links to more detailed information. Right-clicking a link and selecting Open in New Window is not supported. It is expected behavior for this error to appear.

When I press the Enter key, why doesn’t DFM complete the current task?
DFM does not accept pressing the Enter key as a substitute for clicking buttons, such as OK, Finish, or Next, on the application page.
Where is the help button?

You can access help by clicking the Help link at the top right of any home page—the CiscoWorks home page, the DFM home page, or any other application’s home page. See Using Help, page 2-3.

Using Help

To start DFM help:

1. Launch any DFM display from the CiscoWorks home page. See What is the purpose of the DFM Home Page?, page 2-2.

2. Click the Help link near the top right of the page (the Alerts and Activities display provides a Help button).

Note: If you have selected an option in any home page, the context-sensitive help for that option is displayed.

Help is displayed in a separate browser window that remains open until you close it. Online help includes an index and search capability. You can access CiscoWorks help by clicking Main at the top right of the help page.

Understanding the Dates and Times Displayed

Dates and times displayed by DFM reflect the date, time, and time zone set on the server where DFM is installed. If the client system you use to run DFM is located in a time zone other than the time zone set on the server, you will notice the difference; for example:

- Status “as of” the current date and time will not display your local time and time zone and may not match your local date.
- Dates and times shown for previous events are recorded (and displayed) with the server time stamp, which is offset from your local time.
Using Tabular Displays

DFM presents information in tabular displays when the amount of data to be displayed or manipulated could be quite large. Tabular displays ease the task of handling information by providing the following features:

- **Sorting**—You can sort a tabular display in the order you prefer by clicking any clickable column heading.

- **Direct page access**—You can browse a tabular display screen by screen or jump to any screen number in the range by entering a screen number.

  **Note**
  A tabular display can show up to 2,000 records. If more than 2,000 records exist and you need to access the additional records, you can export all records using the data export icon.

- **Data export**—You can export data from a tabular display to a comma separated values (CSV) file, a Portable Document Format (PDF) file, or both, depending upon the tabular display that you are using. See the icon in Table 2-1.

- **Printer friendly**—You can format the tabular display for a printer and print the result from the browser. Like the tabular display, the print-friendly browser display includes a maximum of 2,000 records. See the icon in Table 2-1.
Paging and Sorting Tabular Displays

The sort order for any tabular display is indicated by the presence of a triangle in the column heading. A triangle pointing down indicates records in descending order, which is the default, while a triangle pointing up indicates records in ascending order.

**Step 1**
To sort a tabular display, click any blue column heading label.

The first time you click a column heading on a previously unsorted column, data in that column is sorted in descending order. If you click the column heading again, the records will be sorted in the reverse order.

**Note**
When you sort a tabular display, if there are more than 2,000 records available, all records are sorted, not just those that are displayed. The first 2,000 records are displayed after sorting.

---

**Table 2-1 Tabular Displays—Export and Print-Friendly Icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="CSV icon" /></td>
<td>Exports all data to either a CSV file or a PDF file.</td>
</tr>
<tr>
<td><img src="image" alt="Print icon" /></td>
<td>Reformats the displayed records into print-friendly format, and displays them in a new browser window.</td>
</tr>
</tbody>
</table>
Viewing Data from Tabular Displays with Over 2000 Records

If more than 2,000 records exist, they cannot all be shown in a tabular display. A message will be displayed to notify you when this is the case. If you want to see data for all of the records, you must export the data to a CSV or PDF file. See Exporting Data from Tabular Displays, page 2-6.

You may be able to change which of the more than 2,000 records are displayed by sorting the tabular display. See Paging and Sorting Tabular Displays, page 2-5.

Exporting Data from Tabular Displays

All tabular displays can be exported as comma separated values (CSV) files. Some tabular displays can also be exported as PDF files.

Note

To open a PDF file, you must have Adobe Acrobat Reader 4.0 or higher installed on your client system. However, you can save a file as a PDF file even if you do not have Acrobat Reader on your system.

Step 1
Click the data export icon located on the top-right side of the tabular display. See the icon in Table 2-1.

Step 2
If the dialog box Export to appears, select one of the following and click OK:

- CSV
- PDF

Note

Some tabular displays may only support CSV exports.
Step 3  Save the export file in one of the following ways:

- If you selected PDF and have Adobe Acrobat Reader installed on your client system, the PDF file opens. To save the PDF file, select File > Save as from the browser and follow the online instructions to save the file.
- If you selected PDF and do not have Adobe Acrobat Reader installed, or if you selected CSV, follow the online instructions to save the file.

Printing Tabular Displays

Step 1  Click the print-friendly icon located on the top-right side of the tabular display. See the icon in Table 2-1.

A new browser window opens, displaying the data in print-friendly format.

Step 2  Print the tabular display from the new browser window.

Selecting Objects and Groups

As you use DFM, you will often need to select something—a device or a device group, for example—before you can view information or complete a task. Groups and devices displayed in a selector differ depending upon the application, as described in the following topics:

- Selecting Objects Organized by Group Management, page 2-8
- Selecting Objects Organized by Discovery Status, page 2-11
Selecting Objects Organized by Group Management

This topic shows a few examples of selectors to familiarize you with them. Use the application-specific topics to determine what to select to accomplish your objective.

**Figure 2-1** shows group selectors as they might first appear when you select Configuration > Other Configurations > Group Management.

**Figure 2-1** Device Selector as Displayed Initially on Group Management Page

<table>
<thead>
<tr>
<th>Group Selector</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ CS@MARVER_DAILY</td>
</tr>
<tr>
<td>□ DFM@MARVER-DAILY</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS@MARVER_DAILY</td>
<td>Groups that are controlled by Common Services.</td>
</tr>
<tr>
<td>DFM@MARVER-DAILY</td>
<td>Groups that are controlled by DFM.</td>
</tr>
</tbody>
</table>

**Figure 2-2** shows a group selector as it might appear when you expand the Common Services and DFM folders. Devices are listed according to their group membership.

**Figure 2-2** Expanded Common Services and DFM Groups on Group Management Page

<table>
<thead>
<tr>
<th>Group Selector</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ CS@MARVER-DAILY</td>
</tr>
<tr>
<td>□ DFM@MARVER-DAILY</td>
</tr>
<tr>
<td>□ System Defined Groups</td>
</tr>
<tr>
<td>□ User Defined Groups</td>
</tr>
<tr>
<td>□ System Defined Groups</td>
</tr>
</tbody>
</table>

User Guide for Device Fault Manager
These groups are further described in Managing Groups, page 8-1.

Figure 2-3 also shows a device group selector as it might appear when you expand the DFM System Defined Groups and User Defined Groups folders.
### Figure 2-3  Expanded DFM Groups and Device Selector on Group Management Page

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Defined Access Port Groups</td>
<td>Predefined access port groups used by DFM.</td>
</tr>
<tr>
<td>System Defined Interface Port Groups</td>
<td>Predefined interface port groups used by DFM.</td>
</tr>
<tr>
<td>System Defined Trunk Port Groups</td>
<td>Predefined trunk port groups used by DFM.</td>
</tr>
<tr>
<td>User Defined Customizable Access Port Groups</td>
<td>Groups the user can customize to track access ports.</td>
</tr>
<tr>
<td>User Defined Customizable Groups</td>
<td>Groups the user can customize to track devices.</td>
</tr>
<tr>
<td>User Defined Customizable Interface Groups</td>
<td>Groups the user can customize to track interfaces.</td>
</tr>
<tr>
<td>User Defined Customizable Trunk Port Groups</td>
<td>Groups the user can customize to track trunk ports.</td>
</tr>
</tbody>
</table>
Selecting Objects Organized by Discovery Status

Figure 2-4 shows a device selector as you might see it on the Device Management > View Device Details page. In this example devices are group according to their discovery status (or device state). These groups only appear in your device selector when they have members in that discovery state.

**Figure 2-4 Device Selector with Devices Organized by Discovery State**

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Known Devices</td>
<td>A container for all devices that were successfully imported and are being managed by DFM.</td>
</tr>
<tr>
<td>All Learning Devices</td>
<td>A container for all devices DFM is in the process of discovering.</td>
</tr>
<tr>
<td>All Pending Devices</td>
<td>A container for all devices that are in the process of being deleted from DFM.</td>
</tr>
<tr>
<td>All Questioned Devices</td>
<td>A container for all devices that DFM cannot manage.</td>
</tr>
</tbody>
</table>

Device states are described in Understanding the Device Summary and Device States, page 4-10.
Understanding Your User Role

When you log in to DFM, you enter the username and password assigned to you by a system administrator. Your username is associated with either a CiscoWorks role or a Cisco Secure Access Control Server (ACS) role. By default, CiscoWorks and ACS roles are the same, but an ACS administrator can modify the ACS roles. User roles control the functions that you are allowed to see and use from the DFM home page. If you cannot locate a function in the DFM home page, the task is not permitted for the user role. For more information, do the following:

- View the CiscoWorks Permission Report to determine which tasks are permitted for each user role. From the Common Services home page, select Server > Reports > Permission Report and click Generate Report.
- View the ACS report by logging onto the ACS server and select Shared Profile Components. Refer to the ACS online help for more information.

For more information, refer to these topics:
- Configuring Users (ACS and Non-ACS), page 11-7
- Using DFM in ACS Mode, page 11-9

Responding to Security Alerts

The first time you select nearly any DFM function, you will see a Security Alert window displayed. You should install the self-signed security certificate. You should do this once, on each client system you use to access DFM.

Note

If you see a Security Alert Window with a message that the certificate has expired, you should contact a user with System Administrator privileges to create a self-signed security certificate, and then install it.

Note

If you do not install the self-signed security certificate, you may not be able to access some DFM application pages.
Chapter 2      Getting Started with DFM

Responding to Messages About Device Limits

If you exceed your server’s device limit, DFM will continue to work, but it will not allow you to import any more devices. What happens next depends on whether you use automatic synchronization between the Device and Credentials Repository (DCR) and the DFM inventory, or you add DCR devices to the DFM inventory on a device-by-device basis:

- Manual synchronization with DCR—When you use the Device Selector page to move devices from the DCR into DFM, DFM will display a popup message warning you that you cannot import any more devices (see Understanding the Device and Credentials Repository, page 4-8).

- Automatic synchronization with DCR—You will notice that devices are not appearing on DFM pages. You can check the license log for more information (see Viewing and Maintaining Log Files, page 11-18).

For information about device-based licensing, see Installation Guide for Device Fault Manager.

---

**Step 1**
Click the **View Certificates** button on the Security Alert window. The Certificate window is displayed.

**Step 2**
Install the certificate as follows:

a. Click the **Install Certificate** button. The Certificate Import Wizard window is displayed.

b. Follow the instructions provided by the Certificate Import wizard.
Using the Alerts and Activities Display

These topics describe how to use the Alerts and Activities display:

- How to Use the Alerts and Activities Display, page 3-1
- Starting the Alerts and Activities Display, page 3-2
- Getting Alert Details, page 3-6
- Customizing the Alerts and Activities Display, page 3-10
- Getting Event Details, page 3-11
- Getting Device Information (Detailed Device View), page 3-20
- Suspending Device Monitoring, page 3-26
- Acknowledging, Annotating, and Sending E-Mail Notifications of Alerts, page 3-29

How to Use the Alerts and Activities Display

The Alerts and Activities display provides real-time information about the operational status of your network. The displays are designed so that you can set them up and leave them running, providing an ongoing monitoring tool that signals you when something needs attention. When a fault occurs in your network, Device Fault Manager (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.
If desired, you can change event names to names that are more meaningful to you. These customized names will be reflected in both the Alerts and Activities display and any Fault History reports you generate. For information on changing DFM event names using Notification Customization, see Customizing the Names of DFM Events, page 5-5.

You can monitor all devices that DFM supports, once you have added those devices using Device Management and ensured that the devices are in your view. However, DFM reports alerts on specific devices or components, not on entire device groups.

You can start the Alerts and Activities display from the DFM home page. If the DFM server is using Access Control Server (ACS) mode, ACS may limit the devices you are permitted to view. For more information, refer to Device-Based Filtering, page 11-11.

---

**Note**

All Fault History reports generated from within the Alerts and Activities display provide information from the past 24 hours. To generate a Fault History report on time spans beyond the last 24 hours, use Fault History from DFM home page by selecting **Fault History**. For more information, see Starting Fault History from the DFM Home Page, page 6-5.

---

**Starting the Alerts and Activities Display**

To start the Alerts and Activities display, from the DFM home page select **Alerts and Activities**. Figure 3-1 shows an example of an Alerts and Activities display.

---

**Tip**

After you become familiar with the Alerts and Activities display, you can modify the information it provides as described in Customizing the Alerts and Activities Display, page 3-10.
Starting the Alerts and Activities Display

**Figure 3-1  Alerts and Activities Display**

2. Launch information and view status bar area. See Launch Information and View Status Bar Area, page 3-5.
3. Tabular display pane. See Tabular Display Pane, page 3-5.
Chapter 3  Using the Alerts and Activities Display

Starting the Alerts and Activities Display

3-4

User Guide for Device Fault Manager

78-16266-01

Understanding the Layout of the Alerts and Activities Display

These topics provide details about the information in the Alerts and Activities display.

View Pane

The view pane lists the currently available views, or logical groupings of device groups. Views must be created and activated before they will be shown in the Alerts and Activities display. By default, two views—All Alerts and Suspended Devices—are always shown, and cannot be deleted from your Alerts and Activities display. (To create and activate a view or remove an unwanted view from your display, see Configuring Views for the Alerts and Activities Display, page 9-1.)

The current view is highlighted in the view pane. The contents of the current view are shown in the tabular display pane to the right of the view pane. To select another view, simply click the view name in the view pane.

Figure 3-2 shows four active views; the current view is All Alerts. Icons next to the views indicate the severity of the alerts received from devices in those views, signaling you that the devices may need attention.

Figure 3-2  Alerts and Activities Display—View Pane and Severity Icons

For the current view (All Alerts in this example), severity icons also appear next to the alerts in the tabular display, as shown in Figure 3-2, to help you quickly locate a specific alert.

The view pane is updated every two minutes. You can have up to 18 views in the view pane in a single Alerts and Activities display.
Launch Information and View Status Bar Area

The launch information area shows the time on the server when the Alerts and Activities display was started.

The view status bar lists the selected view, which is shown in the tabular display pane, and the number of alerts in that view.

Tabular Display Pane

The tabular display pane is the core of the Alerts and Activities display. It contains a list of all alerts that are occurring on the devices in your current view. This pane is refreshed every 30 seconds. For an explanation for all of the items in the tabular display, see Table 3-2 on page 3-7.

Icons alert you to what needs attention; for example:

- The severity icons indicate which views and alerts require attention.
- The diamond symbols in the Last Change column indicate which alerts have experienced recent activity. When no diamonds appears in the Last Change column, the alert is no longer current, or stale.

The tabular display pane is scrollable and can store up to 1,000 records. See Figure 3-3 for an illustration of the tabular display pane.

Window Tools Area

The top-right corner of the Alerts and Activities display contains buttons for the available window tools. All buttons are described in Table 3-1.

Table 3-1 Alerts and Activities Display—Window Tools

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Described in...</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Icon" /></td>
<td>Exports the current tabular display to a PDF file.</td>
<td>Exporting Data from Tabular Displays, page 2-6</td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon" /></td>
<td>Opens the Filter page, for refining the tabular display in the Alerts and Activities display.</td>
<td>Filtering Alerts and Activities, page 3-11</td>
</tr>
<tr>
<td><img src="image3.png" alt="Icon" /></td>
<td>Opens a printer-friendly version for printing.</td>
<td>Printing Tabular Displays, page 2-7</td>
</tr>
</tbody>
</table>
Getting Alert Details

Use the tabular display in the Alerts and Activities display to obtain more information about the alerts that are occurring in your current view. In the tabular display, as shown in Figure 3-3, alerts are grouped by their severity: critical, warning, or informational. Within these severity groupings, or buckets, alerts with the latest change are listed first.

When an alert is generated, it remains in the Alerts and Activities display until it expires. DFM sets an alert state to Expired when DFM performs its normal polling and determines that the alarm has been in the Cleared state for 30 minutes or longer (from the time of polling). While the alert is in the display, if any of its events recur, the alert is updated. If an expired alert recurs, a new alert with a new ID is shown.

Note
The Alerts and Activities display does not report alerts generated on VLANs. However, you the event properties page will show the VLAN number to which the port belongs (see Viewing Event Properties, page 3-19). The Detailed Device View will display to which VLAN ports belong (see Starting the Detailed Device View, page 3-20).

*Figure 3-3* provides an example of an Alerts and Activities tabular display. This display is refreshed every 30 seconds.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Described in...</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Icon" /></td>
<td>Opens a DFM Tools window with link to Fault History</td>
<td>Generating a 24-Hour Report on All Alerts in the Current View, page 6-4</td>
</tr>
<tr>
<td><img src="image2" alt="Icon" /></td>
<td>Opens the DFM help window.</td>
<td>Using Help, page 2-3</td>
</tr>
</tbody>
</table>

Table 3-1 Alerts and Activities Display—Window Tools (continued)
Table 3-2 defines the table elements. All elements are updated every 30 seconds.

You can generate a 24-hour Fault History report on all alerts that occurred on devices in your view by opening Fault History from the window tools area of the Alerts and Activities display.

### Table 3-2  Alerts and Activities Tabular Display — Contents

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert ID</td>
<td>Alert identifier number. Clicking this link opens an Alerts and Activities Detail page (see Starting the Alerts and Activities Detail Page, page 3-12).</td>
</tr>
<tr>
<td>Alert Type</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Trap Alert</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>Unidentified Trap alert</td>
<td></td>
</tr>
<tr>
<td>Informational</td>
<td>Informational (for all other alerts)</td>
</tr>
</tbody>
</table>

**Tip**

Figure 3-3  Alerts and Activities — Tabular Display

Table 3-2  Alerts and Activities Tabular Display — Contents

<table>
<thead>
<tr>
<th>Alert ID</th>
<th>Alert Type</th>
<th>Status</th>
<th>Description</th>
<th>Trap Alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000005</td>
<td>Switches and Hubs</td>
<td>Critical</td>
<td>Interface</td>
<td>ACH</td>
</tr>
<tr>
<td>00000006</td>
<td>Voice and Telephones</td>
<td>Warning</td>
<td>Interface</td>
<td>ACH</td>
</tr>
<tr>
<td>00000007</td>
<td>Routers</td>
<td>Unidentified Trap alert</td>
<td>Interface</td>
<td>ACH</td>
</tr>
<tr>
<td>00000008</td>
<td>Switches and Hubs</td>
<td>Critical</td>
<td>Interface</td>
<td>ACH</td>
</tr>
<tr>
<td>00000009</td>
<td>Voice and Telephones</td>
<td>Warning</td>
<td>Interface</td>
<td>ACH</td>
</tr>
<tr>
<td>00000010</td>
<td>Routers</td>
<td>Unidentified Trap alert</td>
<td>Interface</td>
<td>ACH</td>
</tr>
</tbody>
</table>

**Table 3-2**

Table 3-2 defines the table elements. All elements are updated every 30 seconds.

You can generate a 24-hour Fault History report on all alerts that occurred on devices in your view by opening Fault History from the window tools area of the Alerts and Activities display.

**Table 3-2  Alerts and Activities Tabular Display — Contents**

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert ID</td>
<td>Alert identifier number. Clicking this link opens an Alerts and Activities Detail page (see Starting the Alerts and Activities Detail Page, page 3-12).</td>
</tr>
<tr>
<td>Alert Type</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Trap Alert</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>Unidentified Trap alert</td>
<td></td>
</tr>
<tr>
<td>Informational</td>
<td>Informational (for all other alerts)</td>
</tr>
</tbody>
</table>

**Tip**

Figure 3-3  Alerts and Activities — Tabular Display

Table 3-2  Alerts and Activities Tabular Display — Contents

<table>
<thead>
<tr>
<th>Alert ID</th>
<th>Alert Type</th>
<th>Status</th>
<th>Description</th>
<th>Trap Alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000005</td>
<td>Switches and Hubs</td>
<td>Critical</td>
<td>Interface</td>
<td>ACH</td>
</tr>
<tr>
<td>00000006</td>
<td>Voice and Telephones</td>
<td>Warning</td>
<td>Interface</td>
<td>ACH</td>
</tr>
<tr>
<td>00000007</td>
<td>Routers</td>
<td>Unidentified Trap alert</td>
<td>Interface</td>
<td>ACH</td>
</tr>
<tr>
<td>00000008</td>
<td>Switches and Hubs</td>
<td>Critical</td>
<td>Interface</td>
<td>ACH</td>
</tr>
<tr>
<td>00000009</td>
<td>Voice and Telephones</td>
<td>Warning</td>
<td>Interface</td>
<td>ACH</td>
</tr>
<tr>
<td>00000010</td>
<td>Routers</td>
<td>Unidentified Trap alert</td>
<td>Interface</td>
<td>ACH</td>
</tr>
</tbody>
</table>

**Table 3-2**

Table 3-2 defines the table elements. All elements are updated every 30 seconds.

You can generate a 24-hour Fault History report on all alerts that occurred on devices in your view by opening Fault History from the window tools area of the Alerts and Activities display.

**Table 3-2  Alerts and Activities Tabular Display — Contents**

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert ID</td>
<td>Alert identifier number. Clicking this link opens an Alerts and Activities Detail page (see Starting the Alerts and Activities Detail Page, page 3-12).</td>
</tr>
<tr>
<td>Alert Type</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Trap Alert</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>Unidentified Trap alert</td>
<td></td>
</tr>
<tr>
<td>Informational</td>
<td>Informational (for all other alerts)</td>
</tr>
</tbody>
</table>
### Table 3-2  Alerts and Activities Tabular Display—Contents (continued)

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device</strong></td>
<td>Device type. <em>Learning</em> indicates that DFM was discovering the device when the alert occurred. The actual device type is reflected when new events occur. For more information, see <strong>Using Device Management</strong>, page 4-1. If the DFM server is using Access Control Server (ACS) mode, ACS may limit the devices you are permitted to view. For more information, refer to <strong>Device-Based Filtering</strong>, page 11-11.</td>
</tr>
<tr>
<td><strong>Duration</strong></td>
<td>Time span since alert creation, depending upon alert status:</td>
</tr>
<tr>
<td>Active or Acknowledged</td>
<td>Time span between alert creation and current server time.</td>
</tr>
<tr>
<td>Cleared</td>
<td>Time span between alert creation and Last Change time (the Last Change time may also represent when the alert was cleared).</td>
</tr>
<tr>
<td><strong>Last Change</strong></td>
<td>Date and time alert last occurred or was changed. Diamonds indicate alert activity, such as a new event, alert acknowledgement, new user annotation, and so forth; no diamonds indicates that the alert is stale. Alerts are grouped by severity, and within severities, alerts with the latest change are listed first.</td>
</tr>
<tr>
<td><img src="image" alt="Alerts updated within last 15 minutes." /></td>
<td>Alert was updated within last 15 minutes.</td>
</tr>
<tr>
<td><img src="image" alt="Alerts updated within last 16-30 minutes." /></td>
<td>Alert was updated within last 16-30 minutes.</td>
</tr>
<tr>
<td><img src="image" alt="Alerts updated within last 31-45 minutes." /></td>
<td>Alert was updated within last 31-45 minutes.</td>
</tr>
<tr>
<td><img src="image" alt="No diamonds" /></td>
<td>Alert was updated over 46 minutes ago.</td>
</tr>
<tr>
<td><strong>Device Name</strong></td>
<td>Device name or IP address. Clicking this link opens the Detailed Device View (see <strong>Understanding the Layout of the Detailed Device View</strong>, page 3-23).</td>
</tr>
</tbody>
</table>

### Table 3-2  Alerts and Activities Tabular Display—Contents (continued)

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Event category, one of the following: Environment, Interface, Other, Reachability, System Hardware, Utilization. For alerts containing multiple events, the tabular display shows the category of the event with the most recent change.</td>
</tr>
<tr>
<td>Status</td>
<td>Alert status, based on last polling.</td>
</tr>
<tr>
<td>Active</td>
<td>Alert is live. (Note that alerts on suspended devices remain active; see Sending E-Mail in Response to an Alert, page 3-31.)</td>
</tr>
<tr>
<td>Cleared</td>
<td>Alert is no longer live. If the alarm has been in the Cleared state for 30 minutes or more (from the time of polling), the alert expires and is removed from the display.</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>Alert was manually acknowledged by a user (from Alerts and Activities Detail page).</td>
</tr>
</tbody>
</table>
Customizing the Alerts and Activities Display

After adding your devices to a view, you can customize your Alerts and Activities display by selecting specific views and using filters:

- Views control the device groups that appear on the Alerts and Activities display. See Selecting Views for Alerts and Activities, page 3-10.
- Filters control the specific device types you monitor, along with alert severities and their status. See Filtering Alerts and Activities, page 3-11.

You can also change the names of DFM events to names that are more meaningful to you. These names will be reflected in both the Alerts and Activities display and in any Fault History reports you generate. For information on changing DFM event names using Notification Customization, see Customizing the Names of DFM Events, page 5-5.

If the DFM server is using Access Control Server (ACS) mode, ACS may limit the devices you are permitted to view. For more information, refer to Device-Based Filtering, page 11-11.

Selecting Views for Alerts and Activities

When you select Alerts and Activities from the DFM home page to open the Alerts and Activities display, all available views are listed in the view pane on the left side of the display. If the views shown do not meet your needs, you can create a new view as described in Creating a View, page 9-2.

The view pane is updated every two minutes. You can have up to 18 views in the view pane in a single Alerts and Activities display. See Activating and Deactivating a View, page 9-4 for information on how to manage your views.
Filtering Alerts and Activities

Filters allow you to manipulate the Alerts and Activities display to show alerts based on their severity, status, and originating device type.

**Note**

Once you use an alert filter, the filter is applied to all of your views until you change the filter; other clients are not affected. When you end your session, your filters are lost. Filters do not affect severity icons in the view pane.

**Step 1**

From the DFM home page, select **Alerts and Activities**. The Alerts and Activities display opens.

**Step 2**

Click the filtering button in the tool button area at the top-right of the Alerts and Activities display. The Alert Filters page opens. You can populate the Device Type box by selecting device types from the button to the right of the Device Type box. By default, all device types are selected.

**Step 3**

To see all device types that you can filter, click the button to the right of the Device Type box. A Device Types popup window opens.

**Step 4**

Verify that only the filtering criteria you want to use are selected.

**Step 5**

Click **OK**.

---

Getting Event Details

These topics address how to start and use the Alerts and Activities Detail page to get more information on events:

- Starting the Alerts and Activities Detail Page, page 3-12
- Understanding the Layout of the Alerts and Activities Detail Page, page 3-14
- Viewing Events Associated with an Alert, page 3-17
- Viewing Event Properties, page 3-19

You can change the names of DFM events using Notification Services. Refer to Customizing the Names of DFM Events, page 5-5.
Chapter 3  Using the Alerts and Activities Display

Starting the Alerts and Activities Detail Page

The Alerts and Activities Detail page provides information about all of the events that were rolled up into a specific alert. Figure 3-4 provides an example of an Alerts and Activities Detail page.

Note
The Alerts and Activities Detail page does not report alerts generated on VLANs. However, the event properties page will show the VLAN number to which the port belongs (see Viewing Event Properties, page 3-19). The Detailed Device View will display to which VLAN ports belong (see Starting the Detailed Device View, page 3-20).

Step 1
From the DFM home page, select Alerts and Activities. The Alerts and Activities display opens.

Step 2
Locate the alert you want to investigate and click the alert ID. The Alerts and Activities Detail page opens.
Figure 3-4  Alerts and Activities Detail Page

1. Alerts status bar. See the Alert Status Bar, page 3-14.
2. Launch information area. See Launch Information Area, page 3-15.
7. Notes pane. See Notes Pane, page 3-16.
Understanding the Layout of the Alerts and Activities Detail Page

These topics provide details about the information in the Alerts and Activities display.

Alert Status Bar
The alert status bar lists details about the alert with which the listed events are associated. Table 3-3 explains the contents of the alert status bar area.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device name or IP address.</td>
</tr>
<tr>
<td>Device</td>
<td>Device type. <em>Learning</em> indicates that DFM was discovering the device when the alert occurred. The actual device type is reflected when new events occur. For more information, see Using Device Management, page 4-1. If the DFM server is using Access Control Server (ACS) mode, ACS may limit the devices you are permitted to view. For more information, refer to Device-Based Filtering, page 11-11.</td>
</tr>
<tr>
<td>Status</td>
<td>Alert status, based on last polling.</td>
</tr>
<tr>
<td>Active</td>
<td>Alert is live. (Note that alerts on suspended devices remain active; see Sending E-Mail in Response to an Alert, page 3-31.)</td>
</tr>
<tr>
<td>Cleared</td>
<td>Alert is no longer live. If the alarm has been in the Cleared state for 30 minutes or more (from the time of polling), the alert expires and is removed from the page.</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>Alert was manually acknowledged by a user (from Alerts and Activities Detail page). If an event on the alert recurs, the alert state reverts back to Active.</td>
</tr>
<tr>
<td>Alert ID</td>
<td>Alert identifier number.</td>
</tr>
</tbody>
</table>
Getting Event Details

Chapter 3 Using the Alerts and Activities Display

Table 3-3 Alerts and Activities Detail Page—Alert Status Bar Contents (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>Time span since alert creation, depending upon alert status:</td>
</tr>
<tr>
<td></td>
<td>Active or Acknowledged Time span between alert creation and current server time.</td>
</tr>
<tr>
<td></td>
<td>Cleared Time span between alert creation and Last Change time (the Last Change time may also represent when the alert was cleared).</td>
</tr>
</tbody>
</table>

| Last Change | Time and date of last alert update (indicates activity, such as an event recurrence, alert acknowledgement, the addition of an annotation, and so forth). Alerts are grouped by severity, and within severities, alerts with the latest change are listed first. |

Tabular Display Pane

In the Alerts and Activities Detail page, the tabular display pane contains a table that lists details about events. These events are associated with the alert listed in the alert status bar. You can refresh the display by clicking Refresh at the bottom of the pane. For an explanation of all of the items in the table, see Table 3-6 on page 3-17.

The tabular display is scrollable and can store up to 1,000 records. See Figure 3-4 for an illustration of the actions you can perform from this window.

Launch Information Area

The launch information area shows the time on the server when the Alerts and Activities Detail page was started.

Window Tools Area

The top-right corner of the Alerts and Activities Detail page contains a printer tool button, as described in Table 3-4.

Table 3-4 Alerts and Activities Detail Page—Window Tool

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Described in...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Opens a printer-friendly version for printing</td>
<td>Printing Tabular Displays, page 2-7</td>
</tr>
</tbody>
</table>
Tools Drop-Down List
The Tools drop-down list contains a list of applications that can provide more information, depending on your installation. For more information, see Table 3-6 on page 3-17.

Notes Pane
The notes pane lists any alert annotations that users have entered. The notes pane is a convenient tool for making sure that all users see alert information. You can add an annotation by clicking the Annotate button. Adding an annotation is described in Starting the Alerts and Activities Display, page 3-2.

Command Button Area
In addition to the Annotate button in the notes pane, the command button area provides other ways to respond to alerts.

Table 3-5  Alerts and Activities Detail Page—Command Buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>Refreshes the tabular display.</td>
</tr>
<tr>
<td>Acknowledge</td>
<td>Changes the event status to Acknowledged. See Acknowledging an Alert, page 3-30 for more information.</td>
</tr>
<tr>
<td>Suspend</td>
<td>Suspends polling and trap processing on the device or device component by opening a Detailed Device View (DDV), from which you can perform the suspend command. The DDV is described in Starting the Detailed Device View, page 3-20.</td>
</tr>
<tr>
<td>Notify</td>
<td>Sends e-mail notification of the alert. See Sending E-Mail in Response to an Alert, page 3-31 for more information.</td>
</tr>
<tr>
<td>Close</td>
<td>Closes the Alerts and Activities Detail page.</td>
</tr>
</tbody>
</table>
Viewing Events Associated with an Alert

Use the tabular display in the Alerts and Activities Detail page to obtain more information about all of the events associated with a specific alert. In the tabular display, as shown in Figure 3-5, events with the latest change are listed first.

Events remain on the Alerts and Activities Detail page until the parent alert expires. If you suspend a device, all the events are cleared, but the alert remains active. (This way, users cannot remove important information from the display, and you can easily resume the device.)

If an event recurs, the existing event is not updated. Instead, the recurrence is shown as a new event with a new event ID.

Figure 3-5 provides an example of an Alerts and Activities Detail table.

Figure 3-5  Alerts and Activities Detail Page—Tabular Display

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
<th>Component</th>
<th>Time</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 00000001</td>
<td>Exceeded Max Current</td>
<td>IF-172.30.121.14</td>
<td>26-Sep-2004 18:58:42</td>
<td>Active</td>
</tr>
<tr>
<td>2. 00000002</td>
<td>Unresponsive</td>
<td>172.30.121.19</td>
<td>26-Sep-2004 18:58:12</td>
<td>Active</td>
</tr>
<tr>
<td>3. 00000003</td>
<td>Insufficient Power</td>
<td>MBM-172.30.121.14</td>
<td>26-Sep-2004 18:47:42</td>
<td>Active</td>
</tr>
</tbody>
</table>

Table 3-6 defines the table elements. Click Refresh at the bottom of the page to refresh the table contents.

Tip

Remember that you can generate a 24-hour Fault History report on all events that occurred on a selected component by opening Fault History from the window tools area of the Alerts and Activities display.

Table 3-6  Alerts and Activities Detail Tabular Display—Contents

| Event ID | Event identifier number. Clicking this link opens the event properties page (see Getting Event Details, page 3-11). Note that this Event ID is not the same as the Event Code provided by Notification Services. For more information, see Customizing the Names of DFM Events, page 5-5. |
### Getting Event Details

#### Description
DFM event name (as described in Events Processed, page D-1). You can also change the names of DFM events to names that are more meaningful to you. For information on changing DFM event names using Notification Customization, see Customizing the Names of DFM Events, page 5-5.

#### Component
Device element on which the event occurred.

#### Time
Time at which the event occurred.

#### Status
Event status, based on last polling.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Event is live.</td>
</tr>
<tr>
<td>Cleared</td>
<td>Event is no longer live. (Note that events on suspended devices are moved to Cleared, but the alert remains active. See Sending E-Mail in Response to an Alert, page 3-31.)</td>
</tr>
<tr>
<td>Suspended</td>
<td>Device is suspended.</td>
</tr>
<tr>
<td>Resumed</td>
<td>Device is being resumed.</td>
</tr>
<tr>
<td>Deleted</td>
<td>Device has been deleted.</td>
</tr>
</tbody>
</table>

#### Tools
A drop-down list of applications that can provide more information (see Figure 3-6). The Tools drop-down list can include the following, depending upon the applications installed on your server:

- Device Ctr.—Opens the CiscoWorks Device Center, which provides a centralized point for reports, tools, and tasks that you can perform on the selected device.
- UT Report—Opens a User Tracking End Host report that lists end-user hosts in the network. (This tool is available if Campus Manager is installed.)
- CiscoView—Opens the CiscoView chassis view for the device. (This tool is available if CiscoView is installed.)

### Table 3-6 Alerts and Activities Detail Tabular Display—Contents (continued)
Chapter 3      Using the Alerts and Activities Display

Getting Event Details

Figure 3-6 provides an example of an Alerts and Activities Detail tools drop-down list.

**Figure 3-6   Alerts and Activities Detail Tools Drop-Down List**

Viewing Event Properties

The event properties page provides additional details about the event, such as the values of MIB attributes at the time of the event, polling and threshold information, and utilization information.

Note

You can view VLAN properties on the event properties page, if applicable, even though DFM does not display alerts generated on VLANs. The Detailed Device View will display to which VLAN ports belong (see Starting the Detailed Device View, page 3-20).

**Step 1**

From the CiscoWorks home page, select **Alerts and Activities**. The Alerts and Activities display opens.

**Step 2**

Locate the alert you want to investigate and click the alert ID. The Alerts and Activities Detail page appears.

**Step 3**

Locate the event you want to investigate, and click the event ID. The event properties page appears.

The information that is shown on the event properties page depends on the event type.
Getting Device Information (Detailed Device View)

The Detailed Device View (DDV) provides extensive information on the devices and device components listed in Starting the Detailed Device View, page 3-20. You can view information on devices that DFM is currently managing, as well as devices whose management you have suspended (regardless of whether the device is generating an alert):

- View hardware and software information on system, environment, and interface components (including port VLAN information)
- View hardware and software information on subcomponents of aggregate devices (for example, Multilayer Switch Feature Cards (MSFCs) on switches)
- Suspend or resume management of a device or a device component so the device or component is no longer polled, or polling is resumed

See these topics for more information:

- Starting the Detailed Device View, page 3-20
- Understanding the Layout of the Detailed Device View, page 3-23
- Detailed Device View Examples, page 3-24

Starting the Detailed Device View

You can open a DDV for any device in the Alerts and Activities page—or for any known device in the DFM inventory (regardless of whether it is currently managed).

Note: You cannot display a DDV for unidentified trap devices. For more information on unidentified traps, refer to Processed and Pass-Through Traps, and Unidentified Traps and Events, page B-1
Getting Device Information (Detailed Device View)

Chapter 3  Using the Alerts and Activities Display

Step 1  Open the DDV as follows:

- For any known device, from the DFM home page, select Device Management > View Device Details and click the device link.
- For devices with alerts, click the device link in the Alerts and Activities display Device Name column.

The DDV opens. (See Figure 3-7 for an example.)

Step 2  Select an instance from the device tree. The details table is populated.

Step 3  If the item you select is the subdevice of an aggregated device—for example, an MSFC/RSM in a switch—the DDV will show the subdevice’s managed state and device capability. To display a complete DDV of the subcomponent, click the Launch New DDV For This Device button.

Step 4  If you want to suspend a managed device so it is no longer polled and its traps are no longer processed (or if you want to resume a suspended device):

- Click Suspend to change the device’s managed state to Suspended. DFM no longer polls any device components, nor does it process any traps. All alerts and activities change to the Cleared state, and the device is moved to the Suspended Devices view. Subsequent events (including traps) are ignored and no longer processed.
- Click Resume to change the device’s managed state to Active. DFM resumes polling and trap processing on the device, and the device is moved out of the Suspended Devices view and back into its previous view.

Step 5  If you resumed any devices (and you are finished making all of your monitoring status changes), select Configuration > Polling and Thresholds > Apply Changes from the DFM home page so that DFM will resume polling according to the polling and threshold settings for the device. (Because this action is CPU-intensive, wait until you have made all of your monitoring status changes before you apply them.)
Figure 3-7 provides an example of device information for a Cisco 3640 router.

**Figure 3-7  Detailed Device View—Cisco 3640 Router**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Record count. See Record Count, page 3-23.</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 3      Using the Alerts and Activities Display

Getting Device Information (Detailed Device View)

Understanding the Layout of the Detailed Device View

These topics provide details about the information in the DDV.

Component Categories Pane
The component categories pane lists the components of the device: Environment, System, and/or Interface (what is shown depends on the device being viewed). The following are some examples of what you may see in these categories:

- Environment: Temperature, fan, power supply, voltage information
- System: Hard disk, RAM, processor, memory information
- Interface: Interface, port, card information

From a DDV for an aggregate (containing) device, you can launch a DDV for the contained device. For example, for a router containing MSFCs, open a DDV for the router. From the router DDV, you can launch a new DDV for the MSFC. See Detailed Device View Examples, page 3-24.

System Information Pane
The system information pane provides information such as the system name, IP address, SysObjectID, system contact, and so forth. The device type determines what is displayed by the DDV. Examples of different DDVs are provided in Detailed Device View Examples, page 3-24.

If the system information pane lists an attribute with no value, it is because of one of the following reasons:

- The attribute is not populated.
- The attribute is not configured correctly.
- The attribute does not apply to the device.

You can suspend or resume device or component monitoring by clicking the Suspend or Resume button (the button shown depends on the component’s current managed state). These functions are described in these sections:

- Suspend, page 3-27
- Resume, page 3-28

Record Count
The record count lists the number of information types available on the device.
Command Buttons Area

In addition to the Suspend and Resume button in the system information pane, the command button area provides other ways to respond to alerts.

Table 3-7 Detailed Device View—Command Buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>Refreshes the DDV page. (The DDV is not automatically refreshed; you must do so manually.)</td>
</tr>
<tr>
<td>Close</td>
<td>Closes the DDV page.</td>
</tr>
</tbody>
</table>

Launch Information

The launch information tells you when the DDV was started. If you refresh the page, the time is updated.

Detailed Device View Examples

Figure 3-8 shows a DDV for a Cisco Catalyst 6513 switch. This switch (the containing device) contains an MSFC card (a contained device). Containing and contained devices must be added separately (refer to How DFM Handles Containing and Contained Devices, page 4-13 for more information).
This switch contains an MSFC card. If you select the MSFC card, the DDV displays the managed state of the subcomponent on the right side of the display (see Figure 3-9), and a new DDV launch point is provided.
Suspending Device Monitoring

To display a DDV for the MSFC card, click Launch New DDV For This Device. The new DDV appears, as shown in Figure 3-10.

Figure 3-10 Detailed Device View—Cisco MSFC Card

Suspending Device Monitoring

You can stop monitoring a device by selecting it and clicking the Suspend button in the DDV. Conversely, you can resume monitoring by clicking the Resume button. These actions are also available for suspending and resuming specific components. See these topics for more information:

- Suspending/Resuming Devices, page 3-27
- Suspending/Resuming a Device Component, page 3-28
Suspending/Resuming Devices

When you unmanage a device—changing its managed state to false—DFM no longer polls that device for information. Subsequent events (including traps) are ignored and no longer processed.

When you suspend a device, all of the active events on the device are moved to the Cleared state, but the alert remains in the Active state. This happens to ensure that:

- You cannot mistakenly remove important information from the display when you suspend a device (when alerts are cleared, they are removed from the Alerts and Activities display).
- You can easily resume the device.

Note

Your login determines whether you can perform this operation.

Step 1

From the Alerts and Activities display, start the view that contains your device. (Devices not managed will be in the Suspended Devices view.) The DDV opens. Depending upon the managed state of the device, either the Suspend or the Resume button is shown.

Step 2

Do one of the following:

- Click **Suspend** to change the device’s current managed state to Suspended. DFM no longer polls any device components, nor does it process any traps. All alerts and activities change to the Cleared state, and the device is moved to the Suspended Devices view. Subsequent events (including traps) are ignored and no longer processed.
- Click **Resume** to change the device’s current managed state to Active. DFM resumes polling and trap processing on the device, and the device is moved out of the Suspended Devices view and back into its previous view.

Step 3

If you resumed any devices (and you are finished making all of your monitoring status changes), select **Configuration > Polling and Thresholds > Apply Changes** from the DFM home page so that DFM will resume polling according
Suspending/Resuming a Device Component

You can unmanage or remanage device components using the DDV. When you unmanage a component—changing its managed state to false—DFM no longer polls that component for information. Subsequent events (including traps) are ignored and no longer processed.

**Note**

You cannot resume a device component if the parent device is suspended. You must resume the parent device first. If a parent device is suspended, the device components are also suspended.

**Step 1**

From the Alerts and Activities display, click a device in the Device Name column. The DDV opens.

**Step 2**

Select the component with the instance you want to unmanage.

**Step 3**

Locate the instance you want to unmanage, and make your change using the list in the ManagedState column.

**Step 4**

Click **Submit**.

**Step 5**

If you resumed any devices (and you are finished making all of your monitoring status changes), select **Configuration > Polling and Thresholds > Apply Changes** from the DFM home page so that DFM will resume polling according to the polling and threshold settings for the device. (Because this action is CPU-intensive, wait until you have made all of your monitoring status changes before you apply them.)

Figure 3-11 shows the location of the ManagedState column for one of the managed interfaces on a Cisco 3620 router.
Acknowledging, Annotating, and Sending E-Mail Notifications of Alerts

As shown in Figure 3-4 on page 3-13, the Alerts and Activities Detail page provides command buttons in the bottom-right corner of the page. The Suspend button is discussed in Suspending Device Monitoring, page 3-26. This topic explains how you can use the Acknowledge, Annotate, and Notify buttons to respond to alerts.

See these topics for more information:

- Acknowledging an Alert, page 3-30
- Annotating an Alert, page 3-30
- Sending E-Mail in Response to an Alert, page 3-31
Acknowledging an Alert

Acknowledging an active alert signals other users that you are aware of the alert. When you click the **Acknowledge** button on the Alerts and Activities Detail page, this status change is populated to all Alerts and Activities displays.

If an event on the alert recurs, the event status reverts to Active.

**Step 1**
From the Alerts and Activities Detail page, click **Acknowledge**. A confirmation window opens.

**Step 2**
Click **OK**.

Annotating an Alert

You can annotate an alert by clicking the **Annotate** button from the Alerts and Activities Detail page. An editable Annotation dialog box opens; in the dialog box, you can enter up to 255 characters. An annotation will be shown whenever other users view the alert from an Alerts and Activities Detail page.

**Step 1**
From the Alerts and Activities Detail page, click **Annotate**. The Annotation dialog box opens.

**Step 2**
Enter your text. Text that exceeds 255 characters will be truncated without warning. (If this happens, you can add another annotation.)

**Step 3**
Click **OK**. The annotated text is displayed in the Notes box.
Figure 3-12 shows the Alerts and Activities Detail page, containing a previously created annotation.

**Figure 3-12 Annotation on the Alerts and Activities Detail Page**

Sending E-Mail in Response to an Alert

When you click the Notify button on the Alerts and Activities Detail page, DFM opens a dialog box that you can complete to manually send an e-mail notification to multiple recipients. The e-mail notification will contain only the text you add; it will not append any alert or event information. (If you want to send automatic e-mail notifications when alerts or events occur on certain devices, use Notification Services to set up an E-mail Notification subscription. Refer to Managing E-Mail Notifications, page 5-16.)

CiscoWorks Common Services controls the SMTP server used by DFM. For more information, from the CiscoWorks home page, select Common Services > Server > Admin > System Preferences, and click Help.
Step 1  From the Alerts and Activities Detail page, click **Notify**. The E-mail Notification Recipient(s) dialog box opens.

Step 2  In the E-mail Notification Recipient(s) dialog box:

   a. Select your SMTP server by doing one of the following:
      • Click the SMTP Server button and select the SMTP server you want to use.
      • Enter a fully qualified DNS name or IP address for an SMTP server.
   b. Click the Domain Names button and select the domain you want to use.
   c. Enter your e-mail address in the Sender Address field.
   d. Enter a comma-separated list of e-mail addresses in the Recipient Address(es) field.
   e. Enter a subject heading in the Header field.
   f. (Optional) Enter a message in the Message field.
   g. Click **Send**.
Using Device Management

These topics explain how to use Device Fault Manager (DFM) Device Management:

- Getting Started with Device Management, page 4-2
- Understanding the Device and Credentials Repository, page 4-8
- Understanding the Device Summary and Device States, page 4-10
- Importing Devices into DFM, page 4-12
- Exporting Devices, page 4-24
- Editing Device Configuration and Credentials, page 4-26
- Rediscovering Devices, page 4-29
- Deleting Devices, page 4-30
- Viewing Device Details, page 4-32
- Modifying SNMP Timeout and Retries, page 4-34
Getting Started with Device Management

For DFM to monitor a device, you must first add the device to the Device and Credentials Repository (DCR). Use the DCR to perform the following operations:

- Adding devices
- Importing devices
- Exporting devices
- Changing device credentials

Once a device is added to the DCR, you can then add it to the DFM inventory, which is separate from the DCR. You can add devices from the DCR to DFM automatically by activating automatic synchronization (the default), or you can add them selectively by deactivating using the Device Selector. For more information on how DFM is affected by the DCR, refer to Understanding the Device and Credentials Repository, page 4-8.

DFM is the front-end for performing the following operations on devices in the DFM inventory:

- Deleting devices (local delete)
- Viewing device details
- Rediscovering devices
- Suspending and resuming DFM device management

As DFM discovers devices, they pass through various device states until they are fully recognized by DFM (see Verifying Device Import Using Discovery Status, page 4-19 for details). Once a device is discovered, DFM manages the device and its components according to the polling and threshold settings that apply to the device group (when it is added to the DCR, the DCR assigns the device to a device group).

Technically, DFM manages a device when the device’s management state is set to True; conversely, DFM is not managing a device when its management state is set to False. A device with a management state set to False is also called a suspended device. You can also selectively unmanage device components (see Suspending/Resuming a Device Component, page 3-28).
If the DFM server is using Access Control Server (ACS) mode, ACS may limit the devices you are permitted to view. For more information, refer to Device-Based Filtering, page 11-11.

For information on how many devices DFM can manage, refer to Installation and Setup Guide for Device Fault Manager. If the DFM inventory exceeds your device limit, you will see a warning message. For more information, see Responding to Messages About Device Limits, page 2-13.

Types of Devices and Device Elements that DFM Monitors

When devices are added to the DCR, they are assigned to Common Services System Defined Groups. The group to which the DCR assigns the device depends on the device type users specify when they add the device. If a user does not select a device type, or selects the wrong device type, the DCR designates the device as Unknown, and it is assigned to the Common Services Unknown group. (For devices with no specified device type, DFM assigns a device type when it discovers the device.) See Table 4-1 on page 4-11 for more information.

Figure 4-1 shows an example of the Common Services System Defined Groups, as seen in the DFM Object Selector.

Figure 4-1  Common Services System Defined Groups

When devices are imported into CiscoWorks, Common Services assigns each device to the appropriate CiscoWorks Common Services system defined group. These groups are listed in Common Services System Defined Groups, page 8-4. When a device is added to the DFM inventory, DFM assigns the device
components to the appropriate DFM system defined port and interface groups. These groups are listed in DFM System Defined Groups, page 8-6. Figure 4-1 shows the DFM system defined groups, as shown in the DFM object selector.

**Figure 4-2  DFM System Defined Groups**

DFM manages many device components: chassis, cards, fans, interfaces, memory, Multilayer Switch Feature Cards (MSFCs), Multilayer Switch Modules (MSMs), ports, power supplies, processors, Route Switch Feature Cards (RSFCs), Route Switch Modules (RSMs), SNMP agents, temperature sensors, VLANs, and voltage sensors. For a detailed list of specific device families and models that DFM supports, refer to Supported Device Table for Device Fault Manager at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dev_sup/index.htm.

Note
The Alerts and Activities display does not report alerts generated on VLANs. However, you can view VLAN information on the Event properties page and in the Detailed Device View. (Refer to Viewing Event Properties, page 3-19 and Starting the Detailed Device View, page 3-20.)
Ports and Interfaces that DFM Manages

DFM manages device ports and interfaces, as described in the following:

- **Ports (on switches)**—By default, DFM manages trunk ports but does not manage access ports.
  - A *trunk port* is a port that is connected to another Layer 2 device (such as a switch, bridge, or hub).
  - An *access port* is a port that is either not connected to any device, or is connected to a non-Layer 2 device (such as a router).

- **Interfaces (on routers)**—By default, DFM manages all interfaces listed in a device ifTable.

When a device is added to DFM, DFM assigns the device interfaces and ports to DFM system defined groups depending on their type. For more information on port and interface groups, see **DFM System Defined Groups, page 8-6**.

Listing Ports and Interfaces in the DFM Inventory

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

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

Locate the line that is similar to the following:

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

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

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.
Note

The following script is supported only if you have downloaded and installed DFM 2.0 IDU 2.0.1 (or later) from the DFM download site: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm.

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

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

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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-DNetworkAdapterType=Interface</td>
<td>List interfaces, ports, or both (all). The default is all.</td>
</tr>
<tr>
<td>-DPortType=ACCESS</td>
<td>(Ports only.) List access ports, trunk ports, or all ports. The default is all.</td>
</tr>
<tr>
<td>-DGroupName=“device”</td>
<td>List ports or interfaces for a specified device, or for a specified DFM trunk port, access port, or interface group. Use the following formats:</td>
</tr>
<tr>
<td>device</td>
<td>List information for a device, using name or IP address.</td>
</tr>
<tr>
<td>CFG-“group/type”</td>
<td>List information for a port or interface group. group can be Interface Groups, Access Port Groups, or Trunk Port Groups. type can be any subgroup under the port or interface group. For example: “CFG-Interface Groups/1GB Ethernet”</td>
</tr>
<tr>
<td>-DManagedState=managed</td>
<td>List managed or unmanaged ports or interfaces. The default is managed.</td>
</tr>
</tbody>
</table>
The following examples show how you can use the getNetworkAdapters.asl script.

- To list all managed interfaces and ports:
  
  ```bash
  sm_adapter -s DFM utils/getNetworkAdapters.asl
  ```

- To list all managed and unmanaged ports and interfaces on the lab-gw.cisco.com device:
  
  ```bash
  sm_adapter -s DFM -DNetworkAdapterType=all -DPortType=all
  -DGroupName="lab-gw.cisco.com" -DManagedState=all
  utils/getNetworkAdapters.asl
  ```

- To list all managed ports and interfaces on the lab-gw.cisco.com device:
  
  ```bash
  sm_adapter -s DFM -DGroupName="lab-gw.cisco.com"
  utils/getNetworkAdapters.asl
  ```

- To list all managed interfaces on the lab-gw.cisco.com device:
  
  ```bash
  sm_adapter -s DFM -DNetworkAdapterType=Interface
  -DGroupName="lab-gw.cisco.com" -DManagedState=managed
  utils/getNetworkAdapters.asl
  ```

- To list all unmanaged interfaces on the lab-gw.cisco.com device:
  
  ```bash
  sm_adapter -s DFM -DNetworkAdapterType=Interface
  -DGroupName="lab-gw.cisco.com" -DManagedState=unmanaged
  utils/getNetworkAdapters.asl
  ```

- To list all unmanaged 1 GB Ethernet interfaces:
  
  ```bash
  sm_adapter -s DFM -DNetworkAdapterType=all -DPortType=all
  -DGroupName="CFG-Interface Groups/1 Gb Ethernet"
  -DManagedState=unmanaged utils/getNetworkAdapters.asl
  ```

- To list all managed 10/100 MB Ethernet ports (access ports):
  
  ```bash
  sm_adapter -s DFM -DNetworkAdapterType=all -DPortType=all
  -DGroupName="CFG-Port Groups - Access Ports/10/100 Mb Ethernet"
  -DManagedState=managed utils/getNetworkAdapters.asl
  ```

- To list all managed 10/100 MB Ethernet ports (trunk ports):
  
  ```bash
  sm_adapter -s DFM -DNetworkAdapterType=all -DPortType=all
  -DGroupName="CFG-Port Groups - Trunk Ports/10/100 Mb Ethernet"
  -DManagedState=managed utils/getNetworkAdapters.asl
  ```
Chapter 4      Using Device Management

Understanding the Device and Credentials Repository

The DCR is a centralized device repository for sharing device information across applications. It provides a single place for managing device credentials and attributes, ensuring consistency across applications. Individual applications can query the DCR for a device list, device attributes, and device credentials. Changes to the DCR are propagated to all applications. Thus, you should use the DCR to add, import, and export devices, and to change device credentials.

**Note**
A device must be added to the DCR before it can be added to the DFM inventory.

Once a device is added to the DCR, you can add it to the DFM inventory (the DFM inventory is separate from the DCR). When a device is added to the DCR, the DCR assigns a DCR ID to every managed component. The DCR maps components to devices using either the device name or IP address. When the DCR device is added to DFM, DFM maps the DCR ID to a device name during discovery (see How DFM Determines Device Names, page 4-13).

DFM also uses the DCR ID to verify if the device or component already exists in the DFM inventory (in which case it is not added but is designated as an alias device). (Further information on how DFM identifies devices—such as whether DFM uses an IP address or DNS name as the device name—is provided in Importing Devices from the DCR, page 4-12.)

You can add devices from the DCR to DFM automatically by activating automatic synchronization (which is the default), or you can add them selectively by deactivating using the Device Selector. When a device is deleted locally (from the DFM inventory), the DCR is not affected. The device is added to the Device Selector list, which shows which devices are in the DCR but not in DFM. (In this way, you can easily add the device back to DFM, if desired.)

If a device is deleted from the DCR (global delete), it is deleted from DFM (and all other applications that use that DCR). (For information on deleting components of aggregate devices, see How DFM Handles Containing and Contained Devices, page 4-13.)

All synchronization between the DCR and the DFM inventory is controlled from the Device Management > Device Selector page.
For automatic synchronization, the Synchronize with Device and Credentials Repository check box must be selected. Refer to Automatically Importing DCR Devices, page 4-15.

For manual synchronization (in which you selectively add devices from the DCR to the DFM inventory), the Synchronize with Device and Credentials Repository check box must not be selected. Refer to Manually Importing DCR Devices Using the Device Selector, page 4-16. (However, if a device is deleted from the DCR, it is deleted from DFM.)

Note
Do not confuse the DFM discovery process with the DCR synchronization process. DFM discovery/rediscovery is a process that affects only the DFM inventory.

For more information on the DCR, refer to the Common Services online help.

Events That Trigger DCR and DFM Synchronization

The following events will trigger synchronization between the DFM inventory and the DCR:

- Devices are added or deleted, or their credentials (IP address, SNMP credentials, MDF type) are changed in the DCR. (This also triggers a device rediscovery in DFM).
- DCR is changed from:
  - Master to slave
  - Standalone (single server) to slave
- DCR is restored from a different domain.

See these topics for more information:

- Importing Devices from the DCR, page 4-12
- Rediscovering Devices, page 4-29
DCR Masters and Slaves

By default, the DCR mode is standalone (single server), and CiscoWorks supports one DCR per CiscoWorks server. However, you can configure the DCR to use a master/slave model. In this model, the master DCR is the primary repository residing on a CiscoWorks server. Slave DCRs reside on other CiscoWorks servers, and replicate the DCR master. Any change in the master DCR is propagated to slave DCRs. This allows applications on different servers to use a synchronized device inventory. Using the master/slave model is transparent to DFM.

If the DCR used by your instance of DFM is changed from master to slave, or from standalone to slave, the DCR device list is synchronized with the DFM inventory. First, all devices are removed from the DFM inventory (regardless of DCR synchronization mode). If DFM is configured to use manual synchronization, all DCR devices will appear in the Device Selector (as devices not in DFM). For automatic synchronization, all DCR devices are added to the DFM inventory.

For more information on the DCR Master/Slave model, refer to the Common Services online help.

Understanding the Device Summary and Device States

The Device Summary lists the device states for all devices in the DFM inventory. The device summary appears when you select Device Management > Device Summary from the DFM home page. Figure 4-3 shows an example of the Device Summary page.
### Table 4-1 Device Summary and Device States

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
<td>Lists the state the devices are in, from the following possibilities:</td>
</tr>
<tr>
<td>Known</td>
<td>The device has been successfully imported, and is fully managed by DFM.</td>
</tr>
<tr>
<td>Learning</td>
<td>DFM is discovering the device. This is the beginning state, when the device is first added or is being rediscovered. Some of the data collectors may still be gathering device information.</td>
</tr>
<tr>
<td>Questioned</td>
<td>DFM cannot manage the device. See Troubleshooting Device Import and Discovery, page 4-20.</td>
</tr>
<tr>
<td>Pending</td>
<td>The device is being deleted. (DFM is waiting for confirmation from all of its data collectors before purging the device and its details.)</td>
</tr>
<tr>
<td>Unknown</td>
<td>The device is not supported by DFM.</td>
</tr>
</tbody>
</table>

| Number of Devices| The number of devices that are in each device state.                                               |

---

1. Data collector is a term used to refer to all back-end applications that are involved in device rediscovery and device data collection.

---

#### Figure 4-3 Device Summary Page

Table 4-1 describes the information displayed on the Device Summary page.

**Table 4-1 Device Summary and Device States**

<table>
<thead>
<tr>
<th>Status</th>
<th>Number of Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known</td>
<td>20</td>
</tr>
<tr>
<td>Learning</td>
<td>0</td>
</tr>
<tr>
<td>Questioned</td>
<td>7</td>
</tr>
<tr>
<td>Pending</td>
<td>0</td>
</tr>
<tr>
<td>Unknown</td>
<td>0</td>
</tr>
</tbody>
</table>

---

**Figure 4-3 Device Summary Page**

![Device Summary Table](image-url)

- **Device Summary**
  - Status as of Tue 26-Sep-2004 21:57:01 PDT
  - Status: Known, Learning, Questioned, Pending, Unknown
  - Number of Devices: 20, 0, 7, 0, 0

---

**Refresh**
Importing Devices into DFM

A device must be in the DCR before you can add it to the DFM inventory. DFM supports three methods of device import from the DCR:

- Using automatic synchronization between the DCR and DFM (see Automatically Importing DCR Devices, page 4-15)
- Using manual synchronization between the DCR and DFM (see Manually Importing DCR Devices Using the Device Selector, page 4-16)
- Importing DFM 1.2.x devices (see Importing Devices from DFM 1.2.x, page 4-18)

Importing Devices from the DCR

Once a device has been added to the DCR, it can be added to the DFM inventory:

- Automatically (whenever there is an addition or change), if you activate the Synchronize with Device and Credentials Repository check box in the Device Selector.
- Manually (on a device-by-device basis), if you do not activate the Synchronize with Device and Credentials Repository check box in the Device Selector.

To verify which setting you are using, from the DFM home page, select Device Management > Device Selector, and check the synchronization setting.

Note
Your login determines whether you can import devices into DFM.

How DFM Identifies Devices Imported from the DCR

When a device is added to DFM from the DCR, DFM attempts to resolve the DNS name (hostname). DFM does not use the DCR Display Name. Table 4-2 shows how DFM names devices, depending on how the devices are added to the DCR.
Table 4-2 How DFM Determines Device Names

<table>
<thead>
<tr>
<th>When device is added to DCR with...</th>
<th>DFM does the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address and hostname (DNS name)</td>
<td>Uses the DNS name, if DFM can resolve it Uses the IP address, if DFM cannot resolve the DNS name</td>
</tr>
<tr>
<td>IP address only</td>
<td>Uses the DNS name, if DFM can resolve the IP address Uses the IP address, if DFM cannot resolve the DNS name</td>
</tr>
<tr>
<td>DNS name only</td>
<td>Uses the DNS name, even if not resolvable</td>
</tr>
<tr>
<td>IP address, and the IP address was already added to the DCR (this is allowed in the DCR)</td>
<td>Chooses one IP address and makes the other an alias (duplicate)</td>
</tr>
<tr>
<td>IP address, and the IP address corresponds to two interfaces of the same physical device</td>
<td>Chooses one IP address and make the other an alias (duplicate)</td>
</tr>
</tbody>
</table>

Note: Once a device is added to the DCR with a specified MDF type and sysObjectID, no one can overwrite it, even if it is incorrect. The only exception is if no sysObjectID is supplied, as described in the previous table.

For information on how DFM performs polling and discovery, refer to Appendix E, “Polling—SNMP and ICMP.”

How DFM Handles Containing and Contained Devices

DFM supports contained and containing devices (also referred to as aggregate devices). These are devices that have a parent/child relationship with another device, such as a Catalyst switch (parent) containing an MSFC (child). The switch is considered the containing device, and the MSFC is the contained device.
### Table 4-3 How DFM Handles Containing and Contained Devices

<table>
<thead>
<tr>
<th>Action</th>
<th>Effect on Device</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Containing</td>
<td>Contained</td>
<td></td>
</tr>
<tr>
<td><strong>Adding to DFM (regardless of DCR synchronization mode)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Containing</td>
<td>Added</td>
<td>Added¹</td>
<td></td>
</tr>
<tr>
<td>Contained</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td><strong>Rediscovering in DFM</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Containing</td>
<td>Rediscovered</td>
<td>Rediscovered</td>
<td></td>
</tr>
<tr>
<td>Contained</td>
<td>No effect</td>
<td>Rediscovered</td>
<td></td>
</tr>
<tr>
<td><strong>Removing from DFM</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Containing</td>
<td>Deleted</td>
<td>Deleted from DFM (but not deleted from DCR)</td>
<td></td>
</tr>
<tr>
<td>Contained</td>
<td>No effect</td>
<td>Deleted</td>
<td></td>
</tr>
<tr>
<td><strong>Removing from DCR</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Containing</td>
<td>Deleted</td>
<td>Deleted</td>
<td></td>
</tr>
<tr>
<td>Contained</td>
<td>No effect</td>
<td>Deleted</td>
<td></td>
</tr>
<tr>
<td><strong>Suspending in DFM</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Containing</td>
<td>Suspended</td>
<td>Suspended</td>
<td></td>
</tr>
<tr>
<td>Contained</td>
<td>No effect</td>
<td>Suspended</td>
<td></td>
</tr>
<tr>
<td><strong>Resuming in DFM</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Containing</td>
<td>Resumed</td>
<td>Resumed</td>
<td></td>
</tr>
<tr>
<td>Contained</td>
<td>No effect</td>
<td>Resumed only if containing device is resumed</td>
<td></td>
</tr>
</tbody>
</table>

¹. When a containing device is added to the DCR, the DCR does not recognize the contained devices. However, when the device is added to DFM, the contained devices are discovered by DFM and added to the DFM inventory.
Automatically Importing DCR Devices

DFM uses automatic synchronization by default. Use the following procedure to change manual synchronization to automatic synchronization.

**Note**
If you are running the synchronization process for the first time, it may take several hours for DFM to discover all of the devices, depending on how many devices are being added to DFM.

**Step 1**
From the DFM home page, select Device Management > Device Selector. (If you previously removed any devices from DFM, these devices will be listed in the Devices Not in Device Fault Manager field.)

**Step 2**
Activate the Synchronize with Device and Credentials Repository check box.

**Step 3**
Click OK. DFM will be synchronized with the DCR; any DCR devices currently not in DFM will be added. The new devices that are added to DFM will be discovered.

**Step 4**
Verify whether any aliases exist by selecting Device Management > Device Aliases. If you do not require the alias for your deployment, remove it using Common Services > Device and Credentials > Device Management.

**Note**
If you exceed your device limit, DFM will continue to operate, but you will notice that devices are not being added to DFM. Check the license log as described in Viewing and Maintaining Log Files, page 11-18. For information on device-based licensing, see Responding to Messages About Device Limits, page 2-13.

For information on the rediscovery schedule, refer to Configuring Rediscovery Schedules, page 7-7.
Manually Importing DCR Devices Using the Device Selector

Use the following procedure to change automatic synchronization to manual synchronization.

---

**Step 1**  
From the DFM home page, select **Device Management > Device Selector**. (If you previously removed any devices from DFM, these devices will be listed in the Devices Not in Device Fault Manager field.)

**Step 2**  
Make sure the Synchronize with Device and Credentials Repository check box is **not** activated.

**Step 3**  
Click **OK**.

**Step 4**  
To move devices from the DCR into DFM, select the DCR device (or devices) you want to add to DFM, and click **Add**.

**Step 5**  
Click Summary to verify your changes. (If any devices are listed as Duplicate Devices, you can get more information about those devices by selecting **Device Management > Device Aliases**.)

**Step 6**  
Click **OK**. The new devices that are added to DFM will be discovered.

**Step 7**  
Verify whether any aliases exist by selecting **Device Management > Device Aliases**. If you do not require the alias for your deployment, delete it from the DFM inventory using **Common Services > Device and Credentials > Device Management**.

---

**Note**  
If you exceed your device limit, DFM displays a warning message. You can get more information from the license log as described in **Viewing and Maintaining Log Files**, page 11-18. For information on device-based licensing, see **Responding to Messages About Device Limits**, page 2-13.

For information on how to handle duplicate devices, refer to **Viewing Alias (Duplicate) Devices**, page 4-18.
Determining Which Devices Are in DCR But Not in DFM

To identify devices that are in the DCR but not in DFM, use the Device Selector. The Device Selector lists devices that are not in DFM for these reasons:

- The devices have not been added to DFM because DFM is using manual DCR synchronization.
- The devices were deleted from DFM. (Devices you delete from DFM are not deleted from the DCR.)

You can start the Device Selector by selecting **Device Management > Device Selector** from the DFM home page.

*Figure 4-4  DFM Device Selector*
When you click Summary, DFM will display a total of devices in the following categories:

- Devices in DFM inventory
- Devices in DCR
- Duplicate Devices
- Devices in Device Credential Repository and not in Device Fault Manager

For information on moving devices from the DCR into DFM, refer to Manually Importing DCR Devices Using the Device Selector, page 4-16. For information on duplicate devices, refer to Viewing Alias (Duplicate) Devices, page 4-18.

**Importing Devices from DFM 1.2.x**

You can import a list of DFM 1.2.x devices into DFM, but first you must add those DFM 1.2.x devices to the DCR. These are the steps you must perform:

1. From the DFM 1.2.x server, use the command line to create a DCR-format list of your DFM 1.2.x devices and perform the bulk import into the DCR. This procedure is described in *Installation and Setup Guide for Device Fault Manager*.

2. Once the devices are in the DCR, add them to DFM using one of these methods:
   - Automatically Importing DCR Devices, page 4-15
   - Manually Importing DCR Devices Using the Device Selector, page 4-16

**Viewing Alias (Duplicate) Devices**

The Alias Devices page lists all devices for which DFM has found duplicates. DFM considers a device to be an alias when the device is added to DFM using its IP address, device name, or host name; and the IP address, device name, or host name already exists in the DCR.
Chapter 4      Using Device Management

Importing Devices into DFM

**Step 1** From the DFM home page, select Device Management > Device Aliases.

**Step 2** Select the device from the Normal Devices field and click Show Alias Devices. DFM displays all alias devices for the selected device in the Alias Devices field.

**Step 3** If you want to delete the alias device, use Common Services > Device and Credentials > Device Management.

---

**Verifying Device Import Using Discovery Status**

After adding a device, you can verify that it has been imported by using the Discovery Status page.

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

![Discovery Status Page](image)

**Figure 4-5  Discovery Status Page**

**Step 2** In the Device Name column, locate the device you added.
Importing Devices into DFM

Step 3 In the Status column, verify that your device is in the Known state. (The Last Discovered column displays the time it was fully discovered.) A Known state on the device indicates that it was imported successfully.

Note For a complete explanation of the device states, see Understanding the Device Summary and Device States, page 4-10.

Step 4 If the device is not in the Known state, refer to Troubleshooting Device Import and Discovery, page 4-20.

Troubleshooting Device Import and Discovery

Step 1 From the DFM home page, select Device Management > Rediscover/Delete. The Rediscover/Delete Devices page opens. (This page is described in Rediscovering and Deleting Devices, page 4-26.)
Figure 4-6  Rediscover/Delete Devices Page

Step 2  Expand the folder that contains your device (according to its discovery status; refer to Verifying Device Import Using Discovery Status, page 4-19).

Step 3  Click the device name or IP address. This will populate the Item Information field.

Step 4  Proceed as follows:

- To troubleshoot problems with Learning devices, proceed to Step 5.
- To troubleshooting problems with Questioned devices, proceed to Step 6.
- To troubleshoot problems with Pending devices, proceed to Step 7.
**Step 5**  For Learning Devices, locate the Data Collector Status information at the bottom of the Item Information field. If the Discovery Progress percentage does not change in a reasonable amount of time (10 minutes for a single device import and 3 hours for a 1,500-device bulk import), do the following:

a. Verify that the Common Services EssMonitor process (which handles distribution of events between processes) is running:
   - From the Common Services home page, selecting Server > Reports > Process Status, and click Generate.
   - Verify that the ESSMonitor process is running normally. If it is not, stop and start it using Server > Admin > Processes.

b. If the device is in the DCR but not in DFM, do the following:
   - Verify that the DFM InventoryCollector process is running by selecting Server > Reports > Process Status from the Common Services home page, and clicking Generate.
   - Verify that the TISServer process is running normally. If it is not, stop and restart it using Server > Admin > Processes.

   - If the percentage is equal to or less than 69%, stop and start the inventory Interactor process.
   - If the percentage is equal to or greater than 70%, stop and start the DFMOGSServer process.
Step 6  For Questioned Devices, locate your device in one of the following folders:

- SNMP Timeout—The device has timed out. The following are some possible causes:
  - Wrong or insufficient credentials (such as SNMP read-only community string)—Update the device credentials (as described in Editing Device Configuration and Credentials, page 4-26), and readd the device.
  - Wrong SysObjectID or MDF type was used when the device was added to the DCR. (Devices that were added to the DCR with no specified device type are assigned their appropriate device type when DFM discovers them.) You can verify this problem by selecting Device Management > Rediscover/Delete, clicking the device link, and checking the Error Message in the Item Information panel. It will say MDFIdmismatch. Fix the MDF type by reconfiguring the Device Type filed using Common Services > Device and Credentials > Device Management.
  - Device not operational during import—Verify that the device is operational.
  - Device does not support MIB II.
  - Data collector timeout—One of the data collectors did not respond in time. This can occur when the system is under a heavy load. To rediscover the device, see Rediscovering Devices, page 4-29.
  - The SNMP Timeout may be too short. This may be the problem if a device rediscovery times out for several devices. Increase the timeout setting, as described in Modifying SNMP Timeout and Retries, page 4-34.

- Others—In the right pane of the Rediscover/Delete Devices page, error codes and error messages are displayed. Act accordingly to fix the problem.

Step 7  For Pending devices (devices in the process of being deleted), if the device has been in the Pending state for more than ten minutes, stop and restart the InventoryCollector process using the Common Services Process Management page (Server > Admin > Processes).
Exporting Devices

You can export devices to create a backup of your devices list, or to import DFM devices into another CiscoWorks server that accepts DCR-format import files. The export file will contain a list of all managed devices, along with their credentials.

You can export devices using either of the following methods:

- For a list of all devices in the Device and Credentials Repository, use CiscoWorks Common Services. During export, CiscoWorks creates a DCR-format CSV or XML file that contains all of the devices in the DCR. For more information, from the Common Services home page select Device and Credentials > Device Management and click the Help button.

- For a list of all devices in DFM, use the DfmExport command (which is explained in the following procedure). During export, DFM creates a DCR-format CSV or XML file that contains all of the devices in the DFM inventory.

Note

For information on exporting the DFM 1.2.x device list to DFM 2.0, refer to Installation and Setup Guide for Device Fault Manager, which contains all of the migration instructions.

Use the following procedure to create a file containing the DFM 2.0 devices. Log information is written to NMSROOT\log\dfmLogs\TIS\DeviceManagement.log.
Step 1  
Verify that the DFM 2.0 installation has completed by checking the status of the TISServer process:


b. Locate the TISServer process and verify that Running Normally is listed in the State column.

Note  
If you are connecting to the DFM server for the first time, a Security Alert window is displayed after you select nearly any option. Do not proceed without viewing and installing the security certificate. For more information, see Responding to Security Alerts, page 2-12.

Step 2  
From the command prompt on the DFM server, run the export script:

- For Solaris:
  
  \( \text{NMSROOT/bin/dfmexport fn=fileName ft=CSV|XML} \)

- For Windows:
  
  \( \text{NMSROOT\bin\dfmexport.bat fn=fileName ft=CSV|XML} \)

where fn indicates the output filename and ft indicates the format. The export file is saved to the \( \text{NMSROOT/importfiles} \) directory. You should use a unique name for file name so that previous export files are not overwritten.
Editing Device Configuration and Credentials

After you add devices, you can change their configuration setup using CiscoWorks Common Services. From the CiscoWorks home page, select **Device and Credentials > Device Management**. From the Device Properties page, you can edit the following credentials:

- Basic information, IP address, and domain names.
- Device type (MDF group)
- Credentials information such as usernames, passwords, and community strings.
- User-defined fields that store additional user-defined data for a device.

**Note**

If you are changing credentials for a device that also has an alias, be sure to change the credentials on both devices in case the primary device is deleted.

Click the Help button to view more information on the device credentials you can change using Common Services.

Rediscovering and Deleting Devices

Rediscovering and deleting specific devices is controlled by the Rediscover/Delete Devices page. **Figure 4-7** shows the Rediscover/Delete Devices page.
If at any time while using the Rediscover/Delete Devices page, you want to refresh the view, click the **Refresh** button.

The Rediscover/Delete Devices page contains two panes. The left pane displays a device selector, from which you select the device or group that you want to rediscover or delete. The right pane displays the information for the selected object.

The devices that appear in the device selector are organized in folders by device state. (For a description of device states, see Understanding the Device Summary and Device States, page 4-10.) The folders appear only if there is a device to go in the folder. Figure 4-8 shows an example of the device selector.
Devices are displayed in four possible states: Known, Learning, Pending, and Questioned. DFM creates the following folders:

- **All Known Devices in Inventory Services**—This folder is created when there are fully discovered devices in the DFM inventory.
- **All Learning Devices in Inventory Services**—This folder is created when there are devices in the process of being discovered.
- **All Pending Devices in Inventory Services**—This folder is created when devices are being deleted from the DFM inventory.
- **All Questioned Devices in Inventory Services**—Two subfolders are also created, the first listing devices that encountered the SNMP Timeout error, and the second listing devices that encountered other errors. Descriptions of the errors are displayed in the right pane, next to Error Message.
Details about and procedures for rediscovering or deleting devices using this page are provided in these topics:

- Rediscovering Devices, page 4-29
- Deleting Devices, page 4-30

Rediscovering Devices

Through the Rediscover/Delete Devices page, you can rediscover devices or device groups. When rediscovery takes place, if there are any changes to a device or group configuration, the new settings will overwrite any previous settings.

Rediscovery occurs only for active devices. Suspended devices do not go through rediscovery. If some of the devices you are selecting for rediscovery are suspended devices, DFM displays messages indicating that only the active devices will go through rediscovery.

The following events will also trigger rediscovery:

- Inventory collection occurs (when the entire DFM inventory is polled). This is controlled by the Rediscovery Schedule. (Refer to Configuring Rediscovery Schedules, page 7-7.)
- DFM is using automatic synchronization with the DCR, and a device is added, or a change is made to a device in the DCR. Such DCR changes include a device being deleted or having its credentials (IP address, SNMP credentials, MDF type) changed in the DCR.
- DFM is using manual synchronization with the DCR, and a device is added to DFM using the Device Selector.

Note

Do not confuse the DFM discovery process with the DCR synchronization process. DFM discovery/rediscovery is a process that affects only the DFM inventory.
Rediscovering and Deleting Devices

Step 1  From the DFM home page, select Device Management > Rediscover/Delete. The Rediscover/Delete Devices page appears.

Note  If you are connecting to the DFM server for the first time, a Security Alert window is displayed after you select nearly any option. Do not proceed without viewing and installing the security certificate. For more information, see Responding to Security Alerts, page 2-12.

Step 2  Select the device or group that you want to rediscover.

Step 3  Click Rediscover. Rediscovery is started. To view rediscovery status, select Device Management > Discovery Status.

Deleting Devices

The DFM Rediscover/Delete Devices page allows you to delete devices from the DFM inventory (local deletion). It does not affect the DCR (all DCR device management is performed from the Common Services home page).

When a device is deleted from the DCR (which can only be done from the Common Services home page), it is automatically deleted from DFM, regardless of the synchronization setting. If you want to delete an alias device, use Common Services > Device and Credentials > Device Management.

When you delete a device from the DFM inventory and DFM is configured to use manual synchronization, the deleted device will appear in the Device Selector (in the Devices Not in Device Fault Manager field). A deleted device will not be readded when DFM inventory collection is performed.

Local deletions are disabled when DFM is configured to use automatic synchronization.

While a device is being deleted, DFM will not allow any rediscovery, suspend, or resume operations to be performed on the device. When you delete a containing device, all of the contained devices are deleted.
Note If you only want to suspend the managed state of a device, you do not need to delete the device from DFM. You can suspend and resume the managed state of a device through the Detailed Device View page. For more details on suspending and resuming the managed state of a device, see the following:

- Suspending Device Monitoring, page 3-26
- Suspending/Resuming a Device Component, page 3-28

Note Depending upon the load that exists on the system, DFM takes approximately 15 to 40 seconds to delete a device.

Note Your login determines whether you can perform this operation.

Step 1 From the DFM home page, select Device Management > Rediscover/Delete. The Rediscover/Delete Devices page appears.

Note If you are connecting to the DFM server for the first time, a Security Alert window is displayed after you select nearly any option. Do not proceed without viewing and installing the security certificate. For more information, see Responding to Security Alerts, page 2-12.

Step 2 Select the device or group that you want to delete.

Step 3 Click Delete.

Step 4 In the confirmation box, click Yes.
Viewing Device Details

On the Device Details page, you select the devices for which you want to see device details. The Device Details display opens and displays the information for the devices. You can also start a Detailed Device View (DDV) from this page, which is useful when you want to view details about a device that has no current alerts.

The Device Details display provides basic information about the device such as name, IP address, when it was added, and so on. (For a description of the Device Details display, see Understanding the Device Details Display, page 4-33.)

Devices are organized in folders according to their device state. (For a description of device states, see Understanding the Device Summary and Device States, page 4-10.)

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the DFM home page, select <strong>Device Management &gt; Device Details</strong>. The Device Details page appears.</td>
</tr>
<tr>
<td>Step 2</td>
<td>For each device for which you want to view details, expand the folders where the device is located.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select a device by clicking the box next to it. Do this for each device for which you want to view details. If you want to view details for all of the devices in a group, click the box next to the group.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>View</strong>. The Device Details display appears.</td>
</tr>
<tr>
<td>Step 5</td>
<td>To start a DDV for the device, click the Device Name link. The DDV appears. (For information on the DDV, refer to Understanding the Layout of the Detailed Device View, page 3-23.)</td>
</tr>
</tbody>
</table>
Understanding the Device Details Display

The Device Details display shows details for the devices that you select. See Viewing Device Details, page 4-32 for information on selecting devices.

Figure 4-9 shows an example of the Device Details display.

Figure 4-9  Device Details Display

Table 4-4 describes the information displayed in the Device Details display.

Table 4-4  Device Details Display

<table>
<thead>
<tr>
<th>Heading/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device name. Click this link to launch a Detailed Device View.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Device IP address.</td>
</tr>
<tr>
<td>Status</td>
<td>Current state the device is in.</td>
</tr>
<tr>
<td>Function</td>
<td>Description or function of the device.</td>
</tr>
<tr>
<td>First Added</td>
<td>The first time the device was added into DFM.</td>
</tr>
<tr>
<td>Last Discovered</td>
<td>The time and date the device was last discovered.</td>
</tr>
</tbody>
</table>
Modifying SNMP Timeout and Retries

If an SNMP query does not respond in time, DFM will time out. It will then retry contacting the device for as many times as displayed when you select **Device Management > SNMP Config**.

The timeout period is doubled for every subsequent retry. For example, if the timeout value is 4 seconds and the retries value is 3, DFM waits for 4 seconds before the first retry, 8 seconds before the second retry, and 16 seconds before the third retry.

The SNMP timeout and retries are global settings.

The default values are:

- Timeout—4 seconds
- Retries—3

Figure 4-10 shows an example of the SNMP Configuration page.

**Note** Changing the settings on this page will modify the settings on all devices managed by DFM.
Chapter 4 Using Device Management

Modifying SNMP Timeout and Retries

Figure 4-10 SNMP Configuration Page

<table>
<thead>
<tr>
<th>SNMP Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the global SNMP settings for all devices during discovery.</td>
</tr>
<tr>
<td>SNMP Timeout: 34</td>
</tr>
<tr>
<td>seconds</td>
</tr>
<tr>
<td>Number of Retries: 03</td>
</tr>
</tbody>
</table>

Note
Your login determines whether you can perform this operation.

Step 1
From the DFM home page, select Device Management > SNMP Config. The SNMP Configuration page appears.

Note
If you are connecting to the DFM server for the first time, a Security Alert window is displayed after you select nearly any option. Do not proceed without viewing and installing the security certificate. For more information, see Responding to Security Alerts, page 2-12.

Step 2
Select a new SNMP timeout setting.

Step 3
Select a new Number of Retries setting.

Step 4
Click Apply.

Step 5
In the confirmation box, click Yes.
Chapter 4  Using Device Management

Modifying SNMP Timeout and Retries
Device Fault Manager (DFM) generates alerts in response to events occurring in the IP fabric. DFM displays alerts in the Alerts and Activities display. In addition to monitoring operations with the Alerts and Activities display, you can forward information about alerts and events to other systems and users by using notification services.

Note

Because DFM 2.0 does not report alerts generated on VLANs, you cannot create notifications for VLAN faults. However, you can view VLAN information on the event properties page and in the Detailed Device View. (Refer to Viewing Event Properties, page 3-19 and Starting the Detailed Device View, page 3-20.)

The following topics explain notification service concepts and provide procedures for managing notifications:

- Understanding Notifications and Subscriptions, page 5-2
- Customizing the Names of DFM Events, page 5-5
- Configuring Event Sets and Notification Groups for Subscriptions, page 5-6
- Managing SNMP Trap Notifications, page 5-10
- Managing E-Mail Notifications, page 5-16
- Managing Syslog Notifications, page 5-22
Understanding Notifications and Subscriptions

This topic describes the types of notifications that DFM sends, defines a subscription, and explains how DFM matches alerts and events to subscriptions to determine when to send notifications.

Notification Services tracks events on device types, not on device components. For a list of supported events and the device types on which they can occur, refer to Events Processed, page D-1.

**Creating a Notification Subscription**

To create a notification subscription, perform the following steps:

1. If you want to monitor a specific set of events or alerts, create one or more event sets that contain the events you want to monitor. Otherwise, all events and alerts will be monitored.

2. Create a notification group that specifies the criteria DFM should use when generating notifications:
   - One or more event sets (if no event set is specified, all events and alerts are monitored)
   - Devices, alert severity and status, and event severity and status

You can specify the notification group name, along with entering identifying information (using the Customer ID and Customer Revision fields).

3. Create a subscription by doing the following:
   - a. Select the notification type (SNMP Trap, E-Mail, or Syslog).
   - b. Name the subscription and apply a notification group to it.
   - c. Specify the recipients (hostname, e-mail address).
   - d. Save the subscription. It will automatically start running.
Chapter 5      Using Notification Services

Understanding Notifications and Subscriptions

Notification Types
DFM provides three types of notifications:

- **SNMP Trap Notification**—DFM generates traps with information about the alert and the events that caused it. CISCO-EPM-NOTIFICATION-MIB defines the trap message format. For more information, see Notification MIB, page C-1. DFM can also generate SNMP trap notifications for specified events.

  **Note** Using SNMP trap notification is different from forwarding raw traps to another server before they have been processed by DFM. For information about the raw traps that DFM can forward, see Pass-Through SNMP Unidentified Traps, page B-3.

- **E-mail notification**—DFM generates e-mail messages containing information about the alert and the events that caused it. CISCO-EPM-NOTIFICATION-MIB defines the message, which is included in the e-mail in text format. DFM can also generate e-mail notifications for specified events.

- **Syslog Notification**—DFM generates syslog messages that can be forwarded to syslog daemons on remote systems.

Subscriptions
DFM sends notifications based on user-defined subscriptions. You can create up to 32 notification subscriptions. A subscription for SNMP trap notification or e-mail notification includes the following common elements, as determined by the CISCO-EPM-NOTIFICATION-MIB:

- **Devices**—The devices or device groups of importance to the recipients.
- **Alert severity and status**—One or more alert severity levels and status.
- **Event severity and status**—One or more event severity levels and status.
  You can also customize the names of the events used by Notification Services, the Alerts and Activities display, and Fault History. Refer to Customizing the Names of DFM Events, page 5-5.
- **Recipients**—One or more hosts to receive SNMP traps or users to receive e-mail. For syslog notifications, the recipient would be the remote host containing a syslog daemon configured to listen for syslog messages.
- **Name**—A user-defined name to identify the subscription.
Subscriptions are based on user-configured event sets and notification groups. Refer to Configuring Event Sets and Notification Groups for Subscriptions, page 5-6 for more information.

**Alerts and Events**

DFM sends notifications whenever an alert occurs that matches a subscription. DFM also sends notifications whenever specific events occur. For each alert or event, DFM compares the device, severity, and state against subscriptions and sends a notification when there is a match. Matches can be determined by user-configured event sets and notification groups. (The procedure for configuring notification groups is described in Configuring Event Sets and Notification Groups for Subscriptions, page 5-6.)

DFM assigns one severity to each alert or event and changes the state of an alert or event over time, responding to user input and changes on the device. Table 5-1 on page 5-4 lists values for severity and explains how the state of an alert or event changes over time.

---

**Table 5-1  Alert and Event Severity and Status**

<table>
<thead>
<tr>
<th>Severity</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Informational</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>Active—The alert or event is live.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ACK—A user has manually acknowledged the alert. A user can acknowledge only active alerts or events.</td>
</tr>
<tr>
<td></td>
<td>Cleared—The alert or event is no longer active.</td>
</tr>
</tbody>
</table>

---

**Note**

You can change event names to names that are more meaningful to you. Refer to Customizing the Names of DFM Events, page 5-5.

---

**Note**

Alerts or events that have been cleared either expire or, if associated with a suspended device, remain in DFM until a user resumes or deletes the device.
Chapter 5  Using Notification Services

Customizing the Names of DFM Events

For additional information, please see the following topics:
- Getting Alert Details, page 3-6
- Getting Event Details, page 3-11

Customizing the Names of DFM Events

Notification Services allows you to customize the names of events displayed in DFM. When you customize an event name, that name is reflected in all notifications, on the Alerts and Activities display, and in Fault History. The new event name is used for all instances of an event, regardless of the component on which the event occurs.

You can easily revert to the default event names as needed. The Notification Customization page also lists the new name and default name, so you can easily check which names have been changed.

Step 1  From the DFM home page, select Notification Services > Notification Customization. The Notification Customization page appears, as shown in Figure 5-1.

Figure 5-1  Notification Customization Page

Step 2  Select the event names you want to customize by clicking the check box beside each event name.

Step 3  Enter your new names in the New Event Description fields.
Step 4  Do one of the following:

- Click **Save new descriptions** to save your changes but not apply them to the DFM displays.
- Click **Apply saved descriptions** to apply your changes to subsequent DFM displays. When the confirmation window appears, click **Yes**, and your changes will be applied to DFM.

Step 5  To revert to default event names:

a. From the Notification Customization page, select the events you want to restore to their default names, and click **Restore factory settings**.

b. Apply your changes by clicking **Yes** when the confirmation window appears.

For additional information, please see the following topic:

- **Getting Event Details, page 3-11**

---

**Configuring Event Sets and Notification Groups for Subscriptions**

Before you can create an SNMP trap or an e-mail or syslog notification subscription, you must create a notification group. Creating event sets is optional.

- **Event sets** list the events you want monitored for notifications
- **Notification groups** contain the criteria that DFM should use when generating a notification:
  - One or more event sets, or all events and alerts
  - Devices
  - Alert status and severity
  - Event status and severity
  - Fields for user-specified additional information you want to include with the subscription
Chapter 5  Using Notification Services

Configuring Event Sets and Notification Groups for Subscriptions

Creating event sets and notification groups are described in the following topics:

- Configuring Event Sets, page 5-7
- Configuring Notification Groups, page 5-8

Configuring Event Sets

Event sets are simply groups of the events you want to monitor. You can create up to 9 event sets, labeled A through I. Once you have created an event set, you can apply as many of them as you want to a notification group, thereby tracking the specific events in which you are interested. If you do not specify an event set, DFM will monitor all events and alerts for notifications.

Step 1  From the DFM home page, select Notification Services > Event Sets. The Event Sets page appears, as shown in Figure 5-2.

Figure 5-2  Event Sets Page
The Event Sets page contains the following information.

<table>
<thead>
<tr>
<th>Event Code</th>
<th>Notification Services code for the event. This number cannot be changed and is used to map default names to customized names.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Event description (user-defined or default).</td>
</tr>
<tr>
<td>Severity</td>
<td>Event severity.</td>
</tr>
<tr>
<td>A - I</td>
<td>Event set label. If an X appears in this column, the corresponding event belongs to that event set.</td>
</tr>
</tbody>
</table>

**Step 2**
For each event set you want to configure, select events by doing one of the following:

- Select specific events by clicking the editable field under the label, and selecting X.
- Select or deselect all events for an event set using the **Select/Deselect** button.

**Step 3**
Click **Apply**.

**Step 4**
If you want to create a notification subscription, first create a notification group that uses your event set. See **Configuring Notification Groups**, page 5-8.

For additional information, please see the following topic:
- **Configuring Notification Groups**, page 5-8

**Configuring Notification Groups**

When you set up a subscription, DFM lets you choose from existing notification groups. You can then configure an SNMP trap or an e-mail or syslog notification to use a specific notification group. The notification groups contain the following information:

- One or more event sets, if desired (otherwise, the notification group will contain all events and alerts)
- Devices
- Alert status and severity
### Configuring Event Sets and Notification Groups for Subscriptions

- Event status and severity
- Fields for user-specified additional information you want to include with the subscription

You can configure a maximum of 64 notification groups. If the DFM server is using Access Control Server (ACS) mode, ACS may limit the devices you can view and then apply to a notification group. Notification Services will not refilter the devices if there is a change in the device list you may access. For more information, refer to Device-Based Filtering, page 11-11.

**Note**

You cannot delete a notification group that is being used by a running subscription.

---

**Step 1**

From the DFM home page, select **Notification Services > Notification Groups**. The Notification Groups page appears, as shown in [Figure 5-3](#).

![Notification Groups Page](image)

**Figure 5-3 Notification Groups Page**

**Step 2**

To create a notification group, click **Add**. (If you want to edit or delete a notification group, click the appropriate button and follow the instructions.)

**Step 3**

Specify the devices, alert severity and status, event sets (if desired), and event severity and status. Click **Next**.
Managing SNMP Trap Notifications

Step 4 Specify the notification group name, and enter any desired identifying information in the Customer ID and Customer Revision fields.

- For e-mail and syslog notifications, if you leave these fields empty, they are left blank in the notification.
- For SNMP trap notifications, if you leave these fields empty, they are displayed as followed in any notifications:
  
  Customer ID: -
  
  Customer Revision: *

Click Next.

Step 5 Create the notification group by clicking Finish.

Step 6 To create a notification subscription, follow the instructions in one of these topics:

- Adding an SNMP Trap Notification Subscription, page 5-12
- Adding an E-Mail Notification Subscription, page 5-17
- Adding a Syslog Notification Subscription, page 5-24

For additional information, please see the following topic:

- Configuring Event Sets, page 5-7

Managing SNMP Trap Notifications

The SNMP Trap Notifications page displays the following information:

- **Subscription**—The name of the user-defined request for notification.
- **Status**—The subscription status; can be either of the following:
  - Running—DFM is using the subscription while monitoring alerts to determine when to send a notification.
  - Suspended—DFM will not use the subscription unless you resume it.
- **Notification Group**—The name of notification group that is applied to the subscription.
You are completely in control of subscriptions. DFM does not delete subscriptions under any circumstances.

From the SNMP Trap Notifications page, you can perform the tasks listed in Table 5-2.

**Table 5-2 SNMP Trap Notification Subscriptions**

<table>
<thead>
<tr>
<th>Task</th>
<th>Sample Usage</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>• Add a subscription that will send SNMP trap notification for one device with an alert or event of any severity (critical, warning, or informational) and any status (active, acknowledged, or cleared).</td>
<td>Adding an SNMP Trap Notification Subscription, page 5-12</td>
</tr>
</tbody>
</table>
| Edit | • View the notification group and hosts that comprise the subscription.  
• Change the trap recipients/notification groups that comprise the subscription. | Editing an SNMP Trap Notification Subscription, page 5-13 |
| Suspend | • Temporarily stop sending SNMP trap notifications to a host.  
• Temporarily stop sending SNMP trap notifications about a device group. | Suspending an SNMP Trap Notification Subscription, page 5-14 |
| Resume | • Start sending SNMP trap notifications to a host again.  
• Start sending SNMP trap notifications about a device group using a previously suspended subscription. | Resuming an SNMP Trap Notification Subscription, page 5-15 |
| Delete | • Remove SNMP trap notification subscriptions that are no longer useful.  
• Remove redundant SNMP trap notification subscriptions. | Deleting an SNMP Trap Notification Subscription, page 5-15 |
Adding an SNMP Trap Notification Subscription

After you add a subscription for SNMP trap notification, generated SNMP traps are forwarded to the hosts you specify until you change, suspend, or delete the subscription.

Note
Adding a subscription is a multistep process. Your changes are not saved until you click the Finish button on the final page.

Before You Begin
You must create a notification group before you can create an SNMP trap notification subscription. Refer to Configuring Notification Groups, page 5-8.

Step 1
From the DFM home page, select Notification Services > SNMP Trap Notification. The SNMP Trap Notification Subscriptions page appears.

Step 2
Click the Add button.

Step 3
Complete the Trap Subscription Save: Add window:

a. Enter a subscription name.

b. Select a notification group.

c. If you are upgrading DFM and want to use the trap recipients from an earlier configuration, activate the Recipients from Upgrade check box. (This choice is only available for systems that have been upgraded from earlier versions of DFM.)

d. Click Next.
**Managing SNMP Trap Notifications**

**Step 4** Enter one or more hosts as recipients for traps:

a. For each host, enter:
   - An IP address or DNS name for the hostname.
   - A port number on which the host can receive traps. If the port number is unspecified (empty), the port defaults to 162. (You can verify this in Step 5.)
   - (Optional) A comment.

b. Click **Next**.

**Step 5** Review the information that you entered and click **Finish**. The SNMP Trap Notifications page is displayed, showing the new subscription.

---

**Note** No information is saved until you complete **Step 5**.

---

**Editing an SNMP Trap Notification Subscription**

You can edit an **SNMP trap notification** subscription regardless of its status (Running or Suspended).

After you edit an SNMP trap notification subscription, if the subscription status is Running, traps are forwarded as specified until you edit, suspend, or delete the subscription. Editing a suspended subscription automatically resumes it.

---

**Note** Editing a subscription is a multistep process. Your changes are not saved until you click the Finish button on the final page.

---

**Step 1** From the DFM home page, select **Notification Services > SNMP Trap Notification**. The SNMP Trap Notification Subscriptions page appears.

**Step 2** Select the subscription you want to edit by clicking the radio button beside it.

**Step 3** Click the **Edit** button.

No information is saved until you complete **Step 5**.
Managing SNMP Trap Notifications

Step 4 Edit the Trap Subscription Save: Edit window:

a. Change the subscription name.
b. Select another notification group.
c. Click Next.

Step 5 Add or delete a recipient host or change the port number for a host:

a. To add one or more recipients, for each host, enter:
   - An IP address or DNS name for the hostname.
   - A port number on which the host can receive traps. If the port number is unspecified (empty), the port defaults to 162. (You can verify this in Step 6.)
   - (Optional) A comment.

b. To delete a recipient, delete the hostname, port number, and comment, if any.
c. Click the Next button.

Step 6 Review the information that you entered and click the Finish button. The SNMP Trap Notifications page is displayed.

Suspending an SNMP Trap Notification Subscription

After you suspend an SNMP trap notification subscription, DFM stops using the subscription to select and forward traps. The subscription status changes to Suspended.

Step 1 From the DFM home page, select Notification Services > SNMP Trap Notification. The SNMP Trap Notification Subscriptions page appears.

Step 2 Select the subscription you want to suspend by clicking the radio button beside it.

Step 3 Click the Suspend button.

Step 4 Click OK in the confirmation dialog box. The SNMP Trap Notification Subscriptions page is displayed. The subscription status is Suspended.
Resuming an **SNMP Trap Notification Subscription**

You can resume an **SNMP trap notification** subscription only when the subscription status is Suspended. After you resume a subscription, DFM starts using it to identify alerts for which to forward traps. The subscription status changes to Running.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the DFM home page, select <strong>Notification Services &gt; SNMP Trap Notification</strong>. The SNMP Trap Notification Subscriptions page appears.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select the subscription you want to resume by clicking the radio button beside it.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the <strong>Resume</strong> button.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>OK</strong> in the confirmation dialog box. The SNMP Trap Notification Subscriptions page is displayed. The subscription status is Running.</td>
</tr>
</tbody>
</table>

Deleting an **SNMP Trap Notification Subscription**

You can delete an **SNMP trap notification** subscription regardless of the subscription status. Deleting a subscription removes it permanently from DFM.

**Note**

You can also suspend a subscription. Suspending a subscription causes the subscription to not be used until a user resumes it.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the DFM home page, select <strong>Notification Services &gt; SNMP Trap Notification</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select the subscription you want to delete by clicking the radio button beside it.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the <strong>Delete</strong> button.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>OK</strong> in the confirmation dialog box. The SNMP Trap Subscriptions page appears. The subscription is no longer displayed.</td>
</tr>
</tbody>
</table>
Managing E-Mail Notifications

The E-Mail Notifications page displays the following information:

- **Subscription**—The name of the user-defined request for notification.
- **Status**—The subscription status; can be either of the following:
  - Running—DFM is using the subscription while monitoring alerts to determine when to send a notification.
  - Suspended—DFM will not use the subscription unless you resume it.
- **Notification Group**—The name of notification group that is applied to the subscription.

You are completely in control of subscriptions. DFM does not delete subscriptions under any circumstances. From the E-Mail Notifications page, you can perform the tasks listed in Table 5-3.

<table>
<thead>
<tr>
<th>Task</th>
<th>Sample Usage</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>• Add a subscription that will send e-mail notification to a user for one device with an alert or event of any severity (critical, warning, or informational) and any status (active, acknowledged, or cleared).</td>
<td>Adding an E-Mail Notification Subscription, page 5-17</td>
</tr>
<tr>
<td></td>
<td>• View the notification group and e-mail recipients that comprise the subscription.</td>
<td>Editing an E-Mail Notification Subscription, page 5-19</td>
</tr>
<tr>
<td></td>
<td>• Change the e-mail recipients/notification group that comprise the subscription.</td>
<td></td>
</tr>
</tbody>
</table>
Adding an E-Mail Notification Subscription

After you add a subscription for e-mail notification, DFM sends e-mail to the users you specify whenever an alert occurs that matches the subscription.

**Note** Adding a subscription is a multistep process. Your changes are not saved until you click the Finish button on the final page.

**Before You Begin**
You must create a notification group before you can create an E-Mail Notification subscription. Refer to Configuring Notification Groups, page 5-8.

**Table 5-3 E-Mail Notification Subscriptions (continued)**

<table>
<thead>
<tr>
<th>Task</th>
<th>Sample Usage</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resume</td>
<td>• Start sending e-mail notifications to a user again.</td>
<td>Resuming an E-Mail Notification Subscription, page 5-21</td>
</tr>
<tr>
<td></td>
<td>• Start sending e-mail notifications about a device group using a previously suspended subscription.</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>• Remove e-mail notification subscriptions that are no longer useful.</td>
<td>Deleting an E-Mail Notification Subscription, page 5-22</td>
</tr>
<tr>
<td></td>
<td>• Remove redundant e-mail notification subscriptions.</td>
<td></td>
</tr>
</tbody>
</table>

**Adding an E-Mail Notification Subscription**

After you add a subscription for e-mail notification, DFM sends e-mail to the users you specify whenever an alert occurs that matches the subscription.

**Step 1** From the DFM home page, select **Notification Services > E-Mail Notification**.
The E-Mail Notification Subscriptions page appears.

**Step 2** Click the Add button.

**Step 3** Complete the E-Mail Subscription Save: Add window:

- Enter a subscription name.
- Select a notification group.
- If you are upgrading DFM and want to use the e-mail recipients from an earlier configuration, activate the Recipients from Upgrade check box. (This choice is only available for systems that have been upgraded from earlier versions of DFM.)
- Click Next.
Managing E-Mail Notifications

Step 4 Enter the e-mail information:

a. Provide the following information:

- **SMTP Server**—The name of the default Simple Mail Transfer Protocol (SMTP) server may already be displayed. The server is specified using Configuration > Other Configuration > SMTP Default Server. You may also enter a fully qualified DNS name or IP address for an SMTP server.

  Note To select from any nondefault SMTP servers in use by existing subscriptions, click the SMTP Servers button.

- **Sender Address**—Enter the e-mail address that notifications should be sent from. If the sender’s e-mail service is hosted on the SMTP server specified, you need enter only the username. You do not need to enter the domain name.

- **Recipient Address(es)**—Enter one or more e-mail addresses that notifications should be sent to, separating multiple addresses with either a comma or a semicolon. If a recipient’s e-mail service is hosted on the SMTP server specified, you need to enter only the username. You do not need to enter the domain name.

- By default, e-mail notification supplies a fully detailed e-mail message. To omit the message body and send only a subject line, select the Headers Only check box.

b. Click the **Next** button located at the bottom of the page.

Step 5 Review the information that you entered and click the **Finish** button. The E-Mail Notification Subscriptions page is displayed, showing the new subscription.

Note No information is saved until you complete Step 5.

Note For instructions on how to configure a default SMTP server, see Configuring a Default SMTP Server, page 7-15.
Editing an E-Mail Notification Subscription

You can edit an e-mail notification subscription regardless of its status (Running or Suspended).

After you edit an e-mail notification subscription, if the subscription status is Running, e-mail is forwarded as specified until you change, suspend, or delete the subscription. Editing a suspended subscription automatically resumes it.

Note

Editing a subscription is a multistep process. Your changes are not saved until you click the Finish button on the final page.

Step 1
From the DFM home page, select Notification Services > E-Mail Notification. The E-Mail Notification Subscriptions page appears.

Step 2
Select the subscription you want to edit by clicking the radio button beside it.

Step 3
Click the Edit button.

Step 4
Edit the E-Mail Subscription Save: Edit window:

a. Change the subscription name.

b. Select another notification group.

c. Click Next.
Step 5  Change the SMTP server, the sender, the recipients, or the amount of detail sent in e-mail as needed:

- SMTP Server—The name of the default Simple Mail Transfer Protocol (SMTP) server may already be displayed. The server is specified using Configuration > Other Configuration > SMTP Default Server. You may also enter a fully qualified DNS name or IP address for an SMTP server.

  **Note**  To select from any nondefault SMTP servers in use by existing subscriptions, click the SMTP Servers button.

- Sender Address—Enter the e-mail address that notifications should be sent from. If the sender’s e-mail service is hosted on the SMTP server specified, you need to enter only the username. You do not need to enter the domain name.

- Recipient Address(es)—Enter one or more e-mail addresses that notifications should be sent to. When entering multiple addresses, include a comma or a semicolon between addresses. If a recipient’s e-mail service is hosted on the SMTP server specified, you need to enter only the username. You do not need to enter the domain name.

- By default, e-mail notification supplies a fully detailed e-mail message. If, however, the Headers Only check box is selected, the message body is omitted from the e-mail.

Step 6  Click the Next button located at the bottom of the page.

Step 7  Review the information that you entered and click the Finish button. The E-Mail Notification Subscriptions page is displayed.

**Note**  For instructions on how to configure a default SMTP server, see Configuring a Default SMTP Server, page 7-15.
Suspending an E-Mail Notification Subscription

After you suspend an e-mail notification subscription, DFM stops using the subscription to send e-mail notification. The subscription status changes to Suspended.

Step 1  From the DFM home page, select Notification Services > E-Mail Notification. The E-Mail Notification Subscriptions page appears.

Step 2  Select the subscription you want to suspend by clicking the radio button beside it.

Step 3  Click the Suspend button.

Step 4  Click OK in the confirmation dialog box. The E-Mail Notification Subscriptions page is displayed. The subscription status is Suspended.

Resuming an E-Mail Notification Subscription

After you resume an e-mail notification subscription, DFM starts using the subscription to determine when e-mail notification should be sent in response to an alert. The subscription status changes to Running.

Step 1  From the DFM home page, select Notification Services > E-Mail Notification. The E-Mail Notification Subscriptions page appears.

Step 2  Select the subscription you want to resume by clicking the radio button beside it.

Step 3  Click the Resume button.

Step 4  Click OK in the confirmation dialog box. The E-Mail Notification Subscriptions page is displayed. The subscription status is Running.
Deleting an E-Mail Notification Subscription

You can delete an e-mail notification subscription regardless of the subscription status. Deleting a subscription removes it permanently from DFM.

Note

You can also suspend a subscription. Doing so causes the subscription to not be used until a user resumes it.

Step 1
From the DFM home page, select Notification Services > E-Mail Notification.

Step 2
Select the subscription you want to delete by clicking the radio button beside it.

Step 3
Click the Delete button.

Step 4
Click OK in the confirmation dialog box. The E-Mail Subscriptions page appears. The subscription is no longer displayed.

Managing Syslog Notifications

The Syslog Notifications page displays the following information:

- Subscription—The name of the user-defined request for notification.
- Notification Group—The name of notification group that is applied to the subscription.
- Status—The subscription status; can be either of the following:
  - Running—DFM is using the subscription while monitoring alerts to determine when to send a notification.
  - Suspended—DFM will not use the subscription unless you resume it.

You are completely in control of subscriptions. DFM does not change or delete subscriptions under any circumstances. From the syslog Notifications page, you can perform the tasks listed in Table 5-4.
### Table 5-4 Syslog Notification Subscriptions

<table>
<thead>
<tr>
<th>Task</th>
<th>Sample Usage</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>• Add a subscription that will send a syslog notification to a remote machine for one device with an alert or event of any severity (critical, warning, or informational) and any status (active, acknowledged, or cleared).</td>
<td>Adding a Syslog Notification Subscription, page 5-24</td>
</tr>
<tr>
<td>Edit</td>
<td>• View the notification group and syslog recipient that comprise the subscription.</td>
<td>Editing a Syslog Notification Subscription, page 5-25</td>
</tr>
<tr>
<td></td>
<td>• Change the syslog recipients/notification group that comprise the subscription.</td>
<td></td>
</tr>
<tr>
<td>Suspend</td>
<td>• Temporarily stop sending syslog notifications to a remote host.</td>
<td>Suspending a Syslog Notification Subscription, page 5-27</td>
</tr>
<tr>
<td></td>
<td>• Temporarily stop sending syslog notifications about a device group.</td>
<td></td>
</tr>
<tr>
<td>Resume</td>
<td>• Start sending syslog notifications to a remote host again.</td>
<td>Resuming a Syslog Notification Subscription, page 5-27</td>
</tr>
<tr>
<td></td>
<td>• Start sending syslog notifications about a device group using a previously suspended subscription.</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>• Remove syslog notification subscriptions that are no longer useful.</td>
<td>Deleting a Syslog Notification Subscription, page 5-28</td>
</tr>
<tr>
<td></td>
<td>• Remove redundant syslog notification subscriptions.</td>
<td></td>
</tr>
</tbody>
</table>
Adding a Syslog Notification Subscription

After you add a subscription for syslog notification, DFM sends a syslog message to the specified remote hosts whenever an alert or event occurs that matches the subscription.

**Note**
Adding a subscription is a multistep process. Your changes are not saved until you click the Finish button on the final page.

**Before You Begin**
- You must create a notification group before you can create a Syslog Notification subscription. Refer to Configuring Notification Groups, page 5-8.
- A remote machine’s syslog daemon must be configured to listen on a specified port, and you must enter this information in Step 3 of the following procedure. DFM uses the default port 514.

**Step 1**
From the DFM home page, select **Notification Services > Syslog Notification**. The Syslog Notification Subscriptions page appears.

**Step 2**
Click the **Add** button.

a. Enter a subscription name.

b. Select a notification group.

c. Select a facility from the drop-down list (the default is Local Use 0). The Facility field and the event/alert severity are used for the PRI portion of the syslog message, as follows:

   \[
   [Facility*8][Severity]
   \]

   Event/alert severity values are as follows:
   - Critical = 2
   - Warning = 4
   - Information = 6

d. (Optional) Enter location information (up to 29 characters). This information will be populated in the syslog message.

e. Click **Next**.
**Step 3** Enter one or more hosts as recipients for syslog notifications.

a. For each host, enter:
   - An IP address or DNS name for the hostname.
   - A port number on which the syslog daemon is listening. If the port number is unspecified (empty), the port defaults to 514. (You can verify this in Step 5.)
   - (Optional) A comment.

b. Click **Next**.

**Step 4** Enter the name of the subscription in the Save As field and click the **Next** button.

**Step 5** Review the information that you entered and click the **Finish** button. The Syslog Notification Subscriptions page is displayed, showing the new subscription.

---

**Note** No information is saved until you complete **Step 5**.

---

**Editing a Syslog Notification Subscription**

You can edit a syslog notification subscription regardless of its status (Running or Suspended).

After you edit a syslog notification subscription, if the subscription status is Running, syslog messages are forwarded as specified until you change, suspend, or delete the subscription. Editing a suspended subscription automatically resumes it.

---

**Note** Editing a subscription is a multistep process. Your changes are not saved until you click the **Finish** button on the final page.

---

**Step 1** From the DFM home page, select **Notification Services > Syslog Notification**. The Syslog Notification Subscriptions page appears.

**Step 2** Select the subscription you want to edit by clicking the radio button beside it.

**Step 3** Click the **Edit** button.
**Step 4**
Edit the Syslog Subscription Save: Edit window:

a. Change the subscription name.

b. Select a different notification group.

c. Select a Facility from the drop-down list (the default is Local Use 0). The Facility field and the event/alert severity is used for the PRI portion of the syslog message, as follows:

\[
[Facility*8][Severity]
\]

Event/alert severity values are as follows:

- Critical = 2
- Warning = 4
- Informational = 6

d. (Optional) Enter location information (up to 29 characters). This information will be populated in the syslog message.

e. Click **Next**.

**Step 5**
Add or delete a recipient host or change the port number for a host:

a. To add one or more recipients, for each host, enter:

- An IP address or DNS name for the hostname.
- A port number on which the syslog daemon is listening. If the port number is unspecified (empty), the port defaults to 514. (You can verify this in **Step 7**.)
- (Optional) A comment.

b. To delete a recipient, delete the hostname, port number, and comment, if any.

c. Click the **Next** button.

**Step 6**
Click the **Next** button located at the bottom of the page.

**Step 7**
Review the information that you entered and click the **Finish** button. The Syslog Notification Subscriptions page is displayed.
Suspending a Syslog Notification Subscription

After you suspend a syslog notification subscription, DFM stops using the subscription to send syslog notifications. The subscription status changes to Suspended.

Step 1 From the DFM home page, select Notification Services > Syslog Notification. The Syslog Notification Subscriptions page appears.
Step 2 Select the subscription you want to suspend by clicking the radio button beside it.
Step 3 Click the Suspend button.
Step 4 Click OK in the confirmation dialog box. The Syslog Notification Subscriptions page is displayed. The subscription status is Suspended.

Resuming a Syslog Notification Subscription

After you resume a syslog notification subscription, DFM starts using the subscription to determine when syslog notifications should be sent in response to an alert or event. The subscription status changes to Running.

Step 1 From the DFM home page, select Notification Services > Syslog Notification. The Syslog Notification Subscriptions page appears.
Step 2 Select the subscription you want to resume by clicking the radio button beside it.
Step 3 Click the Resume button.
Step 4 Click OK in the confirmation dialog box. The Syslog Notification Subscriptions page is displayed. The subscription status is Running.
Deleting a Syslog Notification Subscription

You can delete a syslog notification subscription regardless of the subscription status. Deleting a subscription removes it permanently from DFM.

Note
You can also suspend a subscription. Doing so causes the subscription to not be used until a user resumes it.

Step 1 From the DFM home page, select Notification Services > Syslog Notification.
Step 2 Select the subscription you want to delete by clicking the radio button beside it.
Step 3 Click the Delete button.
Step 4 Click OK in the confirmation dialog box. The Syslog Subscriptions page appears. The subscription is no longer displayed.
Using Fault History

These topics explain how to use Device Fault Manager (DFM) Fault History:

- Getting Started with Fault History, page 6-1
- Starting Fault History, page 6-3
- Understanding the Fault History: Alerts and Activities Display, page 6-12
- Understanding the Fault History: Events Display, page 6-14

Getting Started with Fault History

Fault History allows you to store and view the history of DFM events and alerts from the past 31 days (this setting cannot be changed). The stored history includes alert information and annotations (informational text that you enter), and event information and properties (for example, the values of MIB attributes at the time of the event, polling and threshold information, and utilization information). For an example of what kind of information Fault History displays, see Figure 6-1 on page 6-12 and Figure 6-2 on page 6-15.

You can also customize the names of events displayed by Fault History (and the Alerts and Activities display) using the Notification Customization feature in Notification Services. For more information, refer to Customizing the Names of DFM Events, page 5-5.
You can start Fault History from within DFM in one of two ways:

- To generate the most granular reports using all saved information in the Fault History database, start Fault History by selecting **Fault History** from the DFM home page. See **Starting Fault History from the DFM Home Page**, page 6-5.

- To generate a quick, contextual 24-hour report, start Fault History from the Alerts and Activities display. See **Starting Fault History from the Alerts and Activities Display**, page 6-3.

A link to Fault History is also provided in the Device Center, which you can open by selecting **Device Troubleshooting > Device Center** from the CiscoWorks home page. The Device Center provides a number of device-centric troubleshooting tools. This Fault History link is useful when you are troubleshooting a specific device, allowing you to quickly search the Fault History database for problems on that device. For more information, open the Device Center and click **Help**.

If Fault History finds more than 2,000 records while generating a report, a popup window tells you the total number of records found. The Fault History displays can show up to 2,000 records as a table you can scroll or page through. If your report exceeds 2,000 records and you want to view all of them, you can use the Export tool button to save all of the information to a CSV or PDF file.

You can use Fault History to generate customized tabular displays of specific alerts, specific events, event dates, event severity, and so forth. You might want to generate a Fault History report when:

- A significant alert is shown in the Alerts and Activities display, and you want to see how often the alert has been generated in the last month.

- You receive an e-mail notification that an unusual event has occurred.

- You want to search for information on events and alerts other than those you are tracking in your customized Alerts and Activities display.

The Fault History database is stored at **NMSROOT\databases\dfmFH\dfmFH.db**. The database stores a maximum of 31 days of data and is purged according to the DFM database purging schedule (see **Configuring the Daily Purging Schedule**, page 7-6.)
If the DFM server is using Access Control Server (ACS) mode, ACS may limit the devices you are permitted to view and for which you can create Fault History displays. For more information, refer to Device-Based Filtering, page 11-11.

**Note** Because DFM 2.0 does not report alerts generated on VLANs, Fault History does not store VLAN fault information in its database. However, you can view VLAN information on the event properties page and in the Detailed Device View. (Refer to Viewing Event Properties, page 3-19 and Starting the Detailed Device View, page 3-20.)

## Starting Fault History

DFM provides two starting points from which you can generate Fault History reports:

- To create a context-sensitive 24-hour report, use Fault History from the Alerts and Activities display. See Starting Fault History from the Alerts and Activities Display, page 6-3.
- To create filtered reports using all of the stored information in the Fault History database, use the DFM home page. See Starting Fault History from the DFM Home Page, page 6-5.

## Starting Fault History from the Alerts and Activities Display

Start Fault History from the Alerts and Activities display to create a 24-hour report on:

- All alerts in your current view, as described in Generating a 24-Hour Report on All Alerts in the Current View, page 6-4.
- All events on a specific device component, as described in Generating a 24-Hour Report on All Events on a Device Component, page 6-5.
Generating a 24-Hour Report on All Alerts in the Current View

To create a report on all the alerts that have occurred in your current view in the past 24 hours, start Fault History from the window tools area in the Alerts and Activities display. (See Window Tools Area, page 3-5.)

**Step 1**
From the DFM home page, select **Alerts and Activities > Alerts and Activities**. The Alerts and Activities display appears.

**Step 2**
Select a view from the view object selector. (See Configuring Views for the Alerts and Activities Display, page 9-1.)

**Step 3**
Launch Fault History from the window tools area to open a 24-hour Fault History tabular display of information about all alerts on all devices in the most recently accessed view. If Fault History finds more than 2,000 records, a popup window reports the total number of records found.

The Fault History: Alerts and Activities display appears. Understanding the Fault History: Alerts and Activities Display, page 6-12, describes the report contents.

**Step 4**
To see if any user annotations are associated with a specific alert, click the Status link. If a user has entered an annotation for this alert, the alert annotations page appears. (Annotations are entered from the Alerts and Activities display. See Annotating an Alert, page 3-30 for more information on annotations.)

If Fault History finds more than 2,000 records based on your search criteria, you can view all of the reports by clicking the Export button (in the upper-right corner of the display) and saving your report to a PDF or CSV file.
Chapter 6      Using Fault History

Generating a 24-Hour Report on All Events on a Device Component

To create a report on all events that have occurred on a specific device component in the past 24 hours, use the Fault History tool in the Alerts and Activities Detail display.

**Step 1** From the DFM home page, select *Alerts and Activities > Alerts and Activities*. The Alerts and Activities display appears.

**Step 2** Click an alert ID. The Alerts and Activities Detail display appears.

Locate the device component in which you are interested, and select Fault History from the list in the Tools column (see Figure 3-6 on page 3-19 for an example). If Fault History finds more than 2,000 records, a popup window reports the total number of records found.

The Fault History: Events display appears. Understanding the Fault History: Events Display, page 6-14, describes the display contents.

**Step 3** If you want to view more details about the event, such as the value of MIB attributes at the time of the event, click the appropriate event ID. The event properties page appears.

If Fault History found more than 2,000 records based on your search criteria, you can view all of the reports found by clicking the Export button (in the upper-right corner of the display) and saving your report to a PDF or CSV file.

Starting Fault History from the DFM Home Page

To gather historical information on alerts and events in the past 31 days, start Fault History from the CiscoWorks navigation tree by selecting *Fault History* from the DFM home page. The following topics explain how you can apply filters and generate reports based on all of the saved information in the Fault History database:

- To search for alerts by alert ID, device, or group, see Getting All Stored Information on an Alert, page 6-6.
- To search for events by event ID, device, alert ID, or group, see Getting All Stored Fault History on an Event, page 6-9.
Getting All Stored Information on an Alert

Fault History provides the following methods for searching for alerts that are in the saved Fault History database:

- Searching for Alerts by Alert ID, page 6-6
- Searching for Alerts by Device, page 6-7
- Searching for Alerts by Group, page 6-8

Searching for Alerts by Alert ID

To determine how often a specific alert has occurred, search for the alert by its alert ID. The alert ID is displayed in the Alerts and Activities display.

Step 1
From the DFM home page, select Fault History > Alert Filtering > Search By Alert ID. The Alert Filtering: Search by Alert ID page appears.

Step 2
Set your filtering criteria:
- a. Enter the alert ID.
- b. Activate all alert severity levels for which you want to search.
- c. Enter the date, selecting either Current Date, One Month, or Range. (The Current Date and One Month fields are read-only and cannot be changed.)

Step 3
Click View. If Fault History finds more than 2,000 records, a popup window reports the total number of records found.

The Fault History: Alerts and Activities display appears. (See Understanding the Fault History: Alerts and Activities Display, page 6-12, for an explanation of the display contents, and how to get more information on the alerts.)

If Fault History finds more than 2,000 records based on your search criteria, you can view them by clicking the Export button (in the upper-right corner of the display) and saving your report to a PDF or CSV file.
Searching for Alerts by Device

Use this procedure to determine what types of alerts are occurring on a specific device.

A link to Fault History is also provided in the Device Center, which provides a number of device-centric troubleshooting tools. This Fault History link is useful when you are troubleshooting a specific device, allowing you to quickly search the Fault History database for problems on that device. For more information, select Device Troubleshooting > Device Center from the CiscoWorks home page and click Help.

If the DFM server is using Access Control Server (ACS) mode, ACS may limit the devices you are permitted to view and for which you can create Fault History displays. For more information, refer to Device-Based Filtering, page 11-11.

---

**Step 1**
From the DFM home page, select Fault History > Alert Filtering > Search By Device. The Alert Filtering: Search by Device page appears.

**Step 2**
Set your filtering criteria:

a. Enter a comma-separated list of devices (as they are listed by Device Management).

b. Activate all alert severity levels for which you want to search.

c. Enter the date, selecting either Current Date, One Month, or Range. (The Current Date and One Month fields are read-only and cannot be changed.)

**Step 3**
Click View. If Fault History finds more than 2,000 records, a popup window reports the total records found.

The Fault History: Alerts and Activities display appears. (See Understanding the Fault History: Alerts and Activities Display, page 6-12, for an explanation of the display contents, and how to get more information on the alerts.)

If Fault History found more than 2,000 records based on your search criteria, you can view all of the reports found by clicking the Export button (in the upper-right corner of the display) and saving your report to a PDF or CSV file.
Chapter 6 Using Fault History

Searching for Alerts by Group

Step 1 From the DFM home page, select Fault History > Alert Filtering > Search By Group. The Alert Filtering: Search by Group page appears.

Step 2 Set your filtering criteria:

a. Select the device group. You can select multiple devices from different groups.

b. Activate all alert severity levels for which you want to search.

c. Enter the date, selecting either Current Date, One Month, or Range. (The Current Date and One Month fields are read-only and cannot be changed.)

Step 3 Click View. If Fault History finds more than 2,000 records, a popup window reports the total records found.

The Fault History: Alerts and Activities display appears. (See Understanding the Fault History: Alerts and Activities Display, page 6-12, for an explanation of the display contents, and how to get more information on the alerts.)

If Fault History found more than 2,000 records based on your search criteria, you can view all of the reports found by clicking the Export button (in the upper-right corner of the display) and save your report to a PDF or CSV file.
Getting All Stored Fault History on an Event

Fault History provides the following methods for searching for alerts that are in the saved Fault History database:

- Searching for Events by Event ID, page 6-9
- Searching for Events by Device, page 6-10
- Searching for Events by Alert ID, page 6-10
- Searching for Events by Group, page 6-11

Searching for Events by Event ID

To determine how often a specific event has occurred, search for the event by its event ID. The event ID is displayed on the Alerts and Activities Detail display. Remember that an event ID is not the same thing as the event codes provided by Notification Services. For more information, refer to Customizing the Names of DFM Events, page 5-5.

Step 1  From the DFM home page, select Fault History > Event Filtering > Search By Event ID. The Event Filtering: Search by Event ID page appears.

Step 2  Set your filtering criteria:
   a. Enter the event ID.
   b. Enter the date, selecting either Current Date, One Month, or Range. (The Current Date and One Month fields are read-only and cannot be changed.)

Step 3  Click View. If Fault History finds more than 2,000 records, a popup window reports the total records found.

The Fault History: Events display appears. (See Understanding the Fault History: Events Display, page 6-14, for an explanation of the display contents.)

Step 4  If you want to view more information about an event, such as the value of MIB attributes at the time of the event, click the appropriate event ID. The event properties page appears.

If Fault History found more than 2,000 records based on your search criteria, you can view all of the reports found by clicking the Export button (in the upper-right corner of the display) and save your report to a PDF or CSV file.
## Searching for Events by Device

**Step 1**
From the DFM home page, select **Fault History > Event Filtering > Search By Device**. The Event Filtering: Search by Device page appears.

**Step 2**
Set your filtering criteria:

- **a.** Enter a comma-separated list of devices (as they are listed by Device Management). You can select multiple devices from different groups.
- **b.** Enter the event description by clicking the popup selector box and activating the events for which you want to search. By default, all events are selected.
- **c.** Enter the date, selecting either Current Date, One Month, or Range. (The Current Date and One Month fields are read-only and cannot be changed.)

**Step 3**
Click **View**. If Fault History finds more than 2,000 records, a popup window reports the total records found.

The Fault History: Events display appears. (See **Understanding the Fault History: Events Display, page 6-14**, for an explanation of the display contents.)

**Step 4**
If you want to view more information about an event, such as the value of MIB attributes at the time of the event, click the appropriate event ID. The event properties page appears.

If Fault History found more than 2,000 records based on your search criteria, you can view all of the reports found by clicking the Export button (in the upper-right corner of the display) and save your report to a PDF or CSV file.

## Searching for Events by Alert ID

**Step 1**
From the DFM home page, select **Fault History > Event Filtering > Search By Alert ID**. The Event Filtering: Search by Alert ID page appears.

**Step 2**
Set your filtering criteria:

- **a.** Enter the Alert ID.
- **b.** (Optional) Enter the event description by clicking the popup selector box and activating the events for which you want to search.
- **c.** Enter the date, selecting either Current Date, One Month, or Range. (The Current Date and One Month fields are read-only and cannot be changed.)
Starting Fault History

Step 3
Click View. If Fault History finds more than 2,000 records, a popup window reports the total records found.

The Fault History: Events display appears. (See “Understanding the Fault History: Events Display” section on page 6-14, for an explanation of the display contents.)

Step 4
If you want to view more information about an event, such as the value of MIB attributes at the time of the event, click the appropriate event ID. The event properties page appears.

If Fault History found more than 2,000 records based on your search criteria, you can view all of the reports found by clicking the Export button (in the upper-right corner of the display) and save your report to a PDF or CSV file.

Searching for Events by Group

Step 1
From the DFM home page, select Fault History > Alert Filtering > Search By Group. The Event Filtering: Search by Group page appears.

Step 2
Set your filtering criteria:
   a. Enter the group.
   b. Enter the event description by clicking the popup selector box and activating the events for which you want to search.
   c. Enter the date, selecting either Current Date, One Month, or Range. (The Current Date and One Month fields are read-only and cannot be changed.)

Step 3
Click View. If Fault History finds more than 2,000 records, a popup window reports the total records found.

The Fault History: Events display appears. (See Understanding the Fault History: Events Display, page 6-14, for an explanation of the display contents.)

Step 4
If you want to view more information about an event, such as the value of MIB attributes at the time of the event, click the appropriate event ID. The event properties page appears.
Understanding the Fault History: Alerts and Activities Display

The Fault History: Alerts and Activities display is shown in Figure 6-1. You can generate this display as described in these sections:

- Generating a 24-Hour Report on All Alerts in the Current View, page 6-4
- Getting All Stored Information on an Alert, page 6-6

The tabular display is a scrollable table that lists up to 2,000 records, based on your filtering criteria. If you want to view database contents beyond the 2,000 records, click the Export tool button in the upper-right corner.

The Fault History: Alerts and Activities display provides two tools, as shown in Table 6-1.
Table 6-1  *Fault History: Alerts and Activities Display—Window Tools*

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Described in...</th>
</tr>
</thead>
<tbody>
<tr>
<td>![PDF or CSV file]</td>
<td>Exports all records found by Fault History to a PDF or CSV file.</td>
<td>Exporting Data from Tabular Displays, page 2-6</td>
</tr>
<tr>
<td>![Printer-friendly version]</td>
<td>Opens a printer-friendly version for printing (maximum of 2,000 records)</td>
<td>Printing Tabular Displays, page 2-7</td>
</tr>
</tbody>
</table>

Table 6-2 describes the contents of the Fault History: Alerts and Activities tabular display.

Table 6-2  *Fault History: Alerts and Activities Tabular Display—Contents*

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert ID</td>
<td>Alert identifier number. Clicking this link opens the Fault History: Events display (see Figure 6-2), which provides details about the events associated with the alert.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Device name or IP address. (If the DFM server is using Access Control Server (ACS) mode, ACS may limit the devices you are permitted to view and for which you can create Fault History displays. (For more information, refer to Device-Based Filtering, page 11-11.)</td>
</tr>
<tr>
<td>Device</td>
<td>Device type. <em>Learning</em> indicates that DFM was discovering the device at the time of the alert. The actual device type is reflected when new events occur. For more information, see Using Device Management, page 4-1.</td>
</tr>
<tr>
<td>Description</td>
<td>Alert category, one of the following: Application, Connectivity, Environment, Interface, Other, Reachability, System Hardware, Utilization. For alerts containing multiple events, the tabular display shows the category of the event with the most recent change. For alerts containing multiple events, the display shows the category of the event with the most recent change.</td>
</tr>
</tbody>
</table>
Understanding the Fault History: Events Display

The Fault History: Events display is shown in Figure 6-2. This display is generated as described in these sections:

- Generating a 24-Hour Report on All Events on a Device Component, page 6-5
- Getting All Stored Fault History on an Event, page 6-9

The tabular display is a scrollable table that lists up to 2,000 records, based on your filtering criteria. If you want to view database contents beyond the 2,000 records, click the Export tool button in the upper-right corner.

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Critical, Warning, or Informational.</td>
</tr>
<tr>
<td>Time</td>
<td>Date and time when the alert was generated.</td>
</tr>
</tbody>
</table>
| Status    | Alert status, based on last polling. Clicking this link opens the alert annotation page, which contains user annotations associated with the alert.  

- Active: Alert is live.  
- Cleared: Alert is no longer live. Also, when a device is suspended, all alerts are cleared. When DFM polling determines that the alarm has been in the Cleared state for 30 minutes or more (from the time of polling), the alarm expires and is removed from the Alerts and Activities display.  
- Acknowledged: Alert was manually recognized by a user (from Alerts and Activities Detail display).
Understanding the Fault History: Events Display

Figure 6-2  Fault History: Events Display

The Fault History: Events display provides two tools, described in Table 6-3.

Table 6-3  Fault History: Events Display—Window Tools

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Described in...</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Toolbar Icon]</td>
<td>Exports the current tabular display to a PDF file.</td>
<td>Exporting Data from Tabular Displays, page 2-6</td>
</tr>
<tr>
<td>![Printer Icon]</td>
<td>Opens a printer-friendly version for printing.</td>
<td>Printing Tabular Displays, page 2-7</td>
</tr>
</tbody>
</table>

Table 6-4 describes the contents of the Fault History: Events tabular display.

Table 6-4  Fault History: Events Tabular Display—Contents

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event ID</td>
<td>Event identifier number. Clicking this link opens the event properties page, which describes the value of MIB attributes at the time of the event.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Device name or IP address. (If the DFM server is using Access Control Server (ACS) mode, ACS may limit the devices you are permitted to view and for which you can create Fault History displays. (For more information, refer to Device-Based Filtering, page 11-11.)</td>
</tr>
<tr>
<td>Component</td>
<td>Device element on which the event occurred.</td>
</tr>
</tbody>
</table>
**Understanding the Fault History: Events Display**

**Table 6-4  Fault History: Events Tabular Display—Contents (continued)**

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>DFM event name (as described in <em>Events Processed, page D-1</em>). You can also customize the names of events displayed by Fault History (and the Alerts and Activities display) using the Notification Customization feature in Notification Services. For more information, refer to <em>Customizing the Names of DFM Events, page 5-5</em>.</td>
</tr>
<tr>
<td><strong>Time</strong></td>
<td>Date and time when the event was generated.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Event status, based on last polling.</td>
</tr>
<tr>
<td></td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td>Cleared</td>
</tr>
<tr>
<td></td>
<td>Suspended</td>
</tr>
<tr>
<td></td>
<td>Resumed</td>
</tr>
<tr>
<td></td>
<td>Deleted</td>
</tr>
<tr>
<td><strong>Alert ID</strong></td>
<td>Alert identifier number associated with this event.</td>
</tr>
</tbody>
</table>
PART 2

Configuring and Administering DFM
CHAPTER 7

User Guide for Device Fault Manager

78-16266-01

Configuring and Administering DFM (Basic)

These topics provide an introduction and overview of Device Fault Manager (DFM) basic configuration and administration tasks:

- Using DFM Configuration, page 7-2
- Applying Changes, page 7-4
- Performing Scheduling Tasks, page 7-5
- Configuring SNMP Trap Receiving and Forwarding, page 7-10
- Configuring a Default SMTP Server, page 7-15

Advanced configuration and administration tasks are addressed in Administering DFM (Advanced), page 11-1.
Using DFM Configuration

When you select **Configuration** from the DFM home page, DFM displays several choices.

**Note**
Your login determines which applications and folders are displayed to you. See **Understanding Your User Role, page 2-12.**

Table 7-1 lists the choices, shows where you can find the instructions and procedures for using each, and provides a brief description of what you can accomplish using the application.

**Table 7-1 Configuration Folder Options**

<table>
<thead>
<tr>
<th>Choices in the Configuration Folder</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling and Thresholds:</td>
<td>Contains all options for controlling polling and threshold settings.</td>
</tr>
<tr>
<td>See Configuring Polling and Thresholds, page 10-1.</td>
<td></td>
</tr>
<tr>
<td>Polling Parameters</td>
<td>Change polling intervals, timeouts, and retries by device group</td>
</tr>
<tr>
<td>Managing Thresholds</td>
<td>Change thresholds, resetting the limits against which polled data will be compared</td>
</tr>
<tr>
<td>Setting Priorities</td>
<td>Reprioritize customizable groups for polling and thresholds</td>
</tr>
<tr>
<td>Apply Changes</td>
<td>Apply your Polling and Threshold changes</td>
</tr>
<tr>
<td></td>
<td>• Start using updated polling parameters and threshold values</td>
</tr>
<tr>
<td></td>
<td>• Resume polling for devices or device elements that were previously suspended</td>
</tr>
</tbody>
</table>
### Table 7-1  Configuration Folder Options (continued)

<table>
<thead>
<tr>
<th>Choices in the Configuration Folder</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Other Configurations</strong></td>
<td>Contains all other DFM system configuration choices.</td>
</tr>
<tr>
<td><strong>Rediscovery Schedule</strong></td>
<td>Add, edit, suspend, resume, and delete rediscovery schedules.</td>
</tr>
<tr>
<td>See Configuring Rediscovery Schedules, page 7-7.</td>
<td></td>
</tr>
<tr>
<td><strong>Group Config</strong></td>
<td>View the rules that govern system-defined device groups.</td>
</tr>
<tr>
<td>See Managing Groups, page 8-1.</td>
<td>Maintain customizable polling and threshold groups.</td>
</tr>
<tr>
<td></td>
<td>Create and maintain user-defined device groups.</td>
</tr>
<tr>
<td><strong>Daily Purging Schedule</strong></td>
<td>Change the time at which to start purging the Fault History database.</td>
</tr>
<tr>
<td><strong>Alerts and Activities Defaults</strong></td>
<td>Create views.</td>
</tr>
<tr>
<td>See Configuring Views for the Alerts and Activities Display, page 9-1.</td>
<td></td>
</tr>
<tr>
<td><strong>Logging</strong></td>
<td>Change the level of messages written to log files.</td>
</tr>
<tr>
<td>See Configuring Logging, page 11-17.</td>
<td></td>
</tr>
<tr>
<td><strong>SNMP Trap Forwarding</strong></td>
<td>Change the port on which DFM listens for SNMP traps.</td>
</tr>
<tr>
<td>See Configuring SNMP Trap Forwarding, page 7-14.</td>
<td></td>
</tr>
<tr>
<td><strong>SNMP Trap Receiving</strong></td>
<td>Set a host and port number as a recipient for pass-through traps.</td>
</tr>
<tr>
<td>See Updating the SNMP Trap Receiving Port, page 7-14.</td>
<td></td>
</tr>
<tr>
<td><strong>Default SMTP Server</strong></td>
<td>Change or enter a default server to use for e-mail notifications.</td>
</tr>
<tr>
<td>See Configuring a Default SMTP Server, page 7-15.</td>
<td></td>
</tr>
</tbody>
</table>
Applying Changes

**Note**

Your login determines whether you can perform this operation.

Changes to polling parameters and threshold values do not take effect until you apply changes, thereby reconfiguring DFM to use the new values. Similarly, after you resume devices or device components that were suspended from polling, you must apply changes for the device elements to be polled.

**Before You Begin**

Applying changes is a CPU-intensive event that may take between one and five minutes to complete. Therefore, to minimize system impact, consider doing the following when possible:

- Consolidating changes to polling parameters and threshold values, thereby limiting the number of times you will need to apply them.
- Applying changes during a low-usage time.

**Step 1**

From the DFM home page, select **Configuration > Apply Changes**. The Apply Changes page appears.

**Step 2**

Click **Yes** to apply the changes:

- If another user has already initiated applying changes, a message is displayed and changes are not applied again.
- If, since the last time changes were applied, polling parameter settings or threshold values have not changed and devices have not been suspended and then resumed, changes will not be applied.

**Tip**

You cannot directly verify that changes have been applied. However, you can do so indirectly. For example, in response to an event, you change a threshold value and apply changes. After DFM finishes applying changes, you can see whether DFM clears the event.
Performing Scheduling Tasks

When DFM is first installed, most tasks listed in Table 7-2 are scheduled by default to ensure that they do not run concurrently. You can configure the schedules for these tasks to meet the requirements of your site. However, you should still avoid running them concurrently.

Table 7-2 Scheduling Considerations

<table>
<thead>
<tr>
<th>Configuration Task</th>
<th>Default Schedule</th>
<th>Comments and Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database purging</td>
<td>Run daily at midnight.</td>
<td>The amount of time it takes to purge the database depends on the size of the database.</td>
</tr>
<tr>
<td>Rediscovery</td>
<td>Run weekly on Monday at 2:00 a.m.</td>
<td>By default, rediscovery starts 2 hours after database purging.</td>
</tr>
</tbody>
</table>

In addition to configuring schedules with DFM, a system administrator can schedule database backups. You should be careful to coordinate the database backup schedule to avoid running concurrently with the tasks listed in Table 7-2.

For more information about schedules, see the following topics:

- Configuring the Daily Purging Schedule, page 7-6
- Configuring Rediscovery Schedules, page 7-7
Configuring the Daily Purging Schedule

Note
Your login determines whether or not you can perform this task. See Understanding Your User Role, page 2-12.

Data for Fault History remains in the DFM database for 31 days. Purging occurs every day to maintain only 31 days of data. You can select the time of day that purging begins. By default, purging begins at 00:00.

Before You Begin
Review the information in Performing Scheduling Tasks, page 7-5 to ensure that daily purging does not conflict with the other scheduled jobs listed there.

Note
Do not use the Common Services Job Browser to manage Rediscovery Schedules; use the DFM Daily Purging Schedule interface. If you suspend the DFM:DataPurge job using the Job Manager, the job is deleted from the DFM Daily Purging Schedule interface, which can be confusing to users.

Step 1
From the DFM home page, select Configuration > Other Configurations > Daily Purging Schedule.

Step 2
Select the Purge Time:
- Hour—From 0 to 23
- Minute—From 0 to 50 in ten-minute intervals

The default purge time is 00:00.

Step 3
Click the Apply button.

Tip
You can check the status of the DFM data purge job from the Job Manager page each day after the job runs. To do so, from the CiscoWorks home page select Common Services > Server > Administration > Job Browser and find DFM:DataPurge under Job Type.
For more information, see the following topics:

- Performing Scheduling Tasks, page 7-5
- Configuring Rediscovery Schedules, page 7-7

**Configuring Rediscovery Schedules**

**Note**  
Your login determines whether or not you can perform this task. See Understanding Your User Role, page 2-12.

DFM rediscovery probes the devices to discover their configuration and verify their manageable elements in inventory.

DFM contains a default discovery schedule that starts rediscovery on a weekly basis. Although you cannot modify the default discovery schedule, you can suspend it and add, modify, or delete additional schedules.

**Suspending a Rediscovery Schedule**

DFM includes a default rediscovery schedule, Default_Schedule. You cannot edit or delete Default_Schedule, but you can suspend it. To completely suspend rediscovery for a period of time, you may have to repeat this procedure to suspend more than one schedule.

**Step 1**  
From the DFM home page, select Configuration > Other Configurations > Rediscovery Schedule.

**Step 2**  
From the Rediscovery Schedule page, select a schedule that does not show Suspended as its status, and click the Suspend button.

**Step 3**  
The status for the schedule changes to Suspended and the schedule does not execute again until you resume the schedule. The schedule remains listed on the Rediscovery Schedule page until you delete it.
Performing Scheduling Tasks

Resuming a Rediscovery Schedule

Step 1 From the DFM home page, select Configuration > Other Configurations > Rediscovery Schedule.

Step 2 From the Rediscovery page, select a schedule with a status of Suspended and click the Resume button.

Step 3 The status for the schedule changes to Scheduled.

Adding a Rediscovery Schedule

Before You Begin
See Performing Scheduling Tasks, page 7-5 to plan the rediscovery schedule for maximum efficiency and minimum system impact.

Step 1 From the DFM home page, select Configuration > Other Configurations > Rediscovery Schedule and click the Add button.

Step 2 Enter a name for the schedule.

Step 3 By default, Weekly is selected for Execute. Select how often the schedule should execute from the following choices:
- Once
- Daily
- Weekly
- Monthly

Step 4 Select the date, hour, and minute on which to start the rediscovery schedule and click Next.

Step 5 Review the information on the Schedule Summary: Add page and click Finish. The Rediscovery Schedule page appears, listing the new schedule.
Editing a Rediscovery Schedule

Before You Begin
See Performing Scheduling Tasks, page 7-5 to plan the rediscovery schedule for maximum efficiency and minimum system impact.

Step 1 From the DFM home page, select Configuration > Other Configurations > Rediscovery Schedule.

Step 2 Select a rediscovery schedule with a status of Scheduled and click the Edit button.

Note You cannot edit Default_Schedule.

Step 3 You can modify how often the schedule executes and when the schedule starts:

a. If desired, select among the available choices for how often the schedule should execute:

b. If desired, select a different date, hour, and minute on which to start rediscovery.

Step 4 Click Next.

Step 5 Review the information on the Schedule Summary: Edit page and click Finish. The Rediscovery Schedule page appears, listing the modified schedule.
Deleting a Rediscovery Schedule

**Step 1**  From the DFM home page, select **Configuration > Other Configurations > Rediscovery Schedule**.

**Step 2**  Select a rediscovery schedule and click the **Delete** button. A confirmation dialog box appears.

**Note**  You cannot delete Default_Schedule.

**Step 3**  Click **Yes**. (Note that the job is removed from this page but will continue to be listed in the Common Services Job Browser.)

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 you must do one of the following:

- Configure SNMP to send traps directly to DFM
- Integrate SNMP trap receiving with an NMS or a trap daemon

To send traps directly to DFM, perform the tasks in **Enabling Devices to Send Traps to DFM, page 7-11**. To integrate SNMP trap receiving with an NMS or a trap daemon, follow the instructions in **Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs, page 7-12**.

The versions of SNMP traps supported by DFM are described in **SNMP and ICMP Polling, page E-1**.
Enabling Devices to Send Traps to DFM

If your devices send SNMP traps to a Network Management System (NMS) or a trap daemon, see Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs, page 7-12.

Because DFM uses SNMP MIB variables and traps to determine device health, you must configure your 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 7-11
- Enabling Catalyst Devices to Send SNMP Traps to DFM, page 7-12

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, refer to the appropriate command reference guide.

Step 1  Log in to Cisco.com.
Step 2  Select Products & Services > Cisco IOS Software.
Step 3  Select the Cisco IOS software release version used by your 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:

```
(en) # set snmp community read-only [community string]
(en) # set snmp trap enable all
(en) # 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, refer to the appropriate command reference guide.

---

**Step 1**
Log in to Cisco.com.

**Step 2**
Select **Products & Services > Cisco Switches**.

**Step 3**
Select the appropriate Cisco Catalyst series switch.

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

---

Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs

You might need to complete one or more of the following steps to integrate SNMP trap receiving with other trap daemons and other Network Management Systems (NMSs):

- If you are integrating DFM with a remote version of HP OpenView or NetView, you must install the appropriate adapter on the remote HP OpenView or NetView (refer to *Installation and Setup Guide for Device Fault Manager*, which also provides information on supported versions). You do not need to install any adapters if HP OpenView or NetView is installed locally.

- 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 7-11. 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 7-14.

- If your network devices are already sending traps to another management application, configure that application to forward traps to DFM.

Table 7-3 describes scenarios for SNMP trap receiving and lists the advantages of each.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network devices send traps to port 162 of the host where DFM is running. DFM receives the traps and forwards them to the NMS.</td>
<td>• No reconfiguration of the NMS is required.</td>
</tr>
<tr>
<td></td>
<td>• No reconfiguration of network devices is required.</td>
</tr>
<tr>
<td></td>
<td>• DFM provides a reliable trap reception and forwarding mechanism.</td>
</tr>
<tr>
<td></td>
<td>• NMS continues to receive traps on port 162.</td>
</tr>
<tr>
<td></td>
<td>• Network devices continue to send traps to port 162.</td>
</tr>
<tr>
<td>The NMS receives traps on default port 162 and forwards them to port 162 on the host where DFM is running.</td>
<td>• No reconfiguration of the NMS is required.</td>
</tr>
<tr>
<td></td>
<td>• No reconfiguration of network devices is required.</td>
</tr>
<tr>
<td></td>
<td>• DFM does not receive traps dropped by the NMS.</td>
</tr>
</tbody>
</table>
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. DFM supports SNMP V1, V2, and V3 traps for trap receiving (although DFM only supports authentication/no privacy and no authentication/no privacy for V3 traps).

**Step 1**
From the DFM home page, select **Configuration > 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 are already in use, see *Ports and Protocols that DFM Uses*, page 11-1.

Configuring SNMP Trap Forwarding

**Note**
Your login determines whether or not you can perform this task. See *Understanding Your User Role*, page 2-12.

By default, DFM does not forward unprocessed (pass-through) SNMP traps. However, you can configure it to do so. All traps are forwarded in V1 format.

**Step 1**
From the DFM home page, select **Configuration > 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.
Configuring a Default SMTP Server

Note
Your login determines whether or not you can perform this task.

This SMTP server is used by default when you add or edit subscriptions for e-mail notifications or send e-mail notifications from the Alerts and Activities display. Common Services also provides a facility for specifying a default SMTP server. Specifying a default server here will override the setting used by Common Services.

Step 1  From the DFM home page, select Configuration > Other Configurations > Default SMTP Server.
Step 2  Enter a fully qualified SMTP server name.
Step 3  Click OK.
Managing Groups

These topics describe the process for configuring Device Fault Manager (DFM) groups:

- Understanding DFM Groups, page 8-1
- Using Group Management, page 8-9
- Viewing Group Details, page 8-27
- Viewing Membership Details, page 8-29
- Refreshing Membership, page 8-30
- Deleting Groups, page 8-31

Understanding DFM Groups

DFM groups are created by DFM, and consist of interface, trunk port, and access port groups. Each group has a set of properties (such as a name, description, permission, etc.), and are defined by the group’s associated rules.

What you see in the DFM group selector depends on the function you are using. Normally when you view the DFM group selector, some groups are displayed under DFM and other groups under Common Services, as shown in Figure 8-1 on page 8-2.
Common Services groups are created by Common Services when devices are added to the DCR. These are device groups. The group to which a device belongs is determined by Common Services group rules. Common Services groups include objects such as routers, switches, and hubs. All Common Services groups are shared with DFM—in other words, they are shown in the DFM user interface. Groups are only shown when they have members.

DFM groups are created by DFM. These are interface, access port, and trunk port groups. The group to which a port or interface belongs is determined by DFM group rules. (DFM also provides some device groups, as explained later in this topic.)

Figure 8-1 shows the object selector, with some groups under Common Services and others under DFM.

![Group Selector Showing Common Services and DFM Groups](image)
As shown in Figure 8-2, the following types of groups are supported:

- **System Defined Groups**—The factory default groups in CiscoWorks. Common Services system defined groups consist of devices; DFM system defined groups consist of access ports, trunk ports, and interfaces.

  You cannot delete a system defined group, nor can you modify the rules that determine the members of system defined groups.

  For a description of each DFM and Common Services system defined group, see Working with System Defined Groups, page 8-4.

- **User Defined Groups**—Groups that you edit or create to reflect the way you manage the network. You can edit or create user defined groups for DFM and determine whether they can be viewed by other CiscoWorks users. User defined groups include the following:

  - **Customizable groups**—Predefined groups that you can modify for your own purposes. DFM provides the four types of customizable groups: access port groups, trunk port groups, interface groups, and device groups. For a detailed description of customizable groups, see Working with Customizable Groups, page 8-7.

  - Miscellaneous groups (to use with views in the Alerts and Activities display, or with notification groups in Notification Services). These are the only groups you can create. These appear in the Group Selector under User Defined Groups so you can view the group membership (device groups are created when the devices are added to the DFM inventory).
Groups and ACS

The CiscoWorks Access Control Server (ACS) provides device-based filtering for many of the DFM user interfaces that use Group Administration. For more information on ACS, refer to Device-Based Filtering, page 11-11.

Working with System Defined Groups

The group selector displays some groups under DFM and other groups under Common Services. The Common Services groups are created by Common Services and are visible when devices are added to the DCR. These groups include groups such as Routers, Switches and Hubs, and IP Telephony. Refer to Common Services System Defined Groups, page 8-4 for more information.

The DFM groups are created by DFM. These groups include Access Port Groups, Trunk Port Groups, and Interface Groups. Refer to DFM System Defined Groups, page 8-6 for more information.

You can control the polling and thresholds settings for these groups using Configuration > Polling and Thresholds. Refer to Configuring Polling and Thresholds, page 10-1.

Common Services System Defined Groups

The Common Services system defined groups, as shown in Figure 8-3, are visible to all CiscoWorks users, and are the factory default groups administered by Common Services. Not all system defined groups are shown in Figure 8-3 because groups only appear in the group selector when they have device members (in other words, devices in the DCR that belong to that group).
The following are the Common Services system defined groups:

- Broadband Cable
- Content Networking
- DSL and LRE
- Interfaces and Modules
- Network Management
- Optical
- Routers
- Security and VPN
- Storage Networking
- Switches and Hubs
- Universal Gateways and Access Servers
- Unknown
- Voice and Telephony
- Wireless

For more information about Common Services system defined groups, refer to the Common Services online help.
DFM System Defined Groups

The DFM system defined groups, as shown in Figure 8-4, are visible to all CiscoWorks users, and are the factory default groups that are administered by DFM.

Figure 8-4  Group Selector Showing DFM System Defined Groups

The following are the DFM system defined groups:

- **System defined access port groups:**
  - 1 GB Ethernet
  - 10MB-100MB Ethernet
  - ATM
  - Others

- **System defined interface groups:**
  - 1 GB Ethernet
  - 10MB-100MB Ethernet
  - ATM
  - Backup
  - Dial-on-Demand
  - FDDI
  - ISDN B channel
  - ISDN D channel
  - ISDN physical interface
- Others
- Serial
- Token Ring

- System defined trunk port groups:
  - 1 GB Ethernet
  - 10MB-100MB Ethernet
  - ATM
  - Others

**Working with Customizable Groups**

Because you cannot change the rules for system defined groups, DFM provides customizable groups that can contain the devices, ports, or interfaces in which you are interested. Port and interface containment is only seen and used by Polling and Thresholds (refer to Configuring Polling and Thresholds, page 10-1), but device groups will contain members when devices are added to the DFM inventory. Once you edit or create a group, you can determine whether other CiscoWorks users can view the group.

*Figure 8-5  Group Selector Showing DFM Customizable Groups*
For each of the parent groups listed in Table 8-1, DFM provides seven configurable subgroups. Table 8-2 describes the restrictions placed on the subgroups.

**Table 8-1 DFM Customizable Groups**

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Use this group to monitor...</th>
<th>Settings you can configure for this group:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizable Access Port</td>
<td>Access ports</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Groups</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customizable Groups</td>
<td>Devices</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Customizable Interface</td>
<td>Interfaces</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Groups</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customizable Trunk Ports</td>
<td>Trunk ports</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Groups</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 8-2 Customizable Groups—Restrictions**

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizable Group A</td>
<td>• Use to troubleshoot a single device (but can contain more than one device)</td>
</tr>
<tr>
<td>Customizable Group B</td>
<td>• Cannot be deleted</td>
</tr>
<tr>
<td>Customizable Group C</td>
<td>• Cannot have subgroups</td>
</tr>
<tr>
<td></td>
<td>• Cannot have name changed</td>
</tr>
<tr>
<td>Customizable Group 1</td>
<td>• Can contain multiple devices</td>
</tr>
<tr>
<td>Customizable Group 2</td>
<td>• Cannot be deleted</td>
</tr>
<tr>
<td>Customizable Group 3</td>
<td>• Cannot have subgroups</td>
</tr>
<tr>
<td>Customizable Group 4</td>
<td>• Cannot have name changed</td>
</tr>
</tbody>
</table>
Using Group Management

The Group Administration and Configuration page is where all group management activities take place. To open the Group Administration and Configuration page, from the DFM home page, select Configuration > Other Configurations > Group Administration.

Note: If you are connecting to the DFM server for the first time, a Security Alert window is displayed after you select nearly any option. Do not proceed without viewing and installing the security certificate. For more information, see Responding to Security Alerts, page 2-12.

See Editing and Creating Groups, page 8-11 for information on how to use Group Administration to create and edit groups. In addition to creating and editing groups, Group Management provides the following functions:

- Refreshing Membership, page 8-30
- Deleting Groups, page 8-31

Figure 8-6 shows an example of the Group Administration and Configuration page.
Table 8-3 describes the fields in the Group Administration and Configuration page.

**Table 8-3  Fields on Group Administration and Configuration Page**

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Selector</td>
<td>A hierarchical display of all available groups.</td>
</tr>
</tbody>
</table>
| Group Info | When you select an item from the Group Selector, the Group Info pane displays the following information:  
  * Group Name—The name of the group you selected.  
  * Type—The type of objects in the selected group.  
  * Description—A text description of the group.  
  * Created By—The person who created the group.  
  * Last Modified By—The last person to modify the group settings. |
| Create | Starts the Group Creation Wizard for creating a group, as described in Editing a Group, page 8-12. |
| Edit | Starts the Group Edit Wizard for editing user defined groups, as described in Editing a Group, page 8-12. (Not supported for view groups created from the Alerts and Activities Defaults page.) |
| Details | Opens the Properties: Details page, as described in Viewing Group Details, page 8-27. |
| Refresh | Refreshes a group’s membership, as described in Refreshing Membership, page 8-30. Not supported for port and interface groups. |
| Delete | Deletes a group, as described in Deleting Groups, page 8-31. |
Editing and Creating Groups

The processes for editing and creating groups are similar. Keep these points in mind:

- You can edit user defined customizable subgroups, for example, the subgroup *Customizable Group 1* under Customizable Access Port Groups. These subgroups are listed in *Working with Customizable Groups, page 8-7*.
- You can create or edit user defined miscellaneous groups (to use with, for example, views in the Alerts and Activities display, or with notification groups in Notification Services). For example, you could create a group called *test*, which would appear directly under DFM User Defined Groups in the DFM group selector. (You cannot edit view groups created from the Alerts and Activities Defaults page.)

DFM uses the Group Creation Wizard to guide you through the steps required to create or edit a group. The wizard consist of four steps:

1. Setting properties (for details, see *Editing a Group, page 8-12* and “Editing a Group” section on page 8-12).
2. Creating rules (for details, see *Understanding Rules, page 8-20*).
3. Modifying group membership (for details, see *Finalizing Group Membership, page 8-26*).
4. Viewing the summary (for details, see *Viewing the Group Summary, page 8-26*).
Editing a Group

You can edit the properties of user defined customizable port, interface, and device groups. You can also edit miscellaneous user defined groups you created using Group Administration. (However, you cannot edit view groups you created using the Alerts and Activities Defaults page.)

**Step 1**
From the DFM home page, select **Configuration > Other Configurations > Group Administration**. The Group Administration and Configuration page appears.

**Note**
If you are connecting to the DFM server for the first time, a Security Alert window is displayed after you select nearly any option. Do not proceed without viewing and installing the security certificate. For more information, see **Responding to Security Alerts**, page 2-12.

**Step 2**
In the Group Selector, select the group you want to edit.

**Step 3**
Click **Edit**. The Properties: Edit page appears, as shown in Figure 8-7.

![Figure 8-7 Properties: Edit Page](image-url)
Step 4  You can modify the following in the Properties: Edit page:

- Group Name (will be automatically populated when editing customizable subgroups; for example, Customizable Group 1 under Customizable Access Port Groups)
- Description
- Membership update type (not supported for port and interface groups)

\[\text{Note} \quad \text{The parent group is displayed, but it cannot be modified.}\]

- Visibility Scope

Step 5  Click Next. The Rules: Edit page appears. For more information on creating rules, see Understanding Rules, page 8-20.

\[\text{Note} \quad \text{If you need to return to any of the previous pages in the wizard, click Back.}\]

Step 6  You can add new rules or delete existing rules in the Rules: Edit page.

\textbf{To add a new rule:}

\begin{enumerate}
  \item From the first list, select a logical operator (applicable when there are multiple rule expressions).

  \[\text{Note} \quad \text{The list of logical operators is enabled after at least one rule expression is entered.}\]

  \item From the Object Type list, select an object type.

  \[\text{Note} \quad \text{All object types contain the prefix :DFM:VASA:DFMObject, which sets the domain for the rule. Meaningful object information follows the prefix.}\]

  \item From the Variable list, select a variable.
  \item From the Operator list, select an operator.
  \item In the Value field, enter a value.
\end{enumerate}
f. Click **Add Rule Expression**. The rule expression appears in the Rule Text box.

![Note]
You can manually add or change any of the text in the Rule Text box. If you enter a single backslash (\), an error is displayed. To enter a single backslash in the Rule Text box, you must type two backslashes (\\) in place of the single backslash. You should always check the syntax after changing a rule expression.

g. If you have added complex rules (containing both AND and OR conditions), you must manually enter parentheses, as in the following example:

```
```

h. To verify that the syntax of the rule is correct, click **Check Syntax**. A dialog box appears, stating that the syntax is valid. Click **OK**.

i. If you want to view the rules for the parent group, select **View Parent Rules**.

![Note]
All rules assigned to a parent group also apply to any of its subgroups.

j. Click **Next**. The Membership: Edit page appears.

**To delete a rule:**

a. In the Rule Text box, select the entire rule text and press the **Delete** key.

After deleting the rule, you must click the page so that the page can refresh, removing the list of logical operators.

b. Click **Next**. The Membership: Edit page appears.
Step 7  You can add or remove specific objects from the group membership (not supported for port and interface groups).

**Note**  The group’s rule captures the list of objects that are added to or deleted from the group. The rule will contain an Includelist and/or Excludelist section to reflect this.

Although it is acceptable for a rule to have more than one Includelist or Excludelist, the recommended practice is to consolidate them, forming one Includelist and one Excludelist. Check for duplicates across both lists and ensure that no device is both included and excluded.

**To add an object:**

a. In the Available Objects from Parent Group column, select the device to add.

b. Click **Add**.

**To remove an object:**

a. In the Objects Matching Membership Criteria column, select the device to remove.

b. Click **Remove**.

Step 8  Click **Next**. The group’s information appears in the Summary: Edit page.

Step 9  Click **Finish**. A dialog box appears, stating that changes to the group have been saved. Click **OK**.
Creating a Group

Creating groups is only supported for user defined miscellaneous groups. Once created, you can edit these groups.

Step 1  From the DFM home page, select Configuration > Other Configurations > Group Administration. The Group Administration and Configuration page appears.

Note  If you are connecting to the DFM server for the first time, a Security Alert window is displayed after you select nearly any option. Do not proceed without viewing and installing the security certificate. For more information, see Responding to Security Alerts, page 2-12.

Step 2  In the Group Selector, select User Defined Groups.

Step 3  Click Create. The Properties: Create page appears, as shown in Figure 8-8.

Figure 8-8 Properties: Edit Page

Step 4  Enter a group name for the new group.
Step 5  If you do not want to copy the attributes of an existing group to your new group, proceed to Step 6. If you want to copy the attributes of an existing group to the new group, do the following:

**Note**  All attributes except the group name are copied to the new group.

a. Click Select Group. The Replicate Attributes page appears.
b. Select the group from which you want to copy the attributes.
c. Click OK.

Step 6  If you want to change the parent group (the location where the group will reside in the Group Selector), do the following:

a. Click Change Parent. The Select Parent page appears.
b. Select the parent group.
c. Click OK.

Step 7  (Optional) Enter a description.

Step 8  Choose how you want the group membership updated (this choice is not displayed for port and interface groups):

- If you want the membership for this group updated automatically, select Automatic.
- If you want the membership for this group updated only when the Refresh button is clicked, select Only upon user request.

Step 9  Select a Visibility Scope:

- Available to Created User Only
- Available to All CiscoWorks Users
Step 10  Click Next. The Rules: Create page appears. (For more information on creating rules, see Understanding Rules, page 8-20.)

Do one of the following:

- To create rules to apply to the group, go to Step 11.
- Click Next and select the objects on the Membership: Create page (not supported for port and interface groups). Then go to Step 12.

Note  If you need to return to any of the previous pages in the wizard, click Back.

Step 11  Create all rules that you want to apply to the group:

a. Select a logical operator (applicable when there are multiple rule expressions).

Note  The list of logical operators is enabled after at least one rule expression is entered.

b. Select an object type.

Note  All object types contain the prefix :DFM:VASA:DFMObject, which sets the domain for the rule. Meaningful object information follows the prefix.

c. Select a variable.

d. Select an operator.

e. In the Value field, enter a value.
f. Click **Add Rule Expression**. The rule expression appears in the Rule Text box.

   ![Note](image)
   You can manually add or change any of the text in the Rule Text box. If you enter a single backslash (\), an error is displayed. To enter a single backslash in the Rule Text box, you must type two backslashes (\\) in place of the single backslash. You should always check the syntax after changing a rule expression.

   g. If you have added complex rules (containing both AND and OR conditions), you must manually enter parentheses, as in the following example:

   ```
   (:DFM:VASA:DFMObject:AccessPort.Mode equals "" OR :
   :DFM:VASA:DFMObject:AccessPort.Mode contains "BACKUP" OR :
   (:DFM:VASA:DFMObject:AccessPort.DuplexMode contains "HALFDUPLEX" OR :
   ```

   h. To verify that the rule syntax is correct, click **Check Syntax**. A dialog box appears, stating the syntax is valid. Click **OK**.

   i. If you want to view the rules for the parent group, select **View Parent Rules**.

   ![Note](image)
   All rules assigned to a parent group also apply to any of its subgroups.

   j. Click **Next**. The Membership: Create page appears.

   **Step 12**
   You can add or remove specific objects from the group membership (not supported for port and interface groups).

   ![Note](image)
   The group’s rule captures the list of objects that are added to or deleted from the group. The rule will contain an Includelist and/or Excludelist section to reflect this.

   Although it is acceptable for a rule to have more than one Includelist or Excludelist, the recommended practice is to consolidate them, forming one Includelist and one Excludelist. Check for duplicates across both lists and ensure that no object is both included and excluded.
To add an object:
   a. In the Available Objects from Parent Group column, select the devices to add.
   b. Click Add.

To delete an object:
   a. In the Objects Matching Membership Criteria column, select the devices to remove.
   b. Click Remove.

Step 13  Click Next. The group’s information appears in the Summary: Create page.

Step 14  Click Finish. A dialog box appears, stating that changes to the group have been saved. Click OK.

Understanding Rules

Every group is defined by a set of rules. A rule set contains a Boolean combination of individual rule expressions.

Rules are created to filter in the objects that you want to belong to the group, and to filter out those that you do not want in the group. When determining which objects belong to a group, Group Management compares object information to the rule. If an object’s information satisfies all of the rule’s requirements, it is placed in the group.

One or more rule expressions can be applied to form a rule. Each rule expression contains the following:

<Object Type>.<Variable> <Operator> <Value>

For example:

:DFM:VASA:DFMObject:Device:Routers.Location equals "San Jose"
Complex rules that contain both OR and AND conditions require you to edit the rule manually. For example, all parentheses in the following rule must be added in the Rule Text field:

\[
\]

Rules are defined through the Group Creation Wizard on the Rules: Create and Rules: Edit pages. You can define the Object Type, Variable, Operator, and Value. For multiple rules, you can also define the Logical Operator.

**Logical Operators**

The logical operator field appears when you are defining multiple rules, which can be the following:

- **OR**—Include devices that fulfill the requirements of either rule.
  
  For interface, access port, and trunk port groups, this operator can only be used between the variables of the *same* type, as in the following valid rule:
  

  If you used an AND operator in the previous port rule, it would be invalid.

- **AND**—Include only objects that fulfill the requirements of both rules.

  For interface, access port, and trunk port groups, this operator can only be used between the variables of *different* types, as in the following example:


  If you used an OR operator in the previous rule, it would be invalid.

  For device groups, this operator can only be used between variables of the *same* type, as in the following example:

The following would be an invalid rule for a device group:

:\DFM:VASA:DFMOBJ:Device:Routers.Model equals "12816" AND
:\DFM:VASA:DFMOBJ:Device:SwitchesAndHubs.Type equals "6509"

In the previous example, you would have to use the OR operator.

- EXCLUDE—Do not include these devices.

Object Type

The Object Type field lists the available objects that you can use to form a group. All rule expressions begin with the same object type, :DFM:VASA:DFMOBJ, which sets the domain for the rule, and is at the top of the hierarchy.

In the Object Type field you will see the following choices:

:\DFM:VASA:DFMOBJ:AccessPort
:\DFM:VASA:DFMOBJ:TrunkPort
:\DFM:VASA:DFMOBJ:Interface
:\DFM:VASA:DFMOBJ:Device:Cable
:\DFM:VASA:DFMOBJ:Device:ContentNetworking
:\DFM:VASA:DFMOBJ:Device:InterfacesAndModules
:\DFM:VASA:DFMOBJ:Device:NetworkManagement
:\DFM:VASA:DFMOBJ:Device:Optical
:\DFM:VASA:DFMOBJ:Device:Routers
:\DFM:VASA:DFMOBJ:Device:SecurityAndVPN
:\DFM:VASA:DFMOBJ:Device:StorageNetworking
:\DFM:VASA:DFMOBJ:Device:SwitchesAndHubs
:\DFM:VASA:DFMOBJ:Device:UniversalGatewaysAndAccessServers
:\DFM:VASA:DFMOBJ:Device:VoiceAndTelephony
:\DFM:VASA:DFMOBJ:Device:Wireless
:\DFM:VASA:DFMOBJ:DSLAndLRE
:\DFM:VASA:DFMOBJ:Group

Variable

The Variable field lists the possible attributes for the selected object type to be used for the rule. The list of possible variables changes based on the object type that is selected. Some variables for port and interface groups are described in Table 8-4 on page 8-23.
Operator

The Operator field defines the operator to be used in the rule. The list of possible operators changes based on the object type and the variable selected.

**Note**

When using the *equals* operator, the rule is case-sensitive.

Value

The Value field describes the value of the rule expression. The possible values depend upon the object type, variable, and operator selected. Depending on the operator selected, the value may be free-form text or a list of values.

Most of the values that can be entered in the Value field of the Rules: Edit page are self-evident, but some of the objects in the Variables field have special meanings or restrictions on how to enter the related attribute in the Value field. Table 8-4 describes the objects that appear in the Variable field of the Value field that might need further explanation.

**Table 8-4   Explanations for the Values of Special Variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>DuplexMode</td>
<td>Duplex mode (FULLDUPLEX, HALFDUPLEX, or UNSPECIFIED).</td>
</tr>
<tr>
<td>InterfaceCode</td>
<td>Interface types, protocols, or encapsulations.</td>
</tr>
<tr>
<td>MaxSpeed</td>
<td>Maximum speed, in bits per second.</td>
</tr>
<tr>
<td>MaxTransferSpeed</td>
<td>Speed of the largest datagram that can be sent or received, specified in octets. For interfaces that use transmitting network datagrams, speed of the largest network datagram that can be sent.</td>
</tr>
<tr>
<td>Mode</td>
<td>Intended purpose (for example, for interfaces, backup, dial-on-demand, and so forth).</td>
</tr>
<tr>
<td>Name</td>
<td>Name of object.</td>
</tr>
<tr>
<td>SystemModel</td>
<td>Name by which system is generally known.</td>
</tr>
<tr>
<td>SystemName</td>
<td>Name of system containing this element.</td>
</tr>
<tr>
<td>SystemObjectID</td>
<td>System Object Identifier associated with vendor of system.</td>
</tr>
</tbody>
</table>
Table 8-4  **Explanations for the Values of Special Variables (continued)**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SystemVendor</td>
<td>Name of system’s supplier.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of element (for example, interface), distinguished according to the</td>
</tr>
<tr>
<td></td>
<td>physical/link protocol(s) immediately below the network layer in the</td>
</tr>
<tr>
<td></td>
<td>protocol stack.</td>
</tr>
</tbody>
</table>

**Note**

After you have defined the rule, you should verify the syntax. You can do this on the Rules: Edit page.

**Figure 8-9** shows an example of the Rules: Edit page.

**Figure 8-9  Rules: Edit Page**

Table 8-5 describes the remaining fields on the Rules: Edit page of the Group Creation Wizard.
You want to create a group that contains all interfaces using full duplex mode in the Dallas location. Form the following rule:

:VASA::DFMObject::Interface::Duplex::Mode contains "FULLDUPLEX" AND Location contains "Dallas"

- **Object Type**—DFM:VASA::DFMObject::Interface
- **Variable**—Duplex::Mode
- **Operator**—Contains
- **Value**—“FULLDUPLEX”
- **Logical Operator**—And
- **Variable**—Location
- **Operator**—contains
- **Value**—“Dallas”

You want to create a group that contains all of the security and VPN devices in the San Jose location. Form the following rule:

:DFM::VASA::DFMObject::Device:SecurityAndVPN::Location contains "SanJose"

- **Object Type**—DFM:VASA::DFMObject::Device::SecurityAndVPN
- **Variable**—Location

---

**Table 8-5 Fields on the Rules: Edit Page**

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Rule Expression</td>
<td>Used to add the rule expression to the group rules.</td>
</tr>
<tr>
<td>Rule Text</td>
<td>Displays the rule. For complex rules (which contain both OR and AND conditions), you must manually add parentheses in this field. (In Editing a Group, page 8-12, see Step 11; in Editing a Group, page 8-12, see Step 6.)</td>
</tr>
<tr>
<td>Check Syntax</td>
<td>Verifies that the rule syntax is correct.</td>
</tr>
<tr>
<td>View Parent Rules</td>
<td>Used to view the parent group rules.</td>
</tr>
</tbody>
</table>

**Note** All parent group rules apply to the subgroups.
Using Group Management

- Operator—Contains
- Value—“San Jose”

To help you to better understand group rules, you may want to look at the rules used for system defined groups. These rules appear in the Properties: Details page. For a description of the Properties: Details page, see Viewing Group Details, page 8-27.

Finalizing Group Membership

After the group rules have been defined, they are evaluated, and you can view the group’s members (except for port and interface groups, which are only used for polling and threshold purposes). In addition, the group membership can be modified by adding or removing specific objects. The group rule will be automatically modified to reflect the objects that were added or removed from the group. You add or remove specific objects from a group’s membership in the Membership: Edit page of the Create Group Wizard.

Viewing the Group Summary

The final step in the Create Group Wizard is a summary page that displays the new group’s definition. Figure 8-10 shows an example of the Summary: Edit page.

Figure 8-10 Summary: Edit Page
Table 8-6 describes the fields on the Group Summary page of the Group Creation Wizard.

Table 8-6  Fields on the Group Summary Page

<table>
<thead>
<tr>
<th>Heading/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Name of the group you are creating.</td>
</tr>
<tr>
<td>Parent Group</td>
<td>The parent group of the group you are creating.</td>
</tr>
<tr>
<td>Description</td>
<td>A text description of the group.</td>
</tr>
<tr>
<td>Membership Update</td>
<td>How group membership is updated. Membership updates can be automatic (updated every time the group is accessed) or can be upon user request only (updated only when you click the Refresh button).</td>
</tr>
<tr>
<td>Rules</td>
<td>The rules used to filter group membership.</td>
</tr>
<tr>
<td>Visibility Scope</td>
<td>Setting that determines whether all CiscoWorks users or only the created user can view the group.</td>
</tr>
</tbody>
</table>

**Viewing Group Details**

A group’s information is displayed on the Properties: Details page.

**Step 1**  From the DFM home page, select Configuration > Other Configurations > Group Administration. The Group Administration and Configuration page appears.

**Note**  If you are connecting to the DFM server for the first time, a Security Alert window is displayed after you select nearly any option. Do not proceed without viewing and installing the security certificate. For more information, see Responding to Security Alerts, page 2-12.

**Step 2**  In the Group Selector, select the group for which you want to view details.

**Step 3**  Click Details. The Properties: Details page appears (see Figure 8-11).
Table 8-7 describes the fields on the Properties: Details page.

### Table 8-7  Fields on the Properties: Details Page

<table>
<thead>
<tr>
<th>Heading/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Name of the group you are viewing.</td>
</tr>
<tr>
<td>Parent Group</td>
<td>The parent group of the group you are viewing.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of the objects that belong to the group.</td>
</tr>
<tr>
<td>Description</td>
<td>A text description of the group.</td>
</tr>
<tr>
<td>Membership Update</td>
<td>How group membership is updated. Membership updates can be automatic (updated every time the group is accessed) or can be upon user request only (updated only when you click the Refresh button).</td>
</tr>
<tr>
<td>Created By</td>
<td>The person who created the group.</td>
</tr>
<tr>
<td>Last Modified By</td>
<td>The last person to modify the group.</td>
</tr>
<tr>
<td>Rules</td>
<td>The rules used to filter group membership.</td>
</tr>
<tr>
<td>View Parent Rules</td>
<td>Used to view the parent group rules.</td>
</tr>
<tr>
<td>Note</td>
<td>All parent group rules apply to the subgroups.</td>
</tr>
</tbody>
</table>
Viewing Membership Details

You can view a list of the objects that belong to a group by accessing the Properties: Details page. Membership is not displayed for port and interface groups, which are used only for polling and threshold purposes.

**Table 8-7  Fields on the Properties: Details Page (continued)**

<table>
<thead>
<tr>
<th>Heading/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Membership Details</td>
<td>Used to view the list of devices that belong to the group. Does not apply to port and interface groups.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Closes the page and takes you back to the Group Administration and Configuration page.</td>
</tr>
</tbody>
</table>

**Viewing Membership Details**

You can view a list of the objects that belong to a group by accessing the Properties: Details page. Membership is not displayed for port and interface groups, which are used only for polling and threshold purposes.

**Step 1** From the DFM home page, select **Configuration > Other Configurations > Group Administration**. The Group Administration and Configuration page appears.

**Note** If you are connecting to the DFM server for the first time, a Security Alert window is displayed after you select nearly any option. Do not proceed without viewing and installing the security certificate. For more information, see **Responding to Security Alerts, page 2-12**.

**Step 2** In the Group Selector, select the group for which you want to view details.

**Step 3** Click **Details**. The Properties: Details page appears.

**Step 4** Click **Membership Details**. The Membership: Details page appears.
Refreshing Membership

Refreshing a group’s membership forces the group to recompute its membership by reevaluating its rules and obtaining membership information from the data collectors. Port and interface group membership listings are not supported, because these groups are only used for polling and threshold purposes.

### Table 8-8 Fields on the Membership: Details Page

<table>
<thead>
<tr>
<th>Heading/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the device for which you want to view membership details.</td>
</tr>
<tr>
<td>Object Type</td>
<td>The type of object for which you want to view details.</td>
</tr>
<tr>
<td>Property Details</td>
<td>Takes you back to the Properties: Details page.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Closes the page and takes you back to the Group Administration and Configuration page.</td>
</tr>
</tbody>
</table>

**Step 1**
From the DFM home page, select **Configuration > Other Configurations > Group Administration**. The Group Administration and Configuration page appears.

**Note**
If you are connecting to the DFM server for the first time, a Security Alert window is displayed after you select nearly any option. Do not proceed without viewing and installing the security certificate. For more information, see *Responding to Security Alerts, page 2-12*.

**Step 2**
In the Group Selector, select the group you want to refresh.

**Step 3**
Click **Refresh**.

**Step 4**
In the confirmation dialog box, click **Yes**. In the next dialog box, click **OK**.
Deleting Groups

You can only delete user defined groups that are not one of the seven customizable groups.

**Step 1**  
From the DFM home page, select **Configuration > Other Configurations > Group Administration**. The Group Administration and Configuration page appears.

*Note*  
If you are connecting to the DFM server for the first time, a Security Alert window is displayed after you select nearly any option. Do not proceed without viewing and installing the security certificate. For more information, see Responding to Security Alerts, page 2-12.

**Step 2**  
In the Group Selector, select the group you want to delete.

**Step 3**  
Click **Delete**.

**Step 4**  
In the confirmation dialog box, click **Yes**. In the next dialog box, click **OK**.

Edit, Refresh, and Delete cause internal processes to start. For this reason, DFM could experience a period of high CPU utilization after these processes are triggered.
Configuring Views for the Alerts and Activities Display

These topics explain how to work with views in the Device Fault Manager (DFM) Alerts and Activities display:

- Getting Started with Views, page 9-1
- Creating a View, page 9-2
- Activating and Deactivating a View, page 9-4
- Modifying a View, page 9-5
- Deleting a View, page 9-7

Getting Started with Views

Simply put, views are logical groupings of existing device groups. You can populate your views with system-defined groups, as described in Working with System Defined Groups, page 8-4, and with groups you have created. Once you decide how you want to cluster your groups into a logical set, create and activate a view of these groups so they are shown in the Alerts and Activities display. View elements are not shown until the view is activated and is displayed in the view pane (normally every two minutes).

An Alerts and Activities display can have a maximum of 18 active views.
Creating a View

By default, the Alerts and Activities display contains two default views: All Alerts and Suspended Devices. These views are static and cannot be modified, deactivated, or deleted.

When you create a view, the view is applied to the server and is available to all clients of the server. Any action you perform on a view affects all clients of that server.

Depending on an alert’s severity, when an alert is raised for a device or element in one of your views, DFM notifies you by displaying the appropriate icon in the view selector, next to the view. This icon tells you which view needs your attention.

If the DFM server is using Access Control Server (ACS) mode, ACS may limit the devices you are permitted to view. For more information, refer to Device-Based Filtering, page 11-11.

Creating a View

You can create views using either:

- System Defined Groups, which are DFM system default groups, or
- User Defined Groups, which you can create yourself

See Managing Groups, page 8-1, for more information on groups.

Once you decide which groups to include in a view, use this procedure to create the view. Be sure to activate the view after creating it.
Creating a View

Note

Another way to create a view is to first create a view group using Grouping Services (under DFM user defined groups), and then create a view using that group. Refer to Editing a Group, page 8-12.

Step 1

From the DFM home page, select Configuration > Other Configurations Alerts and Activities Defaults. The Alerts and Activities Views: View Management page appears. Click Create. The View Properties: Create page appears, as shown in Figure 9-2.

**Figure 9-2  View Properties: Create Page**

Step 2

In the View Properties: Create page, do the following:

a. In the Name field, enter a unique name for your view. The name cannot exceed 18 characters and may use alphanumeric characters, underscores, dashes, hyphens, or spaces. You can use the name of a view that was deleted, but you cannot use the same name as any existing views.

b. (Optional) Enter a description in the Description field.
c. In the group object selector, activate the check boxes for the groups you want to include in your view.

d. Click Next. The View Summary: Create page appears.

Step 3
Do one of the following:
- If your settings are correct, click Finish. Your new view will be listed on the Alerts and Activities Views: View Management page.
- If your settings are incorrect, click Back.
- If you want to cancel the view creation, click Cancel.

Step 4
In the Alerts and Activities Views: View Management page:

a. Select the radio button for the view you want to activate.

b. Click Activate.

The Alerts and Activities display will display your new activated view when the view pane is refreshed (normally every two minutes).

Activating and Deactivating a View

To include a view in the Alerts and Activities display, you must first activate it. When you activate or deactivate a view, your changes are shown in the Alerts and Activities display when the view pane is refreshed (every two minutes). If you deactivate a view, it is removed from your Alerts and Activities display when the view pane is refreshed. The deactivated view can be reactivated from the Alerts and Activities Views: View Management page. An Alerts and Activities display may contain a maximum of 18 active views for each partition.

Note
You cannot deactivate the All Alerts view or Suspended Devices view.
Chapter 9 Configuring Views for the Alerts and Activities Display

Modifying a View

Step 1 From the DFM home page, select Configuration > Other Configurations Alerts and Activities Defaults. The Alerts and Activities Views: View Management page appears.

Step 2 In the Alerts and Activities Views: View Management, page:

a. Select the radio button for the view you want to activate or deactivate.

b. Do one of the following:
   • Click Activate. A confirmation window appears. The view is added to the Alerts and Activities display when the view pane is refreshed (normally every two minutes).
   • Click Deactivate. A confirmation window appears.

Step 3 Click Yes to confirm your action.

The view is added to or deleted from the Alerts and Activities display when the view pane is refreshed (normally every two minutes). The corresponding status change is reflected in the View Management table.

Modifying a View

You can modify views that are active or have been deactivated.

Note You cannot modify the All Alerts or Suspended Devices views.

Step 1 From the DFM home page, select Configuration > Other Configurations Alerts and Activities Defaults. The Alerts and Activities Views: View Management page appears.

Step 2 In the view selector, activate the radio button for the view you want to modify.

Step 3 Click Edit. The View Properties: Edit page appears.
Modifying a View

**Step 4** In the View Properties: Edit page, you can:

- **a.** Change the description in the Description field.
- **b.** Change the view membership by activating or deactivating group check boxes.

**Note** You cannot change the name of the view.

**Step 5** Click **Next**. The View Summary: Edit page appears.

**Step 6** Do one of the following:

- If your settings are correct, click **Finish**. Your new view will be listed on the Alerts and Activities Views: View Management page.
- If your settings are incorrect, click **Back**.
- If you want to cancel the edit, click **Cancel**.

**Step 7** If you edited a deactivated view, activate it (if desired) in the Alerts and Activities: View Management page:

- **a.** Select the view radio button.
- **b.** Click **Activate**.

Your view changes will appear when the view pane is refreshed (normally every two minutes).
Deleting a View

Because active views can be deleted, exercise caution when deleting views. You cannot delete the All Alerts or Suspended Devices views.

You can delete views that are active or have been deactivated.

**Step 1**
From the DFM home page, select **Configuration > Other Configurations Alerts and Activities Defaults**. The Alerts and Activities Views: View Management page appears.

**Step 2**
In the Alerts and Activities Views: View Management page:

a. Select the radio button for the view you want to delete.

b. Click **Delete**. A confirmation message appears.

**Step 3**
Click **Yes** to confirm the deletion.

The view will be removed from the Alerts and Activities view pane when the view pane is refreshed (normally every two minutes).
Deleting a View
Configuring Polling and Thresholds

These topics describe the process for configuring polling settings and threshold values for Device Fault Manager (DFM):

- Overview of Polling and Thresholds, page 10-1
- Updating Polling Parameters and Thresholds, page 10-13
- Managing Polling Parameters, page 10-18
- Managing Thresholds, page 10-26

Overview of Polling and Thresholds

Managing Groups, page 8-1, described how Group Administration organizes devices, device interfaces, and device ports into different groups. The Common Services system-defined groups include groups such as Broadband Cable, Routers, Switches and Hubs, and so forth. These groups have specific polling and threshold settings, while the Broadband Cable device type has different polling and threshold settings. Because a device can belong to multiple groups, the devices uses the polling and threshold settings of the overriding group.

The DFM Polling and Threshold function creates its own corresponding groups based on Common Services and DFM groups:

- Polling groups that determine how often group members are polled for data.
- Threshold groups that determine acceptable levels of performance and utilization for group members.
Overview of Polling and Thresholds

When group objects are polled and any object’s data shows that threshold values have been exceeded, or values have fallen below acceptable levels, DFM generates the appropriate events.

DFM is configured with factory settings (or defaults) for polling parameters and threshold values. You can use the factory settings, modify them, and restore them to factory settings at any time.

In many cases, it may be acceptable to use the factory settings for polling parameters. However, depending on how important a device group is, you can increase or decrease the polling interval to accomplish either of the following objectives:

- Minimize the impact on the polled devices
- Enhance the resolution of the collected data

In addition, you can enhance the performance and utilization of devices by adjusting thresholds, taking into account the following information:

- Location of the devices in the IP fabric
- Resource constraints

Which Settings Are Applied to Devices, Ports, and Interfaces?

Every device, device port, and device interface belongs to at least one system-defined group; in fact, they can belong to several. When a device belongs to several groups, DFM uses the settings of the overriding group. The overriding group is the highest priority device group to which the device belongs. These topics provide more information on priorities:

- Setting Priorities, page 10-4, explains how to change group priorities.
- How Does DFM Prioritize Groups for Polling and Thresholds?, page 10-6, lists default group priorities.
Chapter 10  Configuring Polling and Thresholds

Overview of Polling and Thresholds

Which Polling Settings Are Applied?

You can set and apply polling parameters to device groups (not for individual devices). When a device is polled, its ports and interfaces are also polled; therefore, port and interface polling is controlled at the device level.

Every device belongs to at least one system-defined device group. See Working with System Defined Groups, page 8-4, for information about how devices are assigned to system-defined groups. If a device belongs to more than one group, DFM uses the polling settings of the overriding group (with the highest priority, as described in Setting Priorities, page 10-4).

Which Threshold Settings Are Applied?

You can set and apply threshold parameters to device, interface, and port groups. When a device is polled, DFM compares the new data against the threshold settings. If a threshold value has been exceeded, or a value has fallen below acceptable levels, DFM generates the appropriate event.

If a device, port, or interface belongs to more than one group, DFM uses the threshold settings of the overriding group (the group you determine to have the highest priority, as described in Viewing the Overriding Group—Examples, page 10-9).

What Are Customizable Groups?

Customizable groups are the only user-defined groups for which you can set polling and threshold parameters. They are provided so you can create groups that fit your needs. DFM provides 28 customizable groups, which are divided into four categories:

- Access Port Groups
- Trunk Port Groups
- Interface Groups
- Device Groups
Table 10-1 lists the seven customizable groups that appear in each of the four categories.

**Table 10-1 Polling and Thresholds: Customizable Groups**

<table>
<thead>
<tr>
<th>Customizable Groups</th>
<th>Intended Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>A, B, and C</td>
<td>Consider reserving customizable groups A, B, and C to troubleshoot: Add one device to any of these groups when you need to test; for example, to test a changed threshold or interval value for a polling setting.</td>
</tr>
<tr>
<td>1, 2, 3, and 4</td>
<td>Consider using customizable groups 1, 2, 3, and 4 when you want to override polling settings and thresholds for more than one device.</td>
</tr>
</tbody>
</table>

You configure a customizable group to have the highest priority. To do so, see Setting Priorities, page 10-4. You must add devices to the customizable groups before you can set polling parameters or threshold values for them. To do so, see Working with Customizable Groups, page 8-7.

## Setting Priorities

System-defined groups have a higher priority than customizable groups, but you can change the priorities as needed. This is helpful, for example, when you configure specific customizable groups of interest and want to give them the highest priority. For information on how to view the overriding group for devices, ports and interfaces, refer to Viewing the Overriding Group—Examples, page 10-9.
Step 1  From the DFM home page, select Configuration > Polling and Thresholds > Setting Priorities. The Setting Priorities page appears, displaying the groups in priority order.

Step 2  Activate the radio button that corresponds to the group type, one of the following:

- Polling groups:
  - Device Polling Groups

- Threshold groups:
  - Device Threshold Groups
  - Interface Threshold Groups
  - Access Port Threshold Groups
  - Trunk Port Threshold Groups

Step 3  Rearrange the groups according to your preference (the closer the group is to the top of the list, the higher its priority):

a. Select a group.

b. Move the group up or down using the arrows.

Step 4  Click Save to save the changes.

Note  A device can have different overriding polling and threshold groups.

Note  The changes do not take effect until you apply them to DFM. See Applying Changes, page 7-4.
How Does DFM Prioritize Groups for Polling and Thresholds?

Because devices, ports, and interfaces can belong to multiple groups, DFM uses the highest priority group to which the device belongs to determine which polling and threshold parameters to use. DFM prioritizes groups as shown in the following tables, with groups in descending order of priority:

- Access and Trunk Port Group Priorities for Thresholds, Table 10-2 on page 10-6
- Interface Groups Priorities for Thresholds, Table 10-3 on page 10-7
- Device Groups Priorities for Polling and Thresholds, Table 10-4 on page 10-8

**Note**

To find the overriding group for a device, you can select any device group to which the device belongs and view a Polling Parameter Summary or a Threshold Parameter Summary for the group.

### Table 10-2  Access and Trunk Port Group Priorities for Thresholds

<table>
<thead>
<tr>
<th>Access and Trunk Port Groups in Priority Order</th>
<th>Parameters to Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>1 GB Ethernet</td>
<td>Threshold</td>
</tr>
<tr>
<td>10MB-100MB Ethernet</td>
<td></td>
</tr>
<tr>
<td>ATM</td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td></td>
</tr>
<tr>
<td>User Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Group A</td>
<td>Threshold</td>
</tr>
<tr>
<td>Customizable Group B</td>
<td></td>
</tr>
<tr>
<td>Customizable Group C</td>
<td></td>
</tr>
</tbody>
</table>
### Table 10-3 Interface Groups Priorities for Thresholds

<table>
<thead>
<tr>
<th>Interface Groups in Priority Order</th>
<th>Parameters to Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>1GB Ethernet</td>
<td>Threshold</td>
</tr>
<tr>
<td>10MB-100MB Ethernet</td>
<td>Threshold</td>
</tr>
<tr>
<td>ATM</td>
<td>Threshold</td>
</tr>
<tr>
<td>Token Ring</td>
<td>Threshold</td>
</tr>
<tr>
<td>ISDN Physical Interface</td>
<td>Threshold</td>
</tr>
<tr>
<td>ISDN B Channel</td>
<td>Threshold</td>
</tr>
<tr>
<td>ISDN D Channel</td>
<td>Threshold</td>
</tr>
<tr>
<td>Serial</td>
<td>Threshold</td>
</tr>
<tr>
<td>FDDI</td>
<td>Threshold</td>
</tr>
<tr>
<td>Backup</td>
<td>Threshold</td>
</tr>
<tr>
<td>Dial-on-Demand</td>
<td>Threshold</td>
</tr>
<tr>
<td>Others</td>
<td>Threshold</td>
</tr>
<tr>
<td>User Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Group A</td>
<td>Threshold</td>
</tr>
<tr>
<td>Customizable Group B</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Group C</td>
<td>None</td>
</tr>
</tbody>
</table>
### Table 10-3  Interface Groups Priorities for Thresholds (continued)

<table>
<thead>
<tr>
<th>Interface Groups in Priority Order</th>
<th>Parameters to Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizable Group 1</td>
<td>Threshold</td>
</tr>
<tr>
<td>Customizable Group 2</td>
<td></td>
</tr>
<tr>
<td>Customizable Group 3</td>
<td></td>
</tr>
<tr>
<td>Customizable Group 4</td>
<td></td>
</tr>
</tbody>
</table>

### Table 10-4  Device Groups Priorities for Polling and Thresholds

<table>
<thead>
<tr>
<th>Device Groups in Priority Order</th>
<th>Parameters to Set¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>Security and VPN</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Content Networking</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Voice and Telephony</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Wireless</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Universal Gateways and Access Servers</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Broadband Cable</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Routers</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Storage Networking</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Optical Networking</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Switches and Hubs</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>DSL and Long Reach Ethernet (LRE)</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Cisco Interfaces and Modules</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Network Management</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>User Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Group A</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Customizable Group B</td>
<td></td>
</tr>
<tr>
<td>Customizable Group C</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 10 Configuring Polling and Thresholds

Overview of Polling and Thresholds

For additional information, see the following topics:

- How Can I Set Parameters for a Device, Interface, or Port?, page 10-11
- Selecting Groups, page 10-14

Viewing the Overriding Group—Examples

The Polling Parameter Summary and Threshold Parameter Summary pages provide information on the overriding groups for all devices in a specific group. Locating the overriding group for a port or interface is a bit more complex, as described in the following procedures.

Viewing the Overriding Polling or Threshold Group for a Device

Use the summary page to identify a device’s overriding group.

1. From the DFM home page, select Configuration > Polling and Thresholds.
2. Do one of the following:
   - To view the overriding polling groups, select Polling Parameters.
   - To view the overriding threshold group, select Managing Thresholds.

Note: A device can have different overriding polling and threshold groups. For example, if you assign a router to use the settings from a customizable polling group, it would still use the settings from its original threshold group.
Step 3  Select a device group and click View. The appropriate summary page opens. Locate the device in which you are interested, and check the Overriding Group column.

Viewing the Overriding Polling Group for a Port or Interface

Step 1  From the DFM home page, select Configuration > Polling and Thresholds.

Step 2  Consider the port or interface type and check the appropriate system-defined group for that type, and select Managing Thresholds.

Step 3  Select the port or interface group and click View.

For example, if you think an interface is in the 10MB-100MB Ethernet interface group, you would select Managing Thresholds, choose that group, click View, and Figure 10-1 would open.

Figure 10-1  Viewing the 10MB-100MB Ethernet Interface Group—Step 1 (of 2)

Step 4  Click View Interfaces. A complete list of interfaces is displayed. (If you were searching for a port, the link would say View Ports.)
Overview of Polling and Thresholds

Figure 10-2  Viewing the 10MB-100MB Ethernet Interface Group — Step 2 (of 2)

Step 5  If the interface or port appears as a member, that group is the overriding group. (Ports and interfaces are only listed as members in the overriding group.)

If the interface or port does not appear, repeat this process for all of the customizable groups until you locate the port or interface.

How Can I Set Parameters for a Device, Interface, or Port?

There are several ways in which you can control the parameters for a device, interface, or port. Polling and thresholds are always applied on a group level, not on a specific device, port, or interface level.

Note  Be careful when you change settings for a system-defined group. Your changes will affect the settings of all devices in the group.

Note  To apply settings to a device or component that belongs to multiple groups, make sure the group with the desired settings is the overriding group (has the highest priority), as described in Setting Priorities, page 10-4.
To configure *polling and threshold* settings for a *device*:

- Adjust the polling and threshold settings for the Common Services system-defined group to which the device belongs (and verify the overriding group, if applicable). This changes the settings for all devices in that system-defined group.

- Edit a customizable device group, apply the desired polling and threshold settings to the group, and verify the overriding group. In this way, you can create a group of specific devices in which you are interested, and specify settings for them.

To configure *polling on interfaces and ports*:

- Adjust the polling settings defined by the Common Services system-defined group (and verify the overriding group, if applicable). This changes the polling settings for all interfaces and ports on devices in that system-defined group.

- Edit a customizable device group, apply the desired polling settings to the group, and verify the overriding group. In this way, only the ports and interfaces on specific devices are affected.

To configure *thresholds on interfaces and ports*:

- Adjust the threshold settings defined by the DFM system-defined port or interface group (and verify the overriding group, if applicable). (Make sure the port or interface belongs to that group, as described in *Viewing the Overriding Polling Group for a Port or Interface, page 10-10*.) This changes the threshold settings for all interfaces and ports in that system-defined group.

- Edit a customizable interface or port group, apply the desired threshold settings, and verify the overriding group. In this way, only the ports and interfaces on specific devices are affected.

For additional information, see the following topics:

- Editing Polling Parameters, page 10-20
- Editing Thresholds, page 10-28
Updating Polling Parameters and Thresholds

This topic explains how to update polling parameters and thresholds and provides links to the related procedures.

DFM is preconfigured with factory settings for polling parameters and thresholds for each system-defined group of devices. You can make the following changes:

- Update the polling parameters and thresholds for system-defined groups.
- Restore polling parameters and thresholds to factory settings.
- Add devices to one or more of seven predefined customizable groups and edit their polling parameters and thresholds.

The following describes the basic process for updating polling parameters and thresholds.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedures</th>
</tr>
</thead>
</table>
| **Step 1** If you are working with a customizable group, you may need to attend to the following tasks first:  
  a. Add devices to the customizable group. By default, no devices belong to customizable groups.  
  b. (Optional) Set the priority of the customizable group. By default, customizable groups have a lower priority than system-defined groups, but you may want to change the priority. | **Editing and Creating Groups**, page 8-11  
**Setting Priorities**, page 10-4 |
| **Step 2** Change polling parameters for a device group (either a Common Services system-defined group, or DFM customizable device group). | **Editing Polling Parameters**, page 10-20  
**Restoring Factory Setting Polling Parameters**, page 10-23 |
Selecting Groups

The first thing you must do when you use polling and threshold options is select a group. If you want to view parameters, you can select any group. If you want to edit parameters or restore them to factory settings, you must select a group for which parameters exist.

Table 10-5 lists groups in the order in which they are displayed in the group selector and notes whether applicable parameters exist for the group. The group selector you see may not display all of the device groups listed in Table 10-5:

- Device groups are displayed when they have members.
- Port and interface groups are displayed when a rule has been applied to them, using Group Administration.

<table>
<thead>
<tr>
<th>Device Groups in Display Order</th>
<th>Parameters to Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS@server</td>
<td>None</td>
</tr>
<tr>
<td>System Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>Broadband Cable</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Cisco Interfaces and Modules</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Content Networking</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>DSL and Long Reach Ethernet (LRE)</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Network Management</td>
<td>Thresholds</td>
</tr>
</tbody>
</table>

Table 10-5  Device Groups as Displayed in the Device Selector
### Table 10-5  Device Groups as Displayed in the Device Selector (continued)

<table>
<thead>
<tr>
<th>Device Groups in Display Order</th>
<th>Parameters to Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optical Networking</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Routers</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Security and VPN</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Storage Networking</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Switches and Hubs</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Universal Gateways and Access Servers</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Voice and Telephony</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Wireless</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>DFM@server</td>
<td>None</td>
</tr>
<tr>
<td>System Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>Access Port Groups</td>
<td>None</td>
</tr>
<tr>
<td>1GB Ethernet</td>
<td>Thresholds</td>
</tr>
<tr>
<td>10MB-100MB Ethernet</td>
<td>Thresholds</td>
</tr>
<tr>
<td>ATM</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Others</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Interface Groups</td>
<td>None</td>
</tr>
<tr>
<td>1GB Ethernet</td>
<td>Thresholds</td>
</tr>
<tr>
<td>10MB-100MB Ethernet</td>
<td>Thresholds</td>
</tr>
<tr>
<td>ATM</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Backup</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Dial-on-Demand</td>
<td>Thresholds</td>
</tr>
<tr>
<td>FDDI</td>
<td>Thresholds</td>
</tr>
<tr>
<td>ISDN B Channel</td>
<td>Thresholds</td>
</tr>
<tr>
<td>ISDN D Channel</td>
<td>Thresholds</td>
</tr>
<tr>
<td>ISDN Physical Interface</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Others</td>
<td>Thresholds</td>
</tr>
</tbody>
</table>
Table 10-5 Device Groups as Displayed in the Device Selector (continued)

<table>
<thead>
<tr>
<th>Device Groups in Display Order</th>
<th>Parameters to Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Token Ring</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Trunk Port Groups</td>
<td>None</td>
</tr>
<tr>
<td>1GB Ethernet</td>
<td>Thresholds</td>
</tr>
<tr>
<td>10MB-100MB Ethernet</td>
<td>Thresholds</td>
</tr>
<tr>
<td>ATM</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Others</td>
<td>Thresholds</td>
</tr>
<tr>
<td>User Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Access Port Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Group A</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group B</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group C</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 1</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 2</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 3</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 4</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Group A</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Customizable Group B</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Customizable Group C</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Customizable Group 1</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Customizable Group 2</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Customizable Group 3</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Customizable Group 4</td>
<td>Polling and thresholds</td>
</tr>
</tbody>
</table>
### Table 10-5  Device Groups as Displayed in the Device Selector (continued)

<table>
<thead>
<tr>
<th>Device Groups in Display Order</th>
<th>Parameters to Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizable Interface Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Group A</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group B</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group C</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 1</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 2</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 3</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 4</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Trunk Port Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Group A</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group B</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group C</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 1</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 2</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 3</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 4</td>
<td>Thresholds</td>
</tr>
</tbody>
</table>

For additional information, see the following topics:

- Viewing Polling Parameters, page 10-18
- Editing Polling Parameters, page 10-20
- Viewing Thresholds, page 10-26
- Editing Thresholds, page 10-28
Managing Polling Parameters

After you select Configuration > Polling and Thresholds > Polling Parameters from the DFM home page, you can perform any of the following tasks:

- Viewing Polling Parameters, page 10-18
- Editing Polling Parameters, page 10-20
- Restoring Factory Setting Polling Parameters, page 10-23

You can adjust polling parameters on devices only; port and interface polling is controlled at the device level. Therefore, you can adjust polling for these two types of groups:

- Common Services System Defined Groups
- DFM Customizable Groups (for devices)

Viewing Polling Parameters

When you view polling parameters, you can see the devices that are members of the device group, and you can see the factory setting as well as current values for the polling parameters. Devices belonging to multiple groups use the polling settings of the overriding group. Interface and port polling is controlled at the device level; in other words, switches have a specific polling setting, and that setting determines when the switch ports are polled.

Note

If the DFM server is using Access Control Server (ACS) mode, ACS may limit the devices you are permitted to view when you generate a Polling Parameter Summary. For more information, refer to Device-Based Filtering, page 11-11.

Step 1
From the DFM home page, select Configuration > Polling and Thresholds > Polling Parameters.

Step 2
Select any device group from the group selector. For more information, see Selecting Groups, page 10-14.

Step 3
Click the View button. The Polling Parameter Summary tabular display opens in a separate window. This display provides the following information.
### Chapter 10 Configuring Polling and Thresholds

#### Managing Polling Parameters

**Step 4** When you are done viewing the polling parameters, close the tabular display.

For additional information, see the following topics:

- Viewing the Overriding Group—Examples, page 10-9
- Viewing Data from Tabular Displays with Over 2000 Records, page 2-6
- Printing Tabular Displays, page 2-7

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>IP address or DNS name of a device.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Device function.</td>
</tr>
<tr>
<td>Polling Parameters</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Name of the polling setting to which the values apply.</td>
</tr>
<tr>
<td></td>
<td>Default Value (sec)—Factory setting for number of seconds between successive polls for the setting.</td>
</tr>
<tr>
<td></td>
<td>Default Retries—Factory setting for number of times to retry a failed poll request.</td>
</tr>
<tr>
<td></td>
<td>Default Timeout (msec)—Factory setting for number of milliseconds before a poll request times out.</td>
</tr>
<tr>
<td>Current Value (sec)</td>
<td>Current number of seconds between successive polls for the setting.</td>
</tr>
<tr>
<td>Current Retries</td>
<td>Current number of times to retry a failed poll request.</td>
</tr>
<tr>
<td>Current Timeout (msec)</td>
<td>Current number of milliseconds before a poll request times out.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Whether polling is enabled (true) or disabled (false).</td>
</tr>
<tr>
<td>Overriding Group</td>
<td>Device group from which polling parameter values are applied. (This is the highest priority device group to which the device belongs.)</td>
</tr>
</tbody>
</table>

**Note** If you want to change the polling parameters for a device, you can edit the settings for the overriding group. See Editing Polling Parameters, page 10-20.
Editing Polling Parameters

When you edit polling parameters, you edit settings that are associated with device groups, not with individual devices.

**Step 1**
From the DFM home page, select Configuration > Polling and Thresholds > Polling Parameters.

**Step 2**
Select a device group for which you can set polling parameters. See Selecting Groups, page 10-14 for a list of such device groups.

**Step 3**
Click the Edit button. The Polling Parameters: Edit page appears, displaying the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>The parameters for the selected device group are displayed, including:</td>
</tr>
<tr>
<td></td>
<td>• Current values for each setting</td>
</tr>
<tr>
<td></td>
<td>• Whether values are the factory settings (Default check box selected)</td>
</tr>
<tr>
<td></td>
<td>• Whether polling is enabled for the settings (Enabled check box selected)</td>
</tr>
</tbody>
</table>

**Step 4**
Change the parameters appropriately for each setting. Each setting controls how frequently devices are polled for a particular type of data; for example, reachability.

- To reset all settings to factory settings, select the Default check box in the table heading.
- To disable polling for all settings, deselect the Enabled check box in the table heading.
- To set parameters for individual settings, enter data for the following parameters for each setting.
### Chapter 10  Configuring Polling and Thresholds

#### Managing Polling Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Interval</td>
<td>Enter the number of seconds between successive polls for the setting.</td>
<td>See Device Polling Settings, page 10-24 for the minimum interval for each polling setting.</td>
</tr>
<tr>
<td></td>
<td>Maximum value: 3600</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Minimum value: 30</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Increment: 1</td>
<td></td>
</tr>
<tr>
<td>New Timeout</td>
<td>Enter the number of milliseconds allowed for a poll request before it times out.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Minimum value: 10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maximum value: 60,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Increment: 1</td>
<td></td>
</tr>
<tr>
<td>New Retry</td>
<td>Enter the number of times to retry a failed poll request.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Minimum value: 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maximum value: 10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Increment: 1</td>
<td></td>
</tr>
</tbody>
</table>
Managing Polling Parameters

### Step 5

To save the settings, do one of the following:

- Click **Save** to save the changes and display the Polling Parameters: Edit page again.
- Click **OK** to save the changes and close the Polling Parameters: Edit page.

**Note**: Although the polling parameters are saved in the database, they are not yet applied to the IP fabric. See **Applying Changes**, page 7-4.

For additional information, see the following topics:

- **Selecting Groups**, page 10-14
- **Updating Polling Parameters and Thresholds**, page 10-13
- **Restoring Factory Setting Polling Parameters**, page 10-23
Understanding What Happens When You Apply Changes

After adjusting polling and threshold settings, select Configuration > Polling and Thresholds > Apply Changes to have DFM start using your changes. The following explains the difference between saving your changes and applying your changes.

When you save changes, DFM performs the following tasks:

- Sets the polling and threshold settings of devices in the selected device group.
- Sets the overriding group, based on the priorities of the groups to which devices belong.

When you apply changes, DFM performs the following tasks:

- Recalculates group membership, based on group priority.
- Uses the new polling and threshold settings to gather information from the devices.

You must also apply changes after resuming a device, so that DFM will begin polling the device depending on the appropriate settings.

Restoring Factory Setting Polling Parameters

You can restore all parameter settings for a device group to factory settings using this procedure. If, instead, you want to restore only a few settings, see Editing Polling Parameters, page 10-20.

Before You Begin

To review the factory settings for polling parameters before you apply them, view the Polling Parameter Summary for the device group. See Viewing Polling Parameters, page 10-18. Current settings, along with the factory settings, are displayed.

Step 1  From the DFM home page, select Configuration > Polling and Thresholds > Polling Parameters.

Step 2  Select a device group for which you can restore polling parameters. See Selecting Groups, page 10-14 for a list of such device groups.
Managing Polling Parameters

Step 3  Click the **Factory Setting** button. A confirmation dialog box appears.

Step 4  Click **Yes**.

**Note**  The settings are stored in the database, but not yet applied to the IP fabric. See **Applying Changes, page 7-4**.

---

**Device Polling Settings**

Table 10-6 lists the polling settings that are applicable to each device group (or type), along with the minimum and maximum polling interval for each setting.

**Note**  The minimum interval is usually lower than the factory setting provided by DFM. See **Viewing Polling Parameters, page 10-18**, to obtain information about how to open a Polling Parameter Summary, which lists the factory settings for polling parameter values. This section also describes the minimum and maximum values for Interval, Timeout, and Retry parameters.
Table 10-6 Polling Settings for Device Groups (Device Types)

<table>
<thead>
<tr>
<th>Device Group Type (Device Type)</th>
<th>Polling Settings</th>
<th>Interval (in seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadband Cable</td>
<td>• Reachability settings</td>
<td>30 minimum, 3600 maximum</td>
</tr>
<tr>
<td>Cisco Interfaces and Modules</td>
<td>• Processor and memory utilization</td>
<td></td>
</tr>
<tr>
<td>Content Networking</td>
<td>• Environment</td>
<td></td>
</tr>
<tr>
<td>DSL and Long Reach Ethernet (LRE)</td>
<td>• Connector port and interface</td>
<td></td>
</tr>
<tr>
<td>Optical Networking</td>
<td>• Access port</td>
<td></td>
</tr>
<tr>
<td>Routers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security and VPN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage Networking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switches and Hubs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Universal Gateways and Access Servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice and Telephony</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Management</td>
<td>• Reachability settings</td>
<td>30 minimum, 3600 maximum</td>
</tr>
<tr>
<td></td>
<td>• Connector and port interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Access port</td>
<td></td>
</tr>
</tbody>
</table>
Managing Thresholds

When you select the Managing Thresholds application from the DFM navigation tree, you can perform any of the following tasks:

- Viewing Thresholds, page 10-26
- Editing Thresholds, page 10-28
- Restoring Factory Settings for Thresholds, page 10-30

Viewing Thresholds

You can view the thresholds that are associated with device groups, trunk port groups, access port groups, and interface groups. Because the numbers of ports and interfaces can be very large, the Threshold Parameter Summary page provides a link through which you can launch a separate page that lists all the ports and interface members of the group. If desired, you can save a comma separated value (CSV) version of the port or interface summary.

Note

If the DFM server is using Access Control Server (ACS) mode, ACS may limit the devices you are permitted to view when you generate a Polling Parameter Summary. For more information, refer to Device-Based Filtering, page 11-11.

Step 1

From the DFM home page, select Configuration > Polling and Thresholds > Managing Thresholds.

Step 2

Select any device group from the group selector. For more information, see Selecting Groups, page 10-14.

Step 3

Click the View button. The Thresholds Summary tabular display opens in a separate window. The Thresholds Parameter Summary tabular display provides the following information.
## Chapter 10  Configuring Polling and Thresholds

### Managing Thresholds

#### Step 4

When you are done viewing the threshold parameters, close the tabular display window.

<table>
<thead>
<tr>
<th>Summary Section</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Heading</strong></td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>IP address or DNS name of the device (device group summaries only).</td>
</tr>
<tr>
<td>Device Type</td>
<td>Device function (device group summaries only).</td>
</tr>
<tr>
<td>View xxxxxx</td>
<td>Link that launches a port or interface report, where xxxxxx is Access Ports, Interfaces, or Trunk Ports.</td>
</tr>
<tr>
<td><strong>Threshold Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>Category Name</td>
<td>Threshold category.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Whether threshold analysis is enabled (true) or disabled (false).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Threshold name.</td>
</tr>
<tr>
<td>Metric</td>
<td>Unit of measurement for parameter value:</td>
</tr>
<tr>
<td></td>
<td>•   %—percent.</td>
</tr>
<tr>
<td></td>
<td>•   count—number of occurrences.</td>
</tr>
<tr>
<td></td>
<td>•   sec—number of seconds.</td>
</tr>
<tr>
<td></td>
<td>•   C—centigrade.</td>
</tr>
<tr>
<td>Default</td>
<td>Factory setting for the parameter.</td>
</tr>
<tr>
<td>Current</td>
<td>Current value for the parameter.</td>
</tr>
<tr>
<td>Overriding Group</td>
<td>Group from which threshold parameter values are applied. (This is the highest priority group to which the element belongs.)</td>
</tr>
</tbody>
</table>

---
For additional information, see the following topics:

- Viewing the Overriding Group—Examples, page 10-9
- Viewing Data from Tabular Displays with Over 2000 Records, page 2-6
- Exporting Data from Tabular Displays, page 2-6
- Printing Tabular Displays, page 2-7

## Editing Thresholds

When you edit thresholds, you edit values that are associated with groups, not with individual devices, ports, or interfaces. For ports and interfaces, you can activate or deactivate an entire group of threshold settings (for example, if you want to disable Reachability Settings for an entire interface group).

**Step 1**
From the DFM home page, select **Configuration > Polling and Thresholds > Managing Thresholds**.

**Step 2**
Select a group for which you can set thresholds. See **Selecting Groups, page 10-14** for a list of such device groups.

**Step 3**
Click the **Edit** button. The Thresholds: Edit page appears, displaying the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Type</td>
<td>Device function (not applicable to port or interface groups)</td>
</tr>
<tr>
<td>Threshold Category</td>
<td>Only those categories that are applicable to the members in the group are displayed.</td>
</tr>
<tr>
<td>Parameter</td>
<td>The parameters for the currently selected object and threshold category are displayed, including:</td>
</tr>
<tr>
<td></td>
<td>• Current value for each threshold alongside an entry field for a new value.</td>
</tr>
<tr>
<td></td>
<td>• Default check boxes that allow you to reset factory settings for all thresholds or for selected thresholds.</td>
</tr>
</tbody>
</table>
### Step 4

Edit the thresholds by selecting the threshold category and changing the thresholds appropriately:

- To reset factory settings for all thresholds in the category, select the Default check box in the table heading.
- To set values for individual thresholds for a group, enter data for each threshold.

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Value</td>
<td>(Optional) Enter a new value.</td>
</tr>
<tr>
<td>Default</td>
<td>If you entered a new value, make sure that the Default check box is not selected. To reset thresholds to the factory settings, select this check box.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The Default check box in the table heading can override this setting.</td>
</tr>
</tbody>
</table>

- To activate or deactivate an entire group of threshold settings for interface and port groups—such as Interface/port flapping settings for interface or port groups, or Reachability settings for device groups—select the Customize Settings button.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional Settings</td>
<td>Threshold settings groups that are not currently enabled.</td>
</tr>
<tr>
<td>Active Settings</td>
<td>Threshold settings groups that are currently enabled.</td>
</tr>
</tbody>
</table>

Use the Add or Remove button to select the settings group you want to enable or disable.

- To activate or deactivate all threshold settings, activate or deactivate the Disable All Threshold Settings for this Group check box.
Step 5  To save the thresholds, do one of the following:
- Click **Save** to save the thresholds and display the Thresholds: Edit page again.
- Click **OK** to save the thresholds and close the Thresholds: Edit page.

**Note**  Although the thresholds are saved in the database, they are not yet applied to the IP fabric. See **Applying Changes, page 7-4**.

---

For additional information, see the following topics:
- **Threshold Definitions, page 10-34**
- **Understanding What Happens When You Apply Changes, page 10-23**

### Restoring Factory Settings for Thresholds

You can use this procedure to reset all thresholds for a device group, and you can reset all categories of thresholds to use factory settings.

**Before You Begin**

To review factory settings for thresholds before you apply them, view the thresholds for the device group. See **Viewing Thresholds, page 10-26**. Current values are displayed along with the factory settings.

**Step 1**  From the DFM home page, select **Configuration > Polling and Thresholds > Managing Thresholds**.

**Step 2**  Select a device group for which you can set thresholds. See **Selecting Groups, page 10-14** for a list of such device groups.
Step 3  Click the **Factory Setting** button. A confirmation dialog box appears.

Step 4  Click **Yes**.

**Note**  The settings are stored in the database, but not yet applied to the IP fabric.  See **Applying Changes, page 7-4**.

For additional information, see the following topics:
- Viewing Thresholds, page 10-26
- Threshold Definitions, page 10-34
- Threshold Parameter Values and Events, page 10-40

**Threshold Categories for Devices, Interfaces, and Ports**

Table 10-7 lists the threshold categories for each device group. For the parameters that you can set for each threshold category, see **Threshold Definitions, page 10-34**, or **Threshold Parameter Values and Events, page 10-40**.
### Table 10-7  System-Defined Groups and Applicable Threshold Groups

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Rule</th>
<th>Threshold Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common Services System Defined Groups</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadband Cable</td>
<td>(Controlled by Common Services Group Administration)</td>
<td>Reachability</td>
</tr>
<tr>
<td>Cisco Interfaces and Modules</td>
<td></td>
<td>Processor and Memory Environment</td>
</tr>
<tr>
<td>Content Networking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSL &amp;LREs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optical Networking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security and VPN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage Networking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switches and Hubs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Universal Gateways and Access Servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice and Telephony</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Management</td>
<td></td>
<td>Reachability</td>
</tr>
</tbody>
</table>

**Table 10-7**  

**Managing Thresholds**

**User Guide for Device Fault Manager**

---

**Chapter 10  Configuring Polling and Thresholds**
### Table 10-7  System-Defined Groups and Applicable Threshold Groups (continued)

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Rule</th>
<th>Threshold Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFM System Defined Groups—Interfaces</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 GB Ethernet</td>
<td>MaxSpeed = “1000000000”</td>
<td>Generic interface/port performance</td>
</tr>
<tr>
<td></td>
<td>Type contains “ETHER” or “CSMACD”</td>
<td></td>
</tr>
<tr>
<td>10/100MB Ethernet</td>
<td>Type contains “ETHER” or “CSMACD”</td>
<td>Backup interface support</td>
</tr>
<tr>
<td>ATM</td>
<td>Type contains “ATM”</td>
<td>Dial-On-Demand interface support</td>
</tr>
<tr>
<td>Token Ring</td>
<td>Type contains “TOKEN”</td>
<td>Interface/port flapping</td>
</tr>
<tr>
<td>ISDN physical interface</td>
<td>InterfaceCode contains “ISDNDPHYSICAL”</td>
<td></td>
</tr>
<tr>
<td>ISDN B channel</td>
<td>InterfaceCode contains “ISDNBCHANNEL”</td>
<td></td>
</tr>
<tr>
<td>ISDN D channel</td>
<td>InterfaceCode contains “ISDNDCCHANNEL”</td>
<td></td>
</tr>
<tr>
<td>Serial</td>
<td>Type contains “Serial” or “FrameRelay”</td>
<td></td>
</tr>
<tr>
<td>FDDI</td>
<td>Type contains “FDDI”</td>
<td></td>
</tr>
<tr>
<td>Backup¹</td>
<td>Type contains “ISDN”</td>
<td></td>
</tr>
<tr>
<td>Dial-On-Demand¹</td>
<td>Type contains “PPP” or “SLIP”</td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>DFM System Defined Groups—Access Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 GB Ethernet</td>
<td>MaxSpeed = “1000000000”</td>
<td>Generic interface/port performance</td>
</tr>
<tr>
<td></td>
<td>Type contains “ETHER” or “CSMACD”</td>
<td>Interface/port flapping</td>
</tr>
<tr>
<td>10/100MB Ethernet</td>
<td>Type contains “ETHER” or “CSMACD”</td>
<td></td>
</tr>
<tr>
<td>ATM</td>
<td>Type contains “ATM”</td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>DFM System Defined Groups—Trunk Ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 GB Ethernet</td>
<td>MaxSpeed = “1000000000”</td>
<td>Generic interface/port performance</td>
</tr>
<tr>
<td></td>
<td>Type contains “ETHER” or “CSMACD”</td>
<td>Interface/port flapping</td>
</tr>
<tr>
<td>10/100MB Ethernet</td>
<td>Type contains “ETHER” or “CSMACD”</td>
<td></td>
</tr>
<tr>
<td>ATM</td>
<td>Type contains “ATM”</td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

1. Dial-On-Demand and Backup interface settings are related. If one interface type is set to active and you change the other interface type from optional to active, the first interface type will be changed to from active to optional.
For additional information, see the following topics:

- Threshold Categories for Devices, Interfaces, and Ports, page 10-31
- Threshold Parameter Values and Events, page 10-40

Threshold Definitions

When you manage thresholds, you must select a device group and a threshold category. Threshold categories contain groups of parameters or thresholds that apply to that category. For the threshold parameters that you can set for each category, see Table 10-8 on page 10-40.

Backup Interface Support

The Backup Interface Support threshold configures an interface as a backup. When an interface is identified as a backup:

- The InterfaceOperationallyDown event is not generated if the interface is down.
- The ExceededMaximumUptime event is generated if the interface stays up too long.

Maximum uptime

The maximum length of time, in seconds, that the interface may be up before the ExceededMaximumUptime event is generated. If the value of this parameter is 0, the ExceededMaximumUptime event is disabled.

Dial-On-Demand Interface Support

The Dial-On-Demand Interface Support threshold identifies an interface as dial-on-demand. In this case:

- The InterfaceOperationallyDown event is not generated if the interface is down.
- The ExceededMaximumUptime event is generated if the interface stays up too long.
Chapter 10  Configuring Polling and Thresholds

Managing Thresholds

Maximum uptime

The maximum length of time that the interface may be up before the ExceededMaximumUptime event is generated. If the value of this parameter is 0, the ExceededMaximumUptime event is disabled.

Environment

The Environment threshold controls the monitoring of the system’s environment.

Relative temperature threshold

Indicates how close the current temperature value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value. For example, if the shutdown temperature is 50°C and the Relative temperature threshold is 10%, the OutofRange event occurs if the temperature exceeds 45°C.

Relative voltage threshold

Indicates how close the current voltage value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value. For example, if the shutdown value is +30V and the Relative voltage threshold is 10%, the OutofRange event occurs if the voltage exceeds +27V.

Generic Interface/Port Performance

The Generic Interface/Port Performance thresholds configure the monitoring of a non-Ethernet network adapter’s performance characteristics. The categories include basic parameters—such as utilization, errors, broadcast, and packet drops—common to all media types.

Broadcast threshold

The upper threshold for broadcast traffic, expressed as a percentage of the total bandwidth.
Managing Thresholds

Collision threshold

The upper threshold for collisions, expressed as a percentage of the total number of output packets. This threshold applies only to Ethernet settings for ports, trunks, and interfaces.

Discard threshold

The upper threshold for dropped packets, expressed as a percentage of the total number of packets.

Error threshold

The upper threshold for packet errors, expressed as a percentage of the total number of packets. DFM generates the HighErrorRate event when both the Error threshold and Error traffic threshold are reached or exceeded.

Error traffic threshold

The upper threshold for packet rate, expressed as a percentage of the total bandwidth. DFM generates the HighErrorRate event when both the Error threshold and Error traffic threshold are reached or exceeded. The value for Error traffic threshold can include up to two decimal places.

Queue drop threshold

The acceptable percentage of packets dropped because of full queues, expressed as a percentage of the total number of packets.

Utilization threshold

The upper threshold for link utilization, expressed as a percentage of the total bandwidth.

DFM uses the DuplexMode special variable to specify duplexity (UNSPECIFIED, by default), and DuplexSource to track the duplexity setting source (NONE by default). (For information on the DuplexMode special variable, refer to Table 8-4 on page 8-23.) DFM uses the following algorithm to determine duplexity:
1. DFM checks the portDuplexity MIB attribute in the CISCO-STACK-MIB, and:
   a. If the value is set to either half duplex or full duplex, DFM uses that setting for DuplexMode and sets DuplexSource to ENTERPRISE_MIB.
   b. If the device is not a Cisco stack switch, the portDuplexity attribute is not present, or the portDuplexity attribute is present but its value is auto/disagree, DFM proceeds to Step 2.

2. DFM checks the dot3StatsDuplexStatus MIB attribute in the ETHERLIKE-MIB, and:
   a. If the value is set to either half duplex or full duplex, DFM uses that setting for DuplexMode and sets DuplexSource to ETHERLIKE_MIB.
   b. If the dot3StatsDuplexStatus attribute is not present, or it is present but its value is unknown, DFM proceeds to Step 3.

3. DFM checks the cdpCacheDuplex MIB attribute in the CISCO-CDP-MIB, and:
   a. If the value is set to either half duplex or full duplex, DFM uses that setting for DuplexMode (for both local and remote ports), and sets DuplexSource to NEIGHBOR_MIB.
   b. If the value is unknown, DFM proceeds to Step 4.

4. If DFM cannot correctly determine the duplex mode (because it was not set manually or set from a MIB), DFM will set DuplexSource to ASSUMED and do the following:
   a. If the interface is a 10 MB Ethernet interface, DFM will assume the setting is half duplex. (DFM considers an interface to be a 10 MB Ethernet when its Type="*ETHER*" and its MaxSpeed=10000000.)
   b. For all other interfaces, DFM will assume the setting is full duplex.
Interface/Port Flapping

The Interface/Port Flapping thresholds control the analysis of network adapters (ports and interfaces) that are continually going up and down, or flapping. Flapping analysis monitors SNMP link down traps to identify a flapping network adapter. DFM reports flapping as a fault condition. For more information, How DFM Calculates Repeated Restarts and Flapping, page F-1.

Link trap threshold

The number of SNMP link down traps that must be received within the Link trap window for DFM to consider the interface or port flapping. A value of 0 disables flapping analysis.

Link trap window

The amount of time used to monitor flapping analysis of a port or interface. If the number of link down traps meets or exceeds the Link trap threshold during this window of time, the interface or port is considered to be flapping.

Processor and Memory

The Processor and Memory thresholds control the performance monitoring of a system's processor and its associated memory elements.

Backplane utilization threshold

The upper threshold for a switch’s backplane utilization, expressed as a percentage of the total backplane bandwidth.

Free memory threshold

The lower threshold for the acceptable amount of free memory, as measured by the ratio of free memory to the total memory.

Memory buffer miss threshold

The upper threshold for the number of buffer misses, expressed as a percentage of the total number of buffer requests.
Chapter 10  Configuring Polling and Thresholds

Managing Thresholds

Memory buffer utilization threshold

The upper threshold for the number of buffers used, expressed as a percentage of the total number of buffers.

Memory fragmentation threshold

The lower threshold for memory fragmentation. The fragmentation value is the ratio of the largest number of contiguous unallocated bytes to the total amount of free memory. For example, a value of 5 indicates that the largest free buffer must be at least 5% of the free memory.

Processor utilization threshold

The upper threshold for processor utilization, expressed as a percentage of the total capacity of the processor.

Reachability

The Reachability thresholds configure the reachability parameters for network adapters (ports and interfaces). They also control the analysis of systems that repeatedly restart, triggering RepeatedRestarts and Flapping events. The following parameters are included in the Reachability Settings threshold category.

Restart trap threshold

The number of SNMP cold or warm start traps that must be received within the amount of time set by the Restart trap window parameter for DFM to consider a system to be performing excessive restarts. A value of 0 disables restart analysis. For more information, see How DFM Calculates Repeated Restarts and Flapping, page F-1

Note

If you want cold and warm start traps to generate events to be displayed immediately in the Alerts and Activities display, set the value of Restart trap threshold to 1.
Managing Thresholds

Restart trap window

The amount of time used to monitor a system's repeated restarts. If the number of start traps meets or exceeds the Restart trap threshold during this window of time, the system is considered to be performing excessive restarts.

The minimum value is 30 seconds, and the maximum value is 3600 seconds.

Threshold Parameter Values and Events

Table 10-8 lists threshold categories, the threshold parameters in each category, minimum and maximum values for the threshold parameters, and the events that DFM generates when values pass the threshold.

Note

Most thresholds are upper thresholds, representing the highest acceptable value. Lower thresholds are the exception and are footnoted as such.

Table 10-8  Minimum and Maximum Threshold Parameter Values and Related Events

<table>
<thead>
<tr>
<th>Threshold Category</th>
<th>Applicable Threshold Parameters (with unit of measure)</th>
<th>Values</th>
<th>Events Generated after Value Passes Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Interface Support</td>
<td>Maximum uptime (seconds)</td>
<td>0</td>
<td>ExceededMaximumUptime</td>
</tr>
<tr>
<td>Dial-on-Demand</td>
<td>Maximum uptime (seconds)</td>
<td>0</td>
<td>ExceededMaximumUptime</td>
</tr>
<tr>
<td>Environment</td>
<td>Relative temperature threshold (%)</td>
<td>0</td>
<td>OutOfRange</td>
</tr>
<tr>
<td></td>
<td>Relative voltage threshold (%)</td>
<td>0</td>
<td>OutOfRange</td>
</tr>
<tr>
<td>Generic Interface/Port Performance</td>
<td>Broadcast threshold (%)</td>
<td>0</td>
<td>HighBroadcastRate</td>
</tr>
<tr>
<td></td>
<td>Collision threshold (%)</td>
<td>0</td>
<td>HighCollisionRate</td>
</tr>
<tr>
<td></td>
<td>Discard threshold (%)</td>
<td>0</td>
<td>HighDiscardRate</td>
</tr>
<tr>
<td></td>
<td>Error threshold (%)</td>
<td>0</td>
<td>HighErrorRate</td>
</tr>
<tr>
<td></td>
<td>Error traffic threshold (%)</td>
<td>0.00</td>
<td>HighErrorRate</td>
</tr>
<tr>
<td></td>
<td>Queue drop threshold (%)</td>
<td>0</td>
<td>HighQueueDropRate</td>
</tr>
<tr>
<td></td>
<td>Utilization threshold (%)</td>
<td>0</td>
<td>HighUtilization</td>
</tr>
</tbody>
</table>
### Table 10-8 Minimum and Maximum Threshold Parameter Values and Related Events (continued)

<table>
<thead>
<tr>
<th>Threshold Category</th>
<th>Applicable Threshold Parameters (with unit of measure)</th>
<th>Values</th>
<th>Events Generated after Value Passes Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface/Port Flapping</td>
<td>Link trap threshold (count)</td>
<td>0-10</td>
<td>RepeatedRestarts</td>
</tr>
<tr>
<td></td>
<td>Link trap window (seconds)</td>
<td>30-3600</td>
<td>Flapping</td>
</tr>
<tr>
<td>Processor and Memory</td>
<td>Backplane utilization threshold (%)</td>
<td>0-100</td>
<td>InsufficientFreeMemory</td>
</tr>
<tr>
<td></td>
<td>Free memory threshold (%)</td>
<td>0-100</td>
<td>HighBackplaneUtilization</td>
</tr>
<tr>
<td></td>
<td>Memory buffer miss threshold (%)</td>
<td>0-100</td>
<td>HighBufferMissRate</td>
</tr>
<tr>
<td></td>
<td>Memory buffer utilization threshold (%)</td>
<td>0-100</td>
<td>HighBufferUtilization</td>
</tr>
<tr>
<td></td>
<td>Memory fragmentation threshold (%)</td>
<td>0-100</td>
<td>ExcessiveFragmentation</td>
</tr>
<tr>
<td></td>
<td>Processor utilization threshold (%)</td>
<td>0-100</td>
<td>HighUtilization</td>
</tr>
<tr>
<td>Reachability</td>
<td>Restart trap threshold (count)</td>
<td>0-10</td>
<td>RepeatedRestarts</td>
</tr>
<tr>
<td></td>
<td>Restart trap window (seconds)</td>
<td>30-3600</td>
<td>Flapping</td>
</tr>
</tbody>
</table>

1. Lower threshold—event is generated when the parameter value is lower than the value you set for it.

For additional information, see the following topics:
- Threshold Categories for Devices, Interfaces, and Ports, page 10-31
- Threshold Definitions, page 10-34
Administering DFM (Advanced)

These topics are intended for system administrators who will perform Device Fault Manager (DFM) administrative functions. The topics include:

- Ports and Protocols that DFM Uses, page 11-1
- Security Considerations, page 11-3
- Device Support, page 11-5
- System Administration, page 11-5

Ports and Protocols that DFM Uses

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port Number</th>
<th>Service Name</th>
<th>Direction (of establishment) of Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td>—</td>
<td>Ping</td>
<td>Server to Device</td>
</tr>
<tr>
<td>UDP</td>
<td>161</td>
<td>Simple Network Management Protocol (SNMP)</td>
<td>Server to Device, Device to Server</td>
</tr>
<tr>
<td>UDP</td>
<td>162</td>
<td>SNMP Traps (Standard Port)—Default port number used by DFM for receiving traps</td>
<td>Server to Device, Device to Server</td>
</tr>
<tr>
<td>UDP</td>
<td>9000</td>
<td>Used for trap receiving</td>
<td>Client to Server</td>
</tr>
</tbody>
</table>


Table 11-1  DFM Ports (continued)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port Number</th>
<th>Service Name</th>
<th>Direction (of establishment) of Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>9002</td>
<td>Used by DFM broker (if port 162 is occupied)</td>
<td>Client to Server</td>
</tr>
<tr>
<td>TCP</td>
<td>49</td>
<td>TACACS+ and ACS</td>
<td>Server to ACS</td>
</tr>
<tr>
<td>TCP</td>
<td>15000</td>
<td>Used by log server</td>
<td>Server internal</td>
</tr>
<tr>
<td>TCP</td>
<td>43445</td>
<td>Used by Fault History database engine (dfmFH)</td>
<td>Server internal</td>
</tr>
<tr>
<td>TCP</td>
<td>43446</td>
<td>Used by inventory service database engine (DFMInv)</td>
<td>Server internal</td>
</tr>
<tr>
<td>TCP</td>
<td>43447</td>
<td>Used by event processing database engine (dfmEPM)</td>
<td>Server internal</td>
</tr>
<tr>
<td>TCP</td>
<td>43500-43520</td>
<td>Used by Common Transport Mechanism for internal application messaging</td>
<td>Server internal</td>
</tr>
</tbody>
</table>

Table 11-2  CiscoWorks Common Services Incoming Ports

<table>
<thead>
<tr>
<th>Port Number/Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>42343/tcp</td>
<td>Jrun</td>
</tr>
<tr>
<td>57860/tcp</td>
<td>JRun Server Manager ControlServer: Used for Jrun Administration</td>
</tr>
<tr>
<td>42344/tcp</td>
<td>ANI HTTP server</td>
</tr>
<tr>
<td>43441–43459</td>
<td>Used as database ports: 43441—Used by CiscoWorks Common Services</td>
</tr>
</tbody>
</table>
Security Considerations

These topics address some important DFM security issues:

- File Ownership and Protection, page 11-3
- Secure Socket Layer (SSL), page 11-3
- SNMPv3, page 11-4
- Working with Firewalls, page 11-4

File Ownership and Protection

Security for DFM files is based on the same standards used for CiscoWorks.

Caution

Do not change the protection of any file or directory to be less restrictive. You may, if you wish, make the protections more restrictive.

All DFM files are installed with owner CASUSER. Only CASUSER can create, delete, or modify the files installed in NMSROOT. NMSROOT is the directory where CiscoWorks is installed on your system. If you selected the default directory during installation, on Windows it is C:\Program Files\CSCOpx. On Solaris, it is /opt/CSCOpx.

Note

File protections are not enforced on FAT partitions.

Secure Socket Layer (SSL)

SSL is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. It relies upon certificates, public keys, and private keys. You can enable or disable SSL depending on the need to use secure access.

DFM supports SSL between clients and the server. By default, DFM is not SSL-enabled. For information on enabling SSL, refer to the Common Services online help.
SNMPv3

Like CiscoWorks Common Services, DFM supports SNMPv3 (authentication and access control but no data encryption) between server and devices to eliminate leakage of confidential info. This provides packet-level security, integrity protection, and replay protection, but does not encrypt the packets.

Working with Firewalls

DFM will work across firewalls, but you must perform the following two tasks:

- Configure the DFM server to use a specific port (outgoing connection)
- Configure the firewall to use an automatic established connection (incoming connection)

**Step 1**

Configure the DfmServer process so it binds to a privileged port, using the pdcmd --port option (see Table 11-6 on page 11-25 for more pdreg options):

a. Check the flags that are currently set for the DfmServer process, and write them down (you will need to reset them later):

   ```
   # NMSROOT/bin/pdreg -l DfmServer
   ```

b. Unregister the DfmServer process:

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

c. Re-register the DfmServer process with all the flags found in Step a and the following sm_server flags, as needed:

   ```
   --port=port  Specifies port (for example, on a firewall) on which DfmServer will run
   --privopen=protocol:port  Specifies privileged port to which DfmServer has access (for example, UDP:162)
   ```
Device Support

When support for new devices becomes available for DFM, Incremental Device Updates (IDUs) will be announced on the planner page for DFM on Cisco.com. Visit the planner page for announcements, downloads, and installation instructions for IDUs as they become available.

When a new IDU becomes available, you can download it from Cisco.com by selecting Products and Solutions > Network Management > CiscoWorks LAN Management Solution > CiscoWorks Device Fault Manager > Software Center. (You will be prompted to log into Cisco.com.)

System Administration

DFM system administration can be performed only by the following types of users:

- Users in a System Administrator role. These users can perform system administration tasks that can be started from the CiscoWorks desktop. These tasks include:
  - Configuring users
  - Backing up and restoring data
  - Configuring logging
  - Starting and stopping CiscoWorks processes

Step 2

Configure the established connection keyword in the firewall to be automatic.

For additional information on using the privopen option, see Example: Configuring the DFM Server to Use a Privileged Port, page 11-28.
• Users who log in as local administrator to the system where DFM is installed. These users can view log files.

If the DFM server is using CiscoSecure Access Control Server (ACS) mode, these CiscoWorks roles are mapped to ACS roles.

Registering Additional DFM Servers with the CiscoWorks Home Page

You can register additional DFM servers so that they appear on the CiscoWorks home page. There is no limit to the number of servers you can register, since device limits are enforced from the DFM server side; the CiscoWorks home page is simply a portal for the different applications. However, you will probably want to limit your home page to two or three DFM servers. The local DFM server name is always listed first on the CiscoWorks home page.

If you have multiple instances of DFM on your home page, you can always map a DFM instance to its Common Services instance by the server hostname (DFM@server, CS@server).

Note
When you use a remote version of DFM, CiscoWorks will prompt you to reauthenticate yourself.

Step 1
From the Common Services home page, select Home Page > Application Registration. The Application Registration Status page appears.

Step 2
Click Registration. The Registration Location page opens.

Step 3
Activate the Import from Other Servers radio button, and click Next. The Import Server’s Attributes page opens.

Step 4
In the Import Server’s Attributes page, enter the following information:

• Server Name—Host name or IP address.
• Server Display Name—A user-specified name that will be displayed on the CiscoWorks home page, and as the DFM home page title when you select that DFM instance.
• Port—1741.
Step 5  Click Next. CiscoWorks verifies that the remote server is reachable.

Step 6  When you select the new DFM server instance from the CiscoWorks home page, you will have to authenticate by entering a user name and password for the remote host.

Configuring Users (ACS and Non-ACS)

The CiscoWorks server provides the mechanism for authenticating and authorizing users for CiscoWorks applications. What users can see and do is determined by their user role. System Administrators can configure user roles by selecting Server > Security > User Management. From here you can add, modify, or delete users.

The CiscoWorks server provides two different mechanisms or modes for authenticating users for CiscoWorks applications:

- CiscoWorks Local Mode—By default, the CiscoWorks server uses CiscoWorks Local mode, or non-ACS mode. In CiscoWorks Local mode, CiscoWorks assigns roles, along with privileges associated with those roles, as described in the Common Services Permission Report. (You can generate a Permission Report from the Common Services home page by selecting Server > Reports > Permission Report and clicking Help.) For more information, refer to Configuring Users Using CiscoWorks Local Mode, page 11-8.

- CiscoSecure Access Control Server (ACS) Mode—ACS specifies the privileges associated with roles; however, ACS also allows you to perform device-based filtering, so that users only see authorized devices. Using ACS, which is called ACS mode, is supported when ACS is installed on your network and DFM is registered with ACS. For more information, refer to Configuring Users Using ACS Mode, page 11-8.

If Common Services is using ACS mode, DFM must also use ACS mode; otherwise, DFM users will not have any permissions. However, if another instance of DFM is already integrated with ACS, the new DFM will also be integrated with ACS.
Configuring Users Using CiscoWorks Local Mode

To add a user and specify their user role using CiscoWorks Local Mode, select Server > Security > User Management from the Common Services home page. Click the Help button for information on the configuration steps.

Use the CiscoWorks Permission Report to understand how each user role relates to tasks in DFM. From the Common Services home page, select Server > Reports > Permission Report and scroll down until you find Device Fault Manager.

Configuring Users Using ACS Mode

To use this mode for DFM, Cisco Secure ACS must be installed on your network, and DFM must be registered with ACS.

---

**Step 1**
Verify which mode the CiscoWorks server is using. From the Common Services home page, select Server > Security and check what is listed in the Current Settings table. Either CiscoWorks Local or TACACS (ACS) will be displayed.

**Step 2**
Verify whether DFM is registered with ACS (if ACS Mode is being used) by checking the ACS server.

**Step 3**
To modify ACS roles:
- Refer to the ACS online help (on the ACS server) for information on modifying roles.
- Refer to the Common Services online help for information on the implications of ACS on the DCR (specifically, role dependencies).

---

**Note**
If you modify DFM roles using ACS, your changes will be propagated to all other instances of DFM that are using Common Services servers which are registered with the same ACS server.
See the following for other information related to ACS:

- To register applications with ACS, and for information on supported ACS versions, refer to Installation and Setup Guide for Device Fault Manager.
- To see which DFM user interfaces are affected by ACS device-based filtering, refer to Device-Based Filtering, page 11-11.
- For information on the implications of ACS custom roles on the DCR, see the online help for Common Services.

### Using DFM in ACS Mode

Before performing any tasks that are mentioned here, you must ensure that you have successfully completed configuring Cisco Secure ACS with the CiscoWorks server. If you have installed DFM after configuring the CiscoWorks Login Module to the ACS mode, then DFM users are not granted any permissions. However, the DFM application is registered to Cisco Secure ACS.

**Note**
The System Identity Setup user that is defined in the CiscoWorks server must be added to the Cisco Secure ACS, and this user must have the Network Administrator privilege.

CiscoWorks login modules allow you to add new users using a source of authentication other than the native CiscoWorks server mechanism (that is, the CiscoWorks Local login module). You can use the Cisco Secure ACS services for this purpose.

The following topics provide information on how to use DFM in the ACS mode:

- Modifying CiscoWorks Roles and Privileges, page 11-11
- Device-Based Filtering, page 11-11
By default, the CiscoWorks server authentication scheme has five roles in the ACS mode. They are listed here from least privileged to most privileged:

<table>
<thead>
<tr>
<th>Role</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help Desk</td>
<td>User with this role has the privileges to access network status information from the persisted data. User does not have the privilege to contact any device or schedule a job that will reach the network. Example: Using the Alerts and Activities display.</td>
</tr>
<tr>
<td>Approver</td>
<td>User with this role has the privilege to approve all DFM tasks. User can also perform all the Help Desk tasks. Example: Searching the Fault History database.</td>
</tr>
<tr>
<td>Network Operator</td>
<td>User with this role has the privilege to perform all tasks that involve collecting data from the network. User does not have write access on the network. User can also perform all the Approver tasks. Example: Configuring logging parameters.</td>
</tr>
<tr>
<td>Network Administrator</td>
<td>User with this role has the privilege to change the network. User can also perform Network Operator tasks. Example: Adding devices to DFM from the DCR.</td>
</tr>
<tr>
<td>System Administrator</td>
<td>User with this role has the privilege to perform all CiscoWorks system administration tasks. See the Permission Report on CiscoWorks server (Common Services &gt; Server &gt; Reports &gt; Permission Report). Example: Changing device polling from suspended to resumed (Configuration &gt; Polling and Thresholds &gt; Apply Changes).</td>
</tr>
</tbody>
</table>

Cisco Secure ACS allows you to modify the privileges to these roles. You can also create custom roles and privileges that help you customize Common Services client applications to best suit your business workflow and needs.
To modify the default CiscoWorks privileges, see Cisco Secure ACS online help. (On Cisco Secure ACS, click Online Documentation > Shared Profile Components > Command Authorization Sets.)

Note See the Common Services online help for important information on how ACS custom roles affect the DCR.

Modifying CiscoWorks Roles and Privileges

If another instance of DFM is registered with the same Cisco Secure ACS, your instance of DFM will inherit those role settings. Furthermore, any changes you make to DFM roles will be propagated to other instances of DFM through Cisco Secure ACS. If you reinstall DFM, your Cisco Secure ACS settings will automatically be applied upon DFM restart.

Step 1 Select Shared Profile Components > DFM and click on the DFM roles that you want to modify.
Step 2 Select or deselect any of the DFM tasks that suit your business workflow and needs.
Step 3 Click Submit.

Device-Based Filtering

You can configure ACS to restrict access to all DFM displays. However, device-based filtering can only be performed on the following DFM displays:

Note ACS does not perform any filtering on VLANs.

- Alerts and Activities—All displays.
- Device Management—All displays.
- Notification Services > Notification Groups. (If ACS filtering is changed, Notification Services will not update running notifications.)
• Fault History > Alert Filtering > Search by Device
  Fault History > Alert Filtering > Search by Group
  Fault History > Event Filtering > Search by Device
  Fault History > Event Filtering > Search by Group

• Configuration > Polling and Thresholds: Only the Polling Parameters
  Summary and the Thresholds Parameters Summary pages are filtered.

• Configuration > Other Configurations > Group Administration—All
  displays.

  Note: If any user starts the rediscovery process, all devices managed by DFM
  are rediscovered (not just those for which the user has access).

Most of the DFM tasks are device-centric. The devices listed for you while
performing the DFM tasks are based on your role and associated privileges,
defined in Cisco Secure ACS.

  Note: Refer to the Common Services online help for important information on how ACS
custom roles affect the DCR and device-based filtering.

**Creating Self-Signed Security Certificates Yearly**

When you install DFM, DFM creates a self-signed security certificate on the
server. Users on some client systems must install the certificate; see Responding
to Security Alerts, page 2-12. Self-signed security certificates expire one year
from the date of creation.

Create a new self-signed security certificate yearly, before the certificate expires.
You can also do so after the certificate expires; however, users might not be able
to access DFM until you complete this task.
Step 1  From the Common Services home page, select **Server > Security > Self Signed Certificates**. The Create Certificates page appears.

Step 2  Enter the values for the fields described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country Name</td>
<td>Name of your country</td>
<td>Use two-character country code.</td>
</tr>
<tr>
<td>State or Province</td>
<td>Name of your state or province</td>
<td>Use two-character state or province code or complete name of state or province.</td>
</tr>
<tr>
<td>Locality</td>
<td>Name of your city or town</td>
<td>Use two-character city or town code or complete name of city or town.</td>
</tr>
<tr>
<td>Organization Name</td>
<td>Name of your organization</td>
<td>Use complete name or abbreviation for your organization.</td>
</tr>
<tr>
<td>Organization Unit Name</td>
<td>Name of department in your organization</td>
<td>Use complete name or abbreviation for your department.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Name of server on which DFM is installed</td>
<td>Use the DNS name of the server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Use the proper domain name, which should already be displayed in the Host Name field.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Your e-mail address</td>
<td>—</td>
</tr>
</tbody>
</table>

Step 3  Click **Apply**.
Back up and Restore DFM Data

Use the Common Services home page to perform immediate backups or schedule backups of DFM data. Common Services provides a command line script that restores data, including data from previous versions of Common Services and DFM.

- For backing up data, select Server > Admin > Backup, click Help, and follow the instructions.
- For restoring data, select Server > Admin > Backup, click Help, and click the Help link to the Restoring Data topic.

If you are restoring data from DFM 1.2.x or earlier, you will see a warning message and should follow the instructions in the message.

---

**Step 1**  On the DFM 1.2.x or earlier server, run the following command on Solaris. (NMSROOT is the folder where DFM is installed on the server. If you selected the default directory during installation, it is C:\Program Files\CSCOpx on Windows and /opt/CSCOpx on Solaris.)

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

Run this command on Windows:

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

**Step 2**  Copy seedfile.txt to a temporary location on your upgraded server.

**Step 3**  Use the CiscoWorks pdshow command to verify that the daemon manager is running (cmdmgtd on Windows and dmgtd on Solaris).

**Step 4**  Import the DFM 1.2.x or earlier information, using this command on Solaris:

```
NMSROOT/bin/dfmimport fn=fullpath/seedfile.txt
```

Run this command on Windows:

```
NMSROOT\bin\dfmimport.exe fn=fullpath\seedfile.txt
```
Database files are stored using the backup directory structure described in Table 11-3.
- Format—/generation_number/suite/directory/filename
- Example—/1/dfm/dfmFh.db

**Table 11-3  DFM Backup Directory Structure**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>generationNumber</td>
<td>Backup number</td>
<td>For example, 1, 2, and 3, with 3 being the latest database backup.</td>
</tr>
<tr>
<td>suite</td>
<td>Application, function, or module</td>
<td>When you perform a backup, data for all suites is backed up. The CiscoWorks Common Services suite is cmf. The DFM application suite is dfm.</td>
</tr>
<tr>
<td>directory</td>
<td>What is being stored</td>
<td>Suite applications (if applicable).</td>
</tr>
</tbody>
</table>
| filename   | Specific file that has been backed up | Files include database (.db), log (.log), version (DbVersion.txt), manifest (.txt), tar (.tar), and data files (datafiles.txt). For DFM, the following files are listed directly under generationNumber/suite:
dfmEpm.db
dfmInv.db
dfmFh.db
filebackup.tar
The file backup.tar contains the following directories and file:

```
NMSROOT/objects/smarts/conf
NMSROOT/objects/smarts/local/repos
NMSROOT/objects/smarts/local/logs
NMSROOT/objects/smarts/local/conf
NMSROOT/setup/dfm.info
```
Changing the Password for DFM Databases

Before You Begin
The procedure in this topic enables you to change the password for the following DFM databases. All DFM databases must use the same password.

- dfmEpm—Event promulgation
- dfmFh—Fault History
- dfmInv—Inventory

Step 1
At the command prompt on the DFM server, stop the daemon manager by entering the following command:

- On Windows:
  net stop crmdmgmt
- On Solaris:
  /etc/init.d/dmgtd stop

Step 2
Change directory to \NMSROOT\conf\dfmDb\bin. For example, on Windows:

cd Program Files\CSCOpx\conf\dfmDb\bin

On Solaris:

cd /opt/CSCOpx/conf/dfmDb/bin

Note
\NMSROOT is the folder where DFM is installed on the server. If you selected the default directory during installation, it is C:\Program Files\CSCOpx on Windows and /opt/CSCOpx on Solaris.
Step 3  Enter ChangeDfmDbPasswd.pl, providing a new password as input. For example:

```
ChangeDfmDbPasswd.pl newpassword
```

Step 4  Restart the daemon manager by entering the following command:

- On Windows:
  
  ```
  net start crmdmgmt
  ```

- On Solaris:
  
  ```
  /etc/init.d/dmgtd stop
  ```

### Configuring Logging

DFM writes application log files for all major functional modules. By default, DFM writes only error and fatal messages to these log files; DFM saves the previous three logs as backups. You cannot disable logging. However, you can:

- Collect more data when needed by increasing the logging level
- Return to the default logging level as the norm

This task can be performed by a user logged in to DFM in any of the following roles:

- System Administrator
- Network Administrator
- Network Operator

Step 1  From the DFM home page, select **Configuration > Logging**. The Logging: Level Configuration page is displayed.

**Note**  You cannot disable logging. DFM will always write error and fatal messages to application log files.

Step 2  For each DFM functional module, the Error check box is always selected; you cannot deselect it.
To set all modules to Error, the default logging level:

a. Click the **Default** button. A confirmation page is displayed.

b. Click **OK**.

To change the logging level for individual modules:

a. For each module that you want to change, select one (or deselect all) of the following logging levels:
   
   - **Warning**—Log error messages and warning messages
   - **Informational**—Log error, warning, and informational messages
   - **Debug**—Log error, warning, informational, and debug messages

   **Note**  
   Deselecting all check boxes for a module returns it to Error, the default logging level.

b. Review your changes. To cancel your changes, click the **Cancel** button. Otherwise, click the **Apply** button. Clicking the **Apply** button starts immediately resetting the changed logging levels for the DFM functional modules.

---

**Viewing and Maintaining Log Files**

Each DFM module writes log files to its own folder within the `NMSROOT/log/dfmLogs` folder. **Table 11-4** lists each DFM module, the name of the folder where the log files are stored, the related log files, the maximum log size, and the number of backup logs that are saved.

**Note**  
NMSROOT is the folder where DFM is installed on the server. If you selected the default directory during installation, it is C:\Program Files\CSCOpx. On Solaris it is /opt/CSCOpx.
When a log file reaches its maximum size, the module backs up the file and starts writing to a new log file. The module appends a number to the backup file, until it reaches the maximum allowed backups. In the following example, the oldest file is TISServer.log.2, and TISServer.log is the current log file.

<table>
<thead>
<tr>
<th>Time</th>
<th>Size</th>
<th>Log File</th>
</tr>
</thead>
<tbody>
<tr>
<td>02:42 PM</td>
<td>4,481,607</td>
<td>TISServer.log</td>
</tr>
<tr>
<td>10:22 AM</td>
<td>5,120,447</td>
<td>TISServer.log.1</td>
</tr>
<tr>
<td>03:17 AM</td>
<td>5,120,105</td>
<td>TISServer.log.2</td>
</tr>
</tbody>
</table>

By default, DFM writes error messages only to log files. You can change the logging level and thereby affect the amount of information stored in log files. To do so, see Configuring Logging, page 11-17.

### Table 11-4 DFM Log Files by Module

<table>
<thead>
<tr>
<th>Function/Module</th>
<th>Folder in NMSROOTlog\dfmLogs</th>
<th>Log Files</th>
<th>Maximum Size (KB)</th>
<th>No. of Backup Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerts and Activities Display</td>
<td>AAD</td>
<td>AAD.log</td>
<td>1000</td>
<td>3</td>
</tr>
<tr>
<td>Inventory Interactor</td>
<td>cfi</td>
<td>Interactor.log</td>
<td>1000</td>
<td>5</td>
</tr>
<tr>
<td>Inventory Collector</td>
<td>cfi</td>
<td>InventoryCollector.log</td>
<td>35000</td>
<td>5</td>
</tr>
<tr>
<td>Polling and Threshold Adapter</td>
<td>cfi</td>
<td>PollingThresholdAdapter.log</td>
<td>10000</td>
<td>5</td>
</tr>
<tr>
<td>Detailed Device View</td>
<td>DDV</td>
<td>DDV.log</td>
<td>1000</td>
<td>2</td>
</tr>
<tr>
<td>Daily Purging Schedule</td>
<td>DPS</td>
<td>DPS.log</td>
<td>100</td>
<td>2</td>
</tr>
<tr>
<td>Event Processing Adapters</td>
<td>epa</td>
<td>adapterServer.log</td>
<td>1000</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>dfmEvents.log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Promulgation Module</td>
<td>EPM</td>
<td>EPM.log</td>
<td>15000</td>
<td>5</td>
</tr>
<tr>
<td>Fault History</td>
<td>FH</td>
<td>FHCollector.log</td>
<td>1000</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FHUI.log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logging Services</td>
<td>LogService</td>
<td>DfmLogService.log</td>
<td>500</td>
<td>2</td>
</tr>
<tr>
<td>Processes with multiple threads</td>
<td>LogService</td>
<td>MultiProcLogger.log</td>
<td>10000</td>
<td>5</td>
</tr>
</tbody>
</table>
### Table 11-4  DFM Log Files by Module (continued)

<table>
<thead>
<tr>
<th>Function/Module</th>
<th>Folder in NMSROOT\log\dfmLogs</th>
<th>Log Files</th>
<th>Maximum Size (KB)</th>
<th>No. of Backup Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>License (device limit)</td>
<td>license</td>
<td>licenseCheck.log</td>
<td>100</td>
<td>2</td>
</tr>
<tr>
<td>Notification Services</td>
<td>NOS</td>
<td>nos.log</td>
<td>5000</td>
<td>2</td>
</tr>
<tr>
<td>Polling and Threshold Manager</td>
<td>PTM</td>
<td>PTMClient.log</td>
<td>1000</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PTMServer.log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Polling and Threshold Manager (database)</td>
<td>PTM</td>
<td>PTMDB.log</td>
<td>1000</td>
<td>5</td>
</tr>
<tr>
<td>Polling and Threshold Manager (grouping services)</td>
<td>PTM</td>
<td>PTMOGS.log</td>
<td>1000</td>
<td>5</td>
</tr>
<tr>
<td>Polling and Threshold Manager (Polling and Threshold Adapter)</td>
<td>PTM</td>
<td>PTMPTA.log</td>
<td>1000</td>
<td>5</td>
</tr>
<tr>
<td>Rediscovery Schedule</td>
<td>Rediscovery</td>
<td>Rediscovery.log</td>
<td>100</td>
<td>2</td>
</tr>
<tr>
<td>Device and Credentials Repository Adapter</td>
<td>TIS</td>
<td>DCRAdapter.log</td>
<td>1000</td>
<td>2</td>
</tr>
<tr>
<td>Device Management</td>
<td>TIS</td>
<td>DeviceManagement.log</td>
<td>1000</td>
<td>2</td>
</tr>
<tr>
<td>Inventory Service</td>
<td>TIS</td>
<td>TIServer.log</td>
<td>1000</td>
<td>2</td>
</tr>
<tr>
<td>View Group Management</td>
<td>VGM</td>
<td>vgm.log</td>
<td>1000</td>
<td>3</td>
</tr>
</tbody>
</table>
Starting and Stopping DFM Processes

Note
You cannot stop or unregister a process if any process that depends on it is running. You must first stop or unregister all dependent processes, and then stop or unregister the process.

Step 1
Log in to DFM as a system administrator.

Step 2

Note
If a process is not listed, it has not yet been started.

Step 3
On the Stop Process page, locate the process you want to stop in the Process list.

Step 4
Select the process you want to stop and click the Finish button.

Step 5

Step 6
On the Start Process page, locate the process you want to start in the Process list.

Step 7
Select the process you want to start and click the Finish button.

Table 11-5 provides a complete list of DFM-related CiscoWorks processes. Logs for most of these processes are provided in Table 11-4 on page 11-19.

Table 11-5  DFM-Related CiscoWorks Processes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Dependency</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdapterServer</td>
<td>Event adapter takes events from backend servers.</td>
<td>None</td>
</tr>
<tr>
<td>DataPurge</td>
<td>Data Purge—Starts as scheduled in the GUI and purges the Fault History database.</td>
<td>jrm</td>
</tr>
</tbody>
</table>
DfmBroker

DFM Broker maintains a registry about DFM domain managers, which register the following information with the broker when its initialization is complete:
- Application name of the domain manager
- Hostname where the domain manager is running
- TCP port at which the HTTP server is listening

When a client needs to connect to the domain manager, it first connects to the broker to determine the hostname and TCP port where that server’s HTTP service is listening. It then disconnects from the broker and establishes a connection to the domain manager.

The DfmBroker log file is located at NMSROOT/objects/smarts/local/logs/brstart.log.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Dependency</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFMLogServer</td>
<td>Controls DFM logs.</td>
<td>None</td>
</tr>
<tr>
<td>DFMMultiProcLogger</td>
<td>Handles processes with multiple threads.</td>
<td>None</td>
</tr>
<tr>
<td>DFMOGSServer</td>
<td>DFM Object Grouping Service Server evaluates group membership.</td>
<td>CmfDbEngine, ESS</td>
</tr>
<tr>
<td>DfmServer</td>
<td>Infrastructure device domain manager, a program that provides backend services for DFM. Services include SNMP data retrieval and event analysis. The DfmServer log is NMSROOT/objects/smarts/logs/DFM.log.</td>
<td>DfmBroker</td>
</tr>
<tr>
<td>DFMCTMStartup</td>
<td>Handles interprocess communication.</td>
<td>None</td>
</tr>
<tr>
<td>EPM DbEngine</td>
<td>Event Promulgation Module (EPM) database engine—Repository for the EPM module.</td>
<td>None</td>
</tr>
<tr>
<td>EPM DbMonitor</td>
<td>EPM database monitor.</td>
<td>EPMDbEngine</td>
</tr>
<tr>
<td>EPMServer</td>
<td>Sends events to notification services.</td>
<td>EPMDbEngine</td>
</tr>
</tbody>
</table>

Table 11-5  DFM-Related CiscoWorks Processes (continued)
## Table 11-5  DFM-Related CiscoWorks Processes (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Dependency</th>
</tr>
</thead>
<tbody>
<tr>
<td>FHDbEngine</td>
<td>Fault History database engine—Repository for alerts and events.</td>
<td>None</td>
</tr>
<tr>
<td>FHDbMonitor</td>
<td>Fault History database monitor.</td>
<td>FHDbEngine</td>
</tr>
<tr>
<td>FHpurgeTask</td>
<td>Fault History purge task.</td>
<td>None</td>
</tr>
<tr>
<td>FHServer</td>
<td>Fault History server, a program that runs backend services for Fault History.</td>
<td>EPMServer, EPMDbEngine, FHDBEngine, FHDbMonitor</td>
</tr>
<tr>
<td>Interactor</td>
<td>Provides inventory and device information to the Detailed Device View (DDV); updates the DDV with events.</td>
<td>InventoryCollector</td>
</tr>
<tr>
<td>InventoryCollector</td>
<td>Synchronizes voice device inventory with infrastructure device inventory. Handles all inventory events, such as adding and deleting devices.</td>
<td>ESS, TISServer, DFMOGSServer</td>
</tr>
<tr>
<td>INVDbEngine</td>
<td>Inventory database engine—Repository for devices.</td>
<td>None</td>
</tr>
<tr>
<td>INVDbMonitor</td>
<td>Inventory database monitor.</td>
<td>INVDbEngine</td>
</tr>
<tr>
<td>NOSServer</td>
<td>Notification Server monitors alerts and sends notifications based on subscriptions.</td>
<td>EPMDbEngine, EPMServer, INVDbEngine, DFMOGSServer</td>
</tr>
<tr>
<td>PTMServer</td>
<td>Polling and thresholds server.</td>
<td>DFMOGSServer</td>
</tr>
<tr>
<td>TISServer</td>
<td>Inventory server.</td>
<td>EssMonitor, INVDbEngine</td>
</tr>
</tbody>
</table>
Registering and Unregistering DFM Processes

You can use pdcmd to manually unregister and reregister DFM processes with the CiscoWorks daemon manager. This is useful when you want to do any of the following:

- Specify clients that can connect to DFM.
- Configure adapters to restart automatically whenever the DFM server stops and restarts.
- Configure the DFM server to use a privileged port.

Because these commands are complex, be sure to refer to the examples in these sections:

- Example: Specifying Clients That Can Connect to DFM, page 11-27
- Example: Configuring the DFM Server to Use a Privileged Port, page 11-28

Before registering a process, you must unregister the related processes in this order:

1. Unregister any processes that depend on the DfmServer process.
2. Unregister the DfmServer process.
3. Unregister the DfmBroker process.

Use the following syntax when unregistering DFM processes (for Windows, the command is pdcmd.exe):

```
NMSROOT/bin/pdcmd -u process
```

When you reregister the process, specify all options in the same command instance. If you enter the pdcmd multiple times, only the last instance is used. Register the processes in the following order:

1. Register the DfmBroker process.
2. Register the DfmServer process.
3. Register any processes that depend on DfmServer.

Use the following syntax to reregister the DFM processes. (Refer to Table 11-6 for information about the options and arguments).

```
NMSROOT/bin/pdcmd -r DfmBroker -e path -f arguments
NMSROOT/bin/pdcmd -r DfmServer -e path -d depends -f arguments
NMSROOT/bin/pdcmd -r dependent_process -d DfmServer
```
### Note
To view the default settings for a process, enter

```
NMSROOT/bin/pdreg -l process.
```

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and Arguments</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-u process</code></td>
<td>Unregister <em>process</em>. The processes are listed in Table 11-5 on page 11-21.</td>
</tr>
<tr>
<td><code>-r process</code></td>
<td>Register <em>process</em> to CiscoWorks daemon manager and start <em>process</em> whenever the dependent (parent) process starts (as described in the <code>-d depends</code> option). The processes are listed in Table 11-5 on page 11-21.</td>
</tr>
<tr>
<td><code>-e path</code></td>
<td>Process binary path. <em>path</em> should be:</td>
</tr>
<tr>
<td></td>
<td>• DFM broker: <code>NMSROOT/objects/smarts/bin/brstart</code></td>
</tr>
<tr>
<td></td>
<td>• DFM server: <code>NMSROOT/objects/smarts/bin/sm_server</code></td>
</tr>
<tr>
<td><code>-d depends</code></td>
<td>Process dependency. For DfmServer, <em>depends</em> should be DfmBroker.</td>
</tr>
</tbody>
</table>
### Table 11-6 Options to `pdcmd` (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and Arguments</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-f &quot;arguments&quot;</code></td>
<td>DFM-specific arguments, enclosed in one set of quotes. <code>arguments</code> can be the following:</td>
</tr>
<tr>
<td></td>
<td>--accept <code>host1,host2...</code> (Optional.) Comma-separated list of hostnames or IP addresses specifying clients which can connect to the server. (The DFM server does not use reverse lookups to determine names of connecting host. If you specify clients as hostnames, be sure the hostname is in DNS, especially if you are using DHCP. If you want to specify localhost, use the host name or IP address, not <code>localhost</code>; refer to the “Example: Specifying Clients That Can Connect to DFM” section on page 11-27.)</td>
</tr>
</tbody>
</table>
|                | --privopen=`open-list` (Optional.) Specify the privileged ports and protocol which DfmBroker or DfmServer may open (see Working with Firewalls, page 11-4, for an example). `open-list` can be comma-separated list of the following (IP:protocol is always required): TCP:`port`, UDP:`port`, IP:`protocol`  
The defaults for `open-list` depend on whether DFM is using a reserved port:                                                                                     |
|                | --privopen=IP:`1` Default if reserved port is not being used.                                                                                             |
|                | --privopen=IP:`1`, UDP:`reserved_port` Default if reserved port is being used (normally 162).                                                             |
|                | --output=`file` (Required.) Name of process output file. For DfmServer, `file` should be DFM.                                                                |
|                | --port=`port` (DfmBroker only.) DFM broker port. `port` should always be 9002.                                                                            |
|                | --restore=`file` (DfmBroker only.) Restore broker state from backup file. `file` should always be:                                                        |
|                | --restore=NMSROOT/objects/smarts/conf/broker.rps                                                                                                        |
| `-n`           | Do not restart process when DfmServer is stopped and restarted.                                                                                        |
Example: Specifying Clients That Can Connect to DFM

This example shows how to configure DFM to only accept client connections from the hostnames lucy and ethel. In this case you must unregister and reregister the DFM broker, server, and notification adapter processes.

Note

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

Step 1

Unregister the processes.

a. Unregister the DFM notification adapters:

# NMSROOT/bin/pdcm -u DfmFileNotifier
# NMSROOT/bin/pdcm -u DfmMailNotifier
# NMSROOT/bin/pdcm -u DfmTrapNotifier

b. Unregister the DFM server process:

# NMSROOT/bin/pdcm -u DfmServer

c. Unregister the DFM broker process:

# NMSROOT/bin/pdcm -u DfmBroker

Step 2

Re-register the processes, specifying the clients that can connect to the broker and server:

a. For the DFM broker (the following command is one line):

# NMSROOT/bin/pdcm -r DfmBroker -e NMSROOT/objects/smarts/bin/brstart -f "--output --port=9002 --accept=lucy,ethel --restore=NMSROOT/objects/smarts/conf/broker.rps"
b. For the DFM server (the following command is one line):

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

**Note** When specifying other options (such as --privopen) for DfmServer, use one pdcmd instance. See the “Example: Configuring the DFM Server to Use a Privileged Port” section on page 11-28.

c. For DFM notification adapters (the following commands are each one line):

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

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

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

---

**Example: Configuring the DFM Server to Use a Privileged Port**

This example shows how to configure DFM to use a privileged port.

**Step 1** Unregister any processes that depend on the DfmServer (such as the notification adapters).

```bash
# NMSROOT/bin/pdcmd -u DfmFileNotifier
# NMSROOT/bin/pdcmd -u DfmMailNotifier
# NMSROOT/bin/pdcmd -u DfmTrapNotifier
```

**Step 2** Unregister the DfmServer process:

```bash
# NMSROOT/bin/pdcmd -u DfmServer
```

**Step 3** Re-register the DfmServer process to use UDP port 162 and the IP protocol 1:

```bash
# NMSROOT/bin/pdcmd -r DfmServer -e NMSROOT/objects/smarts/bin/sm_server -d DfmBroker -f 
"--bootstrap=DFM_bootstrap.conf --privopen=IP:1,UDP:162 --output --name=DFM"
```
Step 4  Reregister any processes that depend on DfmServer:

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

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

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

If you also want DFM to accept only specific client connections, you must specify the --accept option when registering the DfmServer process (you do not have to do this for the adapter processes). The following example registers the DfmServer process to use UDP port 162 and IP protocol 1, and specifies that DFM can accept connections from hostnames lucy and ethel:

```
# NMSROOT/bin/pdcmd -r DfmServer -e NMSROOT/objects/smarts/bin/sm_server -d DfmBroker -f
"--bootstrap=DFM_bootstrap.conf --accept=lucy,ethel --privopen=IP:1,UDP:162 --output --name=DFM"
```
PART 3

DFM Reference
Device Fault Manager (DFM) polls certain MIBs for information that is relevant to fault management. Polling is done based on the polling interval, as described in Configuring Polling and Thresholds, page 10-1. Obtaining MIB information depends on several contingencies—namely, whether a device supports a MIB, has the proper SNMP implementation, is accessible, and so forth.

DFM polls the following MIBs:

- ALTIGA-HARDWARE-STATS-MIB
- CISCO-CONENT-ENGINE-MIB
- CISCO-ENVMON-MIB
- CISCO-FC-FE-MIB
- CISCO-FLASH-MIB
- CISCO-FRAME-RELAY-MIB
- CISCO-ISDN-MIB
- CISCO-LS1010-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-METRO-PHY-MIB
- CISCO-PAGP-MIB
- CISCO-PROCESS-MIB
- CISCO-RHINO-MIB
- CISCO-STACK-MIB
- CISCO-SYSTEM-EXT-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VOICE-APPS-MIB
- CISCO-VTP-MIB
- CPQSIINFO-MIB
- CPQHLTH-MIB
- CPQHOST-MIB
- CPQNIC-MIB
- CPQSM2-MIB
- ENTITY-MIB
- ENTITY-FRU-CONTROL-MIB
- ETHERLIKE-MIB
- HOST-RESOURCES-MIB (RFC 1514)
- UMSASSETID-MIB
- UMSEVENT-MIB
- UMSLMSENSOR-MIB
- IF-MIB (RFC 1493)
- IF-MIB (RFC 1573)
- MIB-II (RFC 1213)
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-CPU-MIB
- OLD-CISCO-ENV-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-MEMORY-MIB
- OLD-CISCO-MEMORY-POOL-MIB
- OLD-CISCO-SYSTEM-MIB
- SYS-APPL-MIB
- UMSEVENT-MIB
Processed and Pass-Through Traps, and Unidentified Traps and Events

For some SNMP traps, Device Fault Manager (DFM) either processes them or treats them as pass-through traps. These traps, and how DFM treats them, are described in these topics:

- Processed SNMP Traps, page B-1
- Pass-Through SNMP Unidentified Traps, page B-3
- Unidentifed Traps, page B-5

**Processed SNMP Traps**

When DFM receives certain SNMP traps, it analyzes the data found in the following fields of each SNMP trap message, and changes the property value of the object property (if required):

- Enterprise (the sysObjectID of the agent/object)
- Generic Trap Identifier
- Specific Trap Identifier
Appendix B  Processed and Pass-Through Traps, and Unidentified Traps and Events

**Processed SNMP Traps**

- Variable-Bindings
- IP address of the SNMP agent

**Note**

Use Notification Services to forward specific traps to e-mail recipients or host machines. See Using Notification Services, page 5-1

All processed traps are forwarded in V1 format.

### Processed Standard SNMP Traps (RFC 1215)

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding DFM Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cold Start</td>
<td>RepeatedRestarts</td>
</tr>
<tr>
<td>Warm Start</td>
<td></td>
</tr>
<tr>
<td>Link Up</td>
<td>Flapping</td>
</tr>
<tr>
<td>Link Down</td>
<td></td>
</tr>
</tbody>
</table>

### Processed CISCO-STACK-MIB Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding DFM Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module Up</td>
<td>CardDown</td>
</tr>
<tr>
<td>Module Down</td>
<td></td>
</tr>
</tbody>
</table>

### Processed CISCO-ISDN-MIB Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding DFM Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>demandNbrLayer2Change</td>
<td>OperationallyDown</td>
</tr>
</tbody>
</table>
Appendix B: Processed and Pass-Through Traps, and Unidentified Traps and Events

**Pass-Through SNMP Unidentified Traps**

Pass-through traps are traps that DFM receives from devices that are not in the DFM inventory. These traps are shown in the Alerts and Activities display because of their relevance to fault monitoring. Pass-through traps are displayed as follows:

- As one of the following events:
  - InformAlarm
  - MinorAlarm
  - MajorAlarm
- With the device type and the device name from which it was generated

If DFM does not know which device generated the trap, it ignores the trap.

**Pass-Through Standard SNMP Traps (RFC 1215)**

- Authentication Failure

**Pass-Through CISCO-STACK-MIB Traps**

- lerAlarmOn
- lerAlarmOff
- ipPermitDeniedTrap
- sysConfigChangeTrap

**Pass-Through STP Traps**

- STPnewRoot
- STPtopologyChange

---

**Processed CISCO-ENTITY-FRU-CONTROL-MIB Trap**

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding DFM Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>cefcModuleStatusChange</td>
<td>OperationallyDown</td>
</tr>
</tbody>
</table>
Pass-Through SNMP Unidentified Traps

Pass-Through Repeater MIB Traps

- rptrHealth
- rptrGroupChange
- rptrResetEvent

Pass-Through CISCO-RHINO-MIB Traps

- ciscoLS1010ChassisFailureNotification
- ciscoLS1010ChassisChangeNotification

Pass-Through CISCO-VTP-MIB Traps

- vtpConfigRevNumberError
- rvtpConfigDigestError
- vtpServerDisabled
- vtpMtuTooBig
- vtpVlanRingNumberConfigConflict
- vtpVersionOneDeviceDetected
- vlanTrunkPortDynamicStatusChange

Pass-Through CISCO-ENVMON-MIB Traps

- ciscoEnvMonShutdownNotification

Pass-Through CISCO-VLAN-MEMBERSHIP-MIB Traps

- vmVmpsChange

Pass-Through CISCO-ACCESS-ENVMON-MIB Traps

- caemTemperatureNotification
- caemVoltageNotification
Appendix B      Processed and Pass-Through Traps, and Unidentified Traps and Events

Unidentified Traps

Pass-Through CISCO-CONFIG-MAN-MIB Traps

- ciscoConfigManEvent

Pass-Through CISCO-ENTITY-FRU-CONTROL-MIB Traps

- cevFan15540FTMP
- cevPortTransparent
- cevPortWave

Pass-Through CISCO-CONTENT-ENGINE-MIB Traps

- ciscoContentEngineWriteTransFailed
- ciscoContentEngineOverloadBypass

Pass-Through CISCO-DEVICE-EXCEPTION-REPORTING-MIB Traps

Note

The following pass-through trap is reported only if you have downloaded and installed DFM 2.0 Service Pack 2 (or later) from the DFM download site: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm.

- cderMonitoredExceptionEvent

Unidentified Traps

DFM may display an event as an Unidentified Trap. Normally an Unidentified Trap is reported when an event occurs on a device that is being discovered by DFM. You can get more information on an Unidentified Trap by looking at its Events page.
The CISCO-EPM-NOTIFICATION-MIB specifies the trap message format Device Fault Manager (DFM) uses to generate SNMP traps when an alert occurs. The trap includes the attributes of the alert and the events that caused the alert.

This topic includes the following information:
- MIB Definition, page C-1
- cenAlarmEntry Object-Type—Definitions for Selected Attributes, page C-23


**MIB Definition**

CISCO-EPM-NOTIFICATION-MIB DEFINITIONS ::= BEGIN

IMPORTS

MODULE-IDENTITY, NOTIFICATION-TYPE, Integer32, Unsigned32, OBJECT-TYPE FROM SNMPv2-SMI

MODULE-COMPLIANCE, NOTIFICATION-GROUP, OBJECT-GROUP FROM SNMPv2-CONF

TimeStamp FROM SNMPv2-TC

SnmpAdminString FROM SNMP-FRAMEWORK-MIB

InetAddressType, InetAddress FROM INET-ADDRESS-MIB

ciscoMgmt FROM CISCO-SMI

;
ciscoEpmNotificationMIB MODULE-IDENTITY
LAST-UPDATED "200406070000Z"
ORGANIZATION "Cisco Systems, Inc."
CONTACT-INFO "Cisco Systems
Customer Service
Postal: 170 W Tasman Drive
San Jose, CA 95134
Tel: +1 800 553-NETS
E-mail: tac@cisco.com"
DESCRIPTION
"Notifications directly from hardware and software and processed
notifications from various management applications can be further
processed and forwarded by still other management applications to
indicate the status of devices and software (managed objects).
The status of these managed objects can be reported by traps.

The CISCO-EPM-NOTIFICATION-MIB contains the trap structure which
carries the identity and status info of the managed object as
analyzed by such an event processor. It is not possible for
receivers of these traps to query the mib objects.

A unique but optional feature of the application generating the
trap defined in this mib is the ability to contain multiple
partitions in the same system running the application. A
'Partition' is a logical grouping of a set of managed devices.
These devices can belong to only one partition at any given
time. The trap structure will contain information on the exact
partition number and the partition name of the device where it
resides.

The need for trap generation is to enable multiple management
applications in the network to have a consolidated view of the
whole network of Cisco and non-Cisco devices."

REVISION "200406070000Z"
DESCRIPTION
"Updated the cenAlarmEntry to include new attributes. The new
attributes carries information that adds more value to the
already
existing trap structure.

The Management application computes events for a device via
polling snmp mib objects on the device and/or by listening to
SNMP Traps. Multiple events on a single device roll up into what
is called an Alert - there can be only one alert for a given device at any given time. The objects contained in the cenAlarmEntry are the same for both Alert and Event based notification. The attribute cenAlarmMode added in this revision of the mib can be used to distinguish between the Alert based and event based notification.

In case of event based notification, the cenAlertID would contain the alert id, as computed by the management system, to which the generated event has been rolled up.

Traps generated from systems that support multiple Partition, the cenPartitionNumber and cenPartitionName attributes will carry the exact partition details of the device for which the trap is generated.

Through the management application user interface, the user can customize few attributes of the trap structure. Two attributes included in this mib revision that allows the user to customize each trap sent out are cenCustomerIdentification and cenCustomerRevision.

ciscoEpmNotificationObjects, ciscoEpmNotificationAlarm, and ciscoEpmNotificationMIBCompliance have been deprecated in this revision.

ciscoEpmNotificationAlarmRev1, ciscoEpmNotificationAlarmGroupRev1, ciscoEpmNotificationMIBComplianceRev1, and ciscoEpmNotificationObjectsGroupRev1 have been newly created in this revision.

REVISION  "200308210000Z"
DESCRIPTION  "Included imports for Integer32, Unsigned32, and NOTIFICATION-GROUP."

REVISION  "200207281420Z"
DESCRIPTION  "Initial version of this MIB."
::= { ciscoMgmt 311 }

-- MIB Object Definitions

ciscoEpmNotificationMIBNotifs  OBJECT IDENTIFIER
::= { ciscoEpmNotificationMIB 0 }

ciscoEpmNotificationMIBObjects  OBJECT IDENTIFIER
::= { ciscoEpmNotificationMIB 1 }
ciscoEpmNotificationMIBConform OBJECT IDENTIFIER
::= { ciscoEpmNotificationMIB 2 }

cenAlarmData OBJECT IDENTIFIER
::= { ciscoEpmNotificationMIBObjects 1 }

cenAlarmTableMaxLength OBJECT-TYPE
SYNTAX Unsigned32 ( 1..4294967295 )
MAX-ACCESS read-write
STATUS current
DESCRIPTION "Maximum number of entries permissible in the cenAlarmTable."
DEFVAL { 1 }
::= { cenAlarmData 1 }

cenAlarmTable OBJECT-TYPE
SYNTAX SEQUENCE OF CenAlarmEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "A table containing the device identification and alarm value. The maximum number of entries permissible in this table is defined by cenAlarmTableMaxLength. When the number of entries in the table reaches the maximum limit, the next entry would replace the oldest existing entry in the table."
::= { cenAlarmData 2 }

cenAlarmEntry OBJECT-TYPE
SYNTAX CenAlarmEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "The information regarding a single device status alarm. An entry is created when an alarm is processed."
INDEX { cenAlarmIndex }
::= { cenAlarmTable 1 }

CenAlarmEntry ::= SEQUENCE {
  cenAlarmIndex Unsigned32,
cenAlarmVersion SnmpAdminString,
cenAlarmTimestamp TimeStamp,
cenAlarmUpdatedTimestamp TimeStamp,
cenAlarmInstanceID SnmpAdminString,
cenAlarmStatus Integer32,
cenAlarmStatusDefinition  SnmpAdminString,
cenAlarmType                INTEGER,
cenAlarmCategory            INTEGER12,
cenAlarmCategoryDefinition  SnmpAdminString,
cenAlarmServerAddressType   InetAddressType,
cenAlarmServerAddress       InetAddress,
cenAlarmManagedObjectClass SnmpAdminString,
cenAlarmManagedObjectAddressType InetAddressType,
cenAlarmManagedObjectAddress InetAddress,
cenAlarmDescription        OCTET STRING,
cenAlarmSeverity            INTEGER12,
cenAlarmSeverityDefinition  SnmpAdminString,
cenAlarmTriageValue         INTEGER12,
cenEventIDList              OCTET STRING,
cenUserMessage1             SnmpAdminString,
cenUserMessage2             SnmpAdminString,
cenUserMessage3             SnmpAdminString,
cenAlarmMode                INTEGER,
cenPartitionNumber          Unsigned32,
cenPartitionName            SnmpAdminString,
cenCustomerIdentification   SnmpAdminString,
cenCustomerRevision         SnmpAdminString,
cenAlertID                  SnmpAdminString
}

-- Alarm attributes

cenAlarmIndex     OBJECT-TYPE
SYNTAX     Unsigned32 (1..4294967295)
MAX-ACCESS   not-accessible
STATUS       current
DESCRIPTION
"A monotonically increasing integer for the sole
purpose of indexing the attributes in
ciscoEpmNotificationMIBObjects. When the maximum value is
reached, this value wraps back to 1."
::= { cenAlarmEntry 1 }

cenAlarmVersion   OBJECT-TYPE
SYNTAX     SnmpAdminString (SIZE(1..16))
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION
"The release version of this MIB. The version string will
be of the form <major version>.<minorversion>.
"
::= { cenAlarmEntry 2 }
cenAlarmTimestamp  OBJECT-TYPE
SYNTAX           TimeStamp
MAX-ACCESS       read-only
STATUS           current
DESCRIPTION      
"The time when the alarm was raised."
::= { cenAlarmEntry 3 }

cenAlarmUpdatedTimestamp  OBJECT-TYPE
SYNTAX              TimeStamp
MAX-ACCESS          read-only
STATUS              current
DESCRIPTION         
"Alarms persist over time and can have their field(s)
change values. The last time a field(s) changed, this
alarm is updated. The updated time denotes this time.
Each alarm is identified by the unique alarm instance
id, cenAlarmInstanceID."
::= { cenAlarmEntry 4 }

cenAlarmInstanceID  OBJECT-TYPE
SYNTAX          SnmpAdminString (SIZE(1..20))
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION     
"The Unique Alarm Instance ID."
::= { cenAlarmEntry 5 }

cenAlarmStatus  OBJECT-TYPE
SYNTAX          Integer32 (1..250)
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION     
"The alarm status indicates the status of the alarm
in integer value."
::= { cenAlarmEntry 6 }

cenAlarmStatusDefinition  OBJECT-TYPE
SYNTAX              SnmpAdminString (SIZE(1..255))
MAX-ACCESS          read-only
STATUS              current
DESCRIPTION         
"The short description of the status of the alarm.
The string is formatted in
'\<integer\>,\<alarmStatus description\>' tuples. The \<integer\>
value is the same value that the 'cenAlarmStatus'
attribute holds. <alarmStatus description> contains one line
description of the alarm status generated."
::= { cenAlarmEntry 7 }

cenAlarmType OBJECT-TYPE
SYNTAX INTEGER {
  unknown(1),
  direct(2),
  indirect(3),
  mixed(4)
}
MAX-ACCESS read-only
STATUS current
DESCRIPTION "unknown: When the value for this attribute could not be
determined.
direct: Denotes an alarm generated by a set of events
where all events are reported by an observation(s) of a
managed object.
direct: Denotes an alarm generated by a set of events
where all events were deduced or inferred by the status
of managed objects as determined by the network
management system.
mixed: Denotes an alarm generated by a set of events
which were either direct or indirect."
::= { cenAlarmEntry 8 }

cenAlarmCategory OBJECT-TYPE
SYNTAX Integer32 (1..250)
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The category of the alarm generated represented in
integer value."
::= { cenAlarmEntry 9 }

cenAlarmCategoryDefinition OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The short description of the category of the alarm
generated. The String is formatted in
'<integer>,<alarmCategory description>' tuples. The <integer>
value is the same value that the 'cenAlarmCategory' attribute holds. `<alarmCategory description>` contains one line description of the alarm category generated.

::= { cenAlarmEntry 10 }

cenAlarmServerAddressType  OBJECT-TYPE  
SYNTAX               InetAddressType  
MAX-ACCESS          read-only  
STATUS              current  
DESCRIPTION        "The type of Internet address by which the server is reachable. The Server is the server that is generating this trap."

::= { cenAlarmEntry 11 }

cenAlarmServerAddress  OBJECT-TYPE  
SYNTAX               InetAddress  
MAX-ACCESS          read-only  
STATUS              current  
DESCRIPTION        "The IP Address or the DNS name of the Management Server that raised this alarm to be notified."

::= { cenAlarmEntry 12 }

cenAlarmManagedObjectClass  OBJECT-TYPE  
SYNTAX               SnmpAdminString (SIZE (1..255))  
MAX-ACCESS          read-only  
STATUS              current  
DESCRIPTION        "The class of the managed object for which this alarm was generated. For example, Router, Switch, GateKeeper and VoicePort."

::= { cenAlarmEntry 13 }

cenAlarmManagedObjectAddressType  OBJECT-TYPE  
SYNTAX               InetAddressType  
MAX-ACCESS          read-only  
STATUS              current  
DESCRIPTION        "The type of Internet address by which the managed object is reachable."

::= { cenAlarmEntry 14 }
Appendix C  Notification MIB

cenAlarmManagedObjectAddress  OBJECT-TYPE
SYNTAX             InetAddress
MAX-ACCESS         read-only
STATUS             current
DESCRIPTION        "The IP Address or the DNS name of the Managed Object."
::= { cenAlarmEntry 15 }

cenAlarmDescription   OBJECT-TYPE
SYNTAX               OCTET STRING (SIZE(1..1024))
MAX-ACCESS           read-only
STATUS               current
DESCRIPTION          "A detailed description of the alarm."
::= { cenAlarmEntry 16 }

cenAlarmSeverity     OBJECT-TYPE
SYNTAX          Integer32  (0..100)
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION     "The alarm severity indicates the severity of the alarm in integer value."
::= { cenAlarmEntry 17 }

cenAlarmSeverityDefinition      OBJECT-TYPE
SYNTAX                  SnmpAdminString (SIZE(1..255))
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION             "The short description of the severity of the alarm generated. The String is formatted in '<integer>,<alarmSeverity description>' tuples. The <integer> value is the same value that the 'cenAlarmSeverity' attribute holds. <alarmSeverity description> contains one line description of the alarm severity generated."
::= { cenAlarmEntry 18 }

cenAlarmTriageValue     OBJECT-TYPE
SYNTAX          Integer32(0..100)
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
"The triage value of an alarm is a hierarchical weighting value (applied by the application, and more importantly customizable by the end user) to allow an artificial form of evaluating impact, interest, or other user-determined functions between alarms. The value is a positive number or zero where zero denotes an undetermined or uncomputable value."
 ::= { cenAlarmEntry 19 }

cenEventIDList OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..1024))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Comma separated list of the Unique Event identifiers that led to the generation of this Alarm."
 ::= { cenAlarmEntry 20 }

cenUserMessage1 OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"User input message. This value can be configured."
 ::= { cenAlarmEntry 21 }

cenUserMessage2 OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"User input message. This value can be configured."
 ::= { cenAlarmEntry 22 }

cenUserMessage3 OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"User input message. This value can be configured."
 ::= { cenAlarmEntry 23 }
cenAlarmMode OBJECT-TYPE
   SYNTAX INTEGER {
      unknown(1),
      alert(2),
      event(3)
   }
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION
      "unknown: When the value for this attribute could not be
determined.
      alert: Denotes an alarm generated by a set of events
where
      all events are reported by polling of managed
objects and/or listening to SNMP notifications.
      event: Denotes an event generated by polling of managed
objects and/or listening to SNMP notifications."
   ::= { cenAlarmEntry 24 }

cenPartitionNumber OBJECT-TYPE
   SYNTAX Unsigned32(0..100)
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION
      "In traps generated by the management application that
support
      multiple partitions, the attribute will carry the integer
value assigned to identify the logical group where the
managed
device resides."
   ::= { cenAlarmEntry 25 }

cenPartitionName OBJECT-TYPE
   SYNTAX SnmpAdminString (SIZE(1..255))
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION
      "In traps generated by the management application that
support
      multiple partitions, the attribute will carry the name
assigned to identify the logical group where the managed
device resides."
   ::= { cenAlarmEntry 26 }

cenCustomerIdentification OBJECT-TYPE
   SYNTAX SnmpAdminString (SIZE(1..255))
   MAX-ACCESS read-only
   STATUS current
DESCRIPTION
"User input message. The attribute takes in a free format text. This attribute can be used by advanced management applications to sort responses from the fault management server."
::= { cenAlarmEntry 27 }

cenCustomerRevision OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"User input message. The attribute takes in a free format text. This attribute can be used by advanced management applications to sort responses from the fault management server."
::= { cenAlarmEntry 28 }

cenAlertID OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(1..20))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"In event based notification, this attribute will contain the alert id to which the generated event has been rolled up to. In alert based notification, the cenAlarmInstanceId and cenAlertID would be identical."
::= { cenAlarmEntry 29 }

ciscoEpmNotificationAlarm NOTIFICATION-TYPE
OBJECTS {
  cenAlarmVersion,
  cenAlarmTimestamp,
  cenAlarmUpdatedTimestamp,
  cenAlarmInstanceId,
  cenAlarmStatus,
  cenAlarmStatusDefinition,
  cenAlarmType,
  cenAlarmCategory,
  cenAlarmCategoryDefinition,
  cenAlarmServerAddressType,
  cenAlarmServerAddress,
  cenAlarmManagedObjectClass,
  cenAlarmManagedObjectAddressType,
  cenAlarmManagedObjectAddress,
  cenAlarmDescription,
  cenAlarmSeverity,
  cenAlarmSeverityDefinition,
cenoAlarmTriageValue,
cenEventIDList,
cenUserMessage1,
cenUserMessage2,
cenUserMessage3
}

STATUS             deprecated
DESCRIPTION
"Notification of the status of the managed object as
generated by the management server.

New attributes are added to the ciscoEpmNotificationAlarmRev1.
Hence this notification is deprecated."
::= { ciscoEpmNotificationMIBNotifs 1 }

ciscoEpmNotificationAlarmRev1    NOTIFICATION-TYPE
OBJECTS  {
cenAlarmVersion,
cenAlarmTimestamp,
cenAlarmUpdatedTimestamp,
cenAlarmInstanceID,
cenAlarmStatus,
cenAlarmStatusDefinition,
cenAlarmType,
cenAlarmCategory,
cenAlarmCategoryDefinition,
cenAlarmServerAddressType,
cenAlarmServerAddress,
cenAlarmManagedObjectClass,
cenAlarmManagedObjectAddressType,
cenAlarmManagedObjectAddress,
cenAlarmDescription,
cenAlarmSeverity,
cenAlarmSeverityDefinition,
cenAlarmTriageValue,
cenEventIDList,
cenUserMessage1,
cenUserMessage2,
cenUserMessage3,
cenAlarmMode,
cenPartitionNumber,
cenPartitionName,
cenCustomerIdentification,
cenCustomerRevision,
cenAlertID
}

STATUS             current
DESCRIPTION
"Notification of the status of the managed object as
generated by the management server."
 ::= { ciscoEpmNotificationMIBNotifs 2 }

-- Conformance information

ciscoEpmNotificationMIBCompliances OBJECT IDENTIFIER
 ::= { ciscoEpmNotificationMIBConform 1 }
ciscoEpmNotificationMIBGroups OBJECT IDENTIFIER
 ::= { ciscoEpmNotificationMIBConform 2 }

-- Compliance

ciscoEpmNotificationMIBCompliance MODULE-COMPLIANCE
 STATUS deprecated
 DESCRIPTION
 "The compliance statement for entities which implement the CISCO-EPM-NOTIFICATION-MIB.

New attributes are included in
ciscoEpmNotificationMIBComplianceRev1. Hence this object is deprecated."
 MODULE -- this module
 MANDATORY-GROUPS {
   ciscoEpmNotificationObjectsGroup,
   ciscoEpmNotificationAlarmGroup
 }

GROUP ciscoEpmAlarmConfigGroup
 DESCRIPTION
 "This group is optional."

OBJECT cenAlarmTableMaxLength
 MIN-ACCESS read-only
 DESCRIPTION
 "Write access is not required."

OBJECT cenAlarmVersion
 MIN-ACCESS accessible-for-notify
 DESCRIPTION
 "Read access is not required."
CEN MIB

OBJECT cenAlarmTimestamp
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmUpdatedTimestamp
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmInstanceID
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmStatus
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmStatusDefinition
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmType
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmCategory
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmCategoryDefinition
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmServerAddressType
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."
OBJECT cenAlarmServerAddress
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmManagedObjectClass
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmManagedObjectAddressType
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmManagedObjectAddress
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmDescription
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmSeverity
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmSeverityDefinition
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmTriageValue
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenEventIDList
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."
OBJECT cenUserMessage1
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenUserMessage2
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenUserMessage3
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

::= { ciscoEpmNotificationMIBCompliances 1 }
ciscoEpmNotificationMIBComplianceRev1 MODULE-COMPLIANCE
STATUS current
DESCRIPTION
"The compliance statement for entities which implement the CISCO-EPM-NOTIFICATION-MIB."
MODULE -- this module
MANDATORY-GROUPS {
    ciscoEpmNotificationObjectsGroupRev1, ciscoEpmNotificationAlarmGroupRev1
}

GROUP ciscoEpmAlarmConfigGroup
DESCRIPTION
"This group is optional."

OBJECT cenAlarmTableMaxLength
MIN-ACCESS read-only
DESCRIPTION
"Write access is not required."

OBJECT cenAlarmVersion
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmTimestamp
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."
OBJECT cenAlarmUpdatedTimestamp
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmInstanceID
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmStatus
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmStatusDefinition
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmType
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmCategory
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmCategoryDefinition
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmServerAddressType
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmServerAddress
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."
OBJECT cenAlarmManagedObjectClass
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmManagedObjectAddressType
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmManagedObjectAddress
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmDescription
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmSeverity
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmSeverityDefinition
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmTriageValue
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenEventIDList
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenUserMessage1
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."
OBJECT cenUserMessage2
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenUserMessage3
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmMode
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenPartitionNumber
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenPartitionName
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenCustomerIdentification
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenCustomerRevision
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlertID
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

::= { ciscoRpmNotificationMIBCompliance 2 }
-- Units of Conformance

ciscoBpmNotificationAlarmGroup NOTIFICATION-GROUP
NOTIFICATIONS {
    ciscoBpmNotificationAlarm
}
STATUS deprecated
DESCRIPTION
"The collection of notifications used to indicate managed object status.
ciscoBpmNotificationAlarmGroupRev1 is defined. Hence this object is deprecated."
::= { ciscoBpmNotificationMIBGroups 1 }

ciscoBpmNotificationObjectsGroup OBJECT-GROUP
OBJECTS {
    cenAlarmVersion,
    cenAlarmTimestamp,
    cenAlarmUpdatedTimestamp,
    cenAlarmInstanceID,
    cenAlarmStatus,
    cenAlarmStatusDefinition,
    cenAlarmType,
    cenAlarmCategory,
    cenAlarmCategoryDefinition,
    cenAlarmServerAddressType,
    cenAlarmServerAddress,
    cenAlarmManagedObjectClass,
    cenAlarmManagedObjectAddressType,
    cenAlarmManagedObjectAddress,
    cenAlarmDescription,
    cenAlarmSeverity,
    cenAlarmSeverityDefinition,
    cenAlarmTriageValue,
    cenEventIDList,
    cenUserMessage1,
    cenUserMessage2,
    cenUserMessage3
}
STATUS deprecated
DESCRIPTION
"Trap reflecting the alarm.

New attributes are added to the new notification
`ciscoEpmNotificationObjectsGroupRev1`. Hence
this object is deprecated."

```::= { ciscoEpmNotificationMIBGroups 2 }
```

ciscoEpmAlarmConfigGroup OBJECT-GROUP
OBJECTS { cenAlarmTableMaxLength }
STATUS current
DESCRIPTION
"A collection of objects providing information
about the total number of cenAlarmTable entries
maintained."

```::= { ciscoEpmNotificationMIBGroups 3 }
```

ciscoEpmNotificationAlarmGroupRev1 NOTIFICATION-GROUP
NOTIFICATIONS {
ciscoEpmNotificationAlarmRev1
}
STATUS current
DESCRIPTION
"The collection of notifications used to indicate managed object
status."

```::= { ciscoEpmNotificationMIBGroups 4 }
```

ciscoEpmNotificationObjectsGroupRev1 OBJECT-GROUP
OBJECTS {
cenAlarmVersion,
cenAlarmTimestamp,
cenAlarmUpdatedTimestamp,
cenAlarmInstanceID,
cenAlarmStatus,
cenAlarmStatusDefinition,
cenAlarmType,
cenAlarmCategory,
cenAlarmCategoryDefinition,
cenAlarmServerAddressType,
cenAlarmServerAddress,
cenAlarmManagedObjectClass,
cenAlarmManagedObjectAddressType,
cenAlarmManagedObjectAddress,
cenAlarmDescription,
cenAlarmSeverity,
cenAlarmSeverityDefinition,
cenAlarmTriageValue,
cenEventIDList,
cenUserMessage1,
cenUserMessage2,
cenUserMessage3,
cenAlarmMode,
cenPartitionNumber,
cenPartitionName,
cenCustomerIdentification,
cenCustomerRevision,
cenAlertID

END

cenAlarmEntry Object-Type—Definitions for Selected Attributes

Table C-1 explains the values for attributes related to alert status, category, and severity. You might find it useful to consult this information when you look at a generated trap.

Table C-1 CenAlarmEntry—Alert Status, Category, and Severity

<table>
<thead>
<tr>
<th>Sequence Numbers</th>
<th>Attributes</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>(6)</td>
<td>cenAlarmStatus</td>
<td>Number—From 1 to 3.</td>
</tr>
<tr>
<td>(7)</td>
<td>cenAlarmStatusDefinition</td>
<td>String—Includes number (cenAlarmStatus) and description:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-ACK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2-Active</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-Cleared</td>
</tr>
</tbody>
</table>

**Note**  
Alert status changes from state to state: state is Active; if user acknowledges alert, state is ACK; ultimately, state is Cleared. For more information about alerts, see Using the Alerts and Activities Display, page 3-1
### Table C-1  \textit{CenAlarmEntry—Alert Status, Category, and Severity (continued)}

<table>
<thead>
<tr>
<th>Sequence Numbers</th>
<th>Attributes</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>(9)</td>
<td>cenAlarmCategory</td>
<td>Number—From 0 to 9.</td>
</tr>
<tr>
<td>(10)</td>
<td>cenAlarmCategoryDefinition</td>
<td>String—Includes number (cenAlarmCategory) and description:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0-Unknown</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-Application</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2-Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-Interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4-Reachability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5-Connectivity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6-Utilization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7-System Hardware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8-Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9-Other</td>
</tr>
<tr>
<td>(17)</td>
<td>cenAlarmSeverity</td>
<td>Number—From 1 to 3.</td>
</tr>
<tr>
<td>(18)</td>
<td>cenAlarmSeverityDefinition</td>
<td>String—Includes number (cenAlarmSeverity) and description:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-Informational</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2-Warning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-Critical</td>
</tr>
</tbody>
</table>
Events Processed

Table D-1 lists all possible events you might see in a Device Fault Manager (DFM) Alerts and Activities Detail page, along with the following:

- **Description**: A summary of the event, including typical causes (if known).
- **Trigger**: How DFM learns of the event—either from normal polling, a threshold that was exceeded, or a trap that was received.
- **Severity**: The severity that DFM assigns to the event—critical, warning, or informational.
- **Device Type**: The devices, as classified in DFM, on which the event can occur.
- **Event Code**: The code used by Notification Services to track changes to default DFM event names using the Notification Customization feature. (For more information, see Customizing the Names of DFM Events, page 5-5.)

Event names correspond to what is displayed in the Description column of the Alerts and Activities Detail page.

The events a device can report are determined by the device function. See Configuring Polling and Thresholds, page 10-1 for information on device functions.
Table D-1   Events that DFM Supports

<table>
<thead>
<tr>
<th>Event</th>
<th>Description, Cause, Severity, and Event Code</th>
</tr>
</thead>
</table>
| BackupActivated     | **Description**: Backup port or interface has come online, indicating that the port or interface it backs up has gone down.  
                      **Trigger**: Polling.  
                      **Severity**: Warning.  
                      **Device Type**: All.  
                      **Event Code**: 1000. |
| Duplicate           | **Description**: Same IP address is configured on multiple managed systems.  
                      **Trigger**: Polling (often during rediscovery).  
                      **Severity**: Critical.  
                      **Device Type**: All.  
                      **Event Code**: 1001. |
| ExceededMaximumUptime| **Description**: A backup or dial-on-demand port or interface has been in the Up state for too long.  
                      **Trigger**: Exceeded Maximum uptime threshold.  
                      **Severity**: Warning.  
                      **Device Type**: All (except Network Management).  
                      **Event Code**: 1002. |
| ExcessiveFragmentation| **Description**: System memory is highly fragmented.  
                      **Trigger**: Exceeded Memory fragmentation threshold.  
                      **Severity**: Critical.  
                      **Device Type**: All.  
                      **Event Code**: 1003. |
### Flapping

**Description:** Port or interface is repeatedly alternating between Up and Down states over a short period of time. DFM issues this event by monitoring the number of link downs received within the link window for a particular network adapter (using the Link threshold and Link Window parameters).

**Trigger:** Exceeded Link trap threshold for Link trap window; or processed trap (see Processed SNMP Traps, page B-1, and How DFM Calculates Repeated Restarts and Flapping, page F-1).

**Severity:** Critical.

**Device Type:** All.

**Event Code:** 1004.

### HighBackplaneUtilization

**Description:** Utilization of the backplane’s bandwidth exceeds the Backplane utilization threshold.

**Trigger:** Exceeded Backplane utilization threshold.

**Severity:** Critical.

**Device Type:** All.

**Event Code:** 1005.

### HighBroadcastRate

**Description:** Input packet broadcast percentage exceeds the Broadcast threshold. The input packet broadcast percentage calculates the percentage of total capacity that was used to receive broadcast packets.

**Trigger:** Exceeded Broadcast threshold.

**Severity:** Critical.

**Device Type:** All.

**Event Code:** 1006.
### Table D-1  Events that DFM Supports (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Description, Cause, Severity, and Event Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>HighBufferMissRate</td>
<td><strong>Description</strong>: Rate of buffer misses exceeds the Memory buffer miss threshold.</td>
</tr>
<tr>
<td></td>
<td><strong>Trigger</strong>: Exceeded Memory buffer miss threshold.</td>
</tr>
<tr>
<td></td>
<td><strong>Severity</strong>: Critical.</td>
</tr>
<tr>
<td></td>
<td><strong>Device Type</strong>: All.</td>
</tr>
<tr>
<td></td>
<td><strong>Event Code</strong>: 1007.</td>
</tr>
<tr>
<td>HighBufferUtilization</td>
<td><strong>Description</strong>: Number of buffers used exceeds the Memory buffer utilization threshold.</td>
</tr>
<tr>
<td></td>
<td><strong>Trigger</strong>: Exceeded Memory buffer utilization threshold.</td>
</tr>
<tr>
<td></td>
<td><strong>Severity</strong>: Critical.</td>
</tr>
<tr>
<td></td>
<td><strong>Device Type</strong>: All.</td>
</tr>
<tr>
<td></td>
<td><strong>Event Code</strong>: 1008.</td>
</tr>
<tr>
<td>HighCollisionRate</td>
<td><strong>Description</strong>: Rate of collisions exceeds the Collision threshold.</td>
</tr>
<tr>
<td></td>
<td><strong>Trigger</strong>: Exceeded Collision threshold.</td>
</tr>
<tr>
<td></td>
<td><strong>Severity</strong>: Critical.</td>
</tr>
<tr>
<td></td>
<td><strong>Device Type</strong>: All.</td>
</tr>
<tr>
<td></td>
<td><strong>Event Code</strong>: 1009.</td>
</tr>
</tbody>
</table>
### Table D-1  Events that DFM Supports (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Description, Cause, Severity, and Event Code</th>
</tr>
</thead>
</table>
| HighDiscardRate   | **Description:** A HighDiscardRate event occurs when:  
|                   | • The input packet queued rate is greater than the minimum packet rate, and the input packet discard percentage is greater than the Discard threshold. The input packet queued rate is the rate of packets received without error. The input packet discard percentage is calculated by dividing the rate of input packets discarded by the rate of packets received.  
|                   | • The output packet queued rate is greater than the minimum packet rate, and the output packet discard percentage is greater than the Discard threshold. The output packet queued rate is the rate of packets sent without error. The output packet discard percentage is calculated by dividing the rate of output packets discarded by the rate of packets sent.  
|                   | **Trigger:** Exceeded Discard threshold.  
|                   | **Severity:** Critical.  
|                   | **Device Type:** All.  
|                   | **Event Code:** 1010. |
| HighErrorRate     | **Description:** A HighErrorRate event occurs for input or output packets when both of the following thresholds are exceeded:  
|                   | • Error threshold—Percentage of packets in error  
|                   | • Error traffic threshold—Percentage of bandwidth in use  
|                   | **Trigger:** Exceeded Error threshold and equaled or exceeded Error traffic threshold.  
|                   | **Severity:** Critical.  
|                   | **Device Type:** All.  
|                   | **Event Code:** 1011. |
# Events that DFM Supports (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Description, Cause, Severity, and Event Code</th>
</tr>
</thead>
</table>
| HighQueueDropRate      | **Description**: Number of packets discarded due to input or output queue overflow exceeding the Queue drop threshold. The input (or output) queue overflow is derived by dividing the number of packets designated to be sent (or received) that were discarded due to queue overflow, by the total number of packets in the queue.  
**Trigger**: Exceeded Queue drop threshold.  
**Severity**: Critical.  
**Device Type**: All.  
**Event Code**: 1012. |
| HighUtilization        | **Description**: Current utilization exceeds the utilization threshold configured for this network adapter. (Processor utilization threshold defines the upper limit for CPU utilization and is expressed as a percentage of total CPU capacity.)  
**Note**: For information on how DFM determines interface duplexity when duplexity is not specified, refer to [Utilization threshold, page 10-36.](#)  
**Trigger**: Exceeded one of these thresholds:  
- Processor utilization  
- Utilization (interface settings)  
**Severity**: Critical.  
**Device Type**: All.  
**Event Code**: 1013. |
| InformAlarm            | **Description**: An information pass-through trap was generated.  
**Trigger**: Pass-through trap. See [Pass-Through SNMP Unidentified Traps, page B-3.](#)  
**Severity**: Informational.  
**Device Type**: All.  
**Event Code**: 1014. |
### Event Description, Cause, Severity, and Event Code

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
<th>Trigger</th>
<th>Severity</th>
<th>Device Type</th>
<th>Event Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>InsufficientFreeMemory</td>
<td>System is running out of memory resources. Also reported if there has been a failure to allocate a buffer due to lack of memory.</td>
<td>Exceeded Free memory threshold.</td>
<td>Critical</td>
<td>All</td>
<td>1015</td>
</tr>
<tr>
<td>MajorAlarm</td>
<td>Critical pass-through trap was generated.</td>
<td>Pass-through trap. See Pass-Through SNMP Unidentified Traps, page B-3.</td>
<td>Informational</td>
<td>All</td>
<td>1016</td>
</tr>
<tr>
<td>MinorAlarm</td>
<td>Significant pass-through trap was generated.</td>
<td>Pass-through trap. See Pass-Through SNMP Unidentified Traps, page B-3.</td>
<td>Informational</td>
<td>All</td>
<td>1017</td>
</tr>
</tbody>
</table>
### Table D-1  Events that DFM Supports (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Description, Cause, Severity, and Event Code</th>
</tr>
</thead>
</table>
| OperationallyDown| **Description:** Interface—Card or network adapter’s operational state is not normal. System Hardware—Disk’s operational state is not normal.  
**Trigger:** Polling, or processed trap (see Processed SNMP Traps, page B-1).  
**Note**  
For interfaces, DFM will only generate an OperationallyDown clear event if the card is reinserted into the same slot, and if the module index is the same before and after the card is reinserted.  
**Severity:** Critical.  
**Device Type:** All.  
**Event Code:** 1018. |
| OutofRange       | **Description:** Device temperature or voltage is outside the normal operating range. When an OutofRange event is generated, you will normally also see fan, power supply, or temperature events.  
**Trigger:** Exceeded one of these thresholds:  
- Relative temperature threshold  
- Relative voltage threshold  
**Severity:** Critical.  
**Device Type:** All.  
**Event Code:** 1019. |
<table>
<thead>
<tr>
<th>Event</th>
<th>Description, Cause, Severity, and Event Code</th>
</tr>
</thead>
</table>
| RepeatedRestarts       | **Description**: System repeatedly restarts over a short period of time. DFM issues this event by monitoring the number of system cold and warm starts received within the restart window (using the Restart threshold and the RestartWindow parameters).  
**Trigger**: Exceeded Restart trap threshold for Restart trap window; or processed trap (see Processed SNMP Traps, page B-1, and How DFM Calculates Repeated Restarts and Flapping, page F-1).  
**Severity**: Critical.  
**Device Type**: All.  
**Event Code**: 1020. |
| StateNotNormal         | **Description**: A fan, power supply, temperature sensor, or voltage sensor is not acting normally. When an OutofRange event is generated, you will also see a fan, power supply, or temperature event.  
**Trigger**: Polling.  
**Severity**: Critical.  
**Device Type**: All.  
**Event Code**: 1021. |
Table D-1  Events that DFM Supports (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Description, Cause, Severity, and Event Code</th>
</tr>
</thead>
</table>
| Unresponsive| **Description**: Device does not respond to ICMP or SNMP requests. Probable causes are:  
- On a system: ICMP Ping requests and SNMP queries to the device timeout received no response.  
- On an SNMP Agent: Device ICMP ping requests are successful, but SNMP requests time out with no response.  
**Note**: A system might also be reported as Unresponsive if the only link (for example, an interface) to the system goes down.  
**Trigger**: Polling.  
**Severity**: Critical.  
**Device Type**: All.  
**Event Code**: 1022. |
Polling—SNMP and ICMP

The topics in this appendix describe the SNMP versions that Device Fault Manager (DFM) supports. They also describe how the ICMP and SNMP polling processes that DFM uses work.

The following topics are covered:

- SNMP and ICMP Polling, page E-1
- How DFM Calculates ICMP Polling Intervals, page E-4

SNMP and ICMP Polling

These topics describe the polling DFM uses to obtain reachability and network health information:

- ICMP Polling, page E-1
- SNMP Polling, page E-2

ICMP Polling

DFM uses a high-performance, asynchronous ICMP poller. The poller uses two threads: one sends polls, and the other receives polls. These separate operations allow polling to continue at a stable rate.

An ICMP poll will determine an element to be in one of three possible states, as shown in Figure E-1: Up, Notification Pending, and Down.
When an element in the Up state fails to respond to an ICMP poll, DFM moves it to the Notification Pending state until DFM can determine whether it is up or down.

- The element returns to the Up state when the poll exceeds the maximum success retry count.
- The element is returned to the Up state when it responds to an ICMP poll before the maximum failure entry retry count is exceeded. If it does not respond in time, it is placed in the Down state. DFM does not poll the element again until the next scheduled polling cycle. An element stays in the Down state until it responds to an ICMP poll.
- When the element responds, DFM changes the status of the element to the Up state.

DFM performs this polling for each managed IP endpoint.

### SNMP Polling

By default, the SNMP poller uses ten synchronous polling threads. The SNMP poller supports the following SNMP versions:

- SNMP V1
- SNMP V2C
- SNMP V3 (Authentication and access control, but no data encryption)
DFM uses a 32-bit counter in its correlation analysis for SNMP V1. For SNMP V2C or V3, DFM uses high-capacity, 64-bit counters (this is critical to avoid wrapping—overflow of counters between polls—for high-speed data links).

DFM supports polling devices with multiple IP addresses because the SNMP poller supports multiple IP addresses for each SNMP agent. The poller automatically switches to an alternate IP address during failures.

**Just-in-Time Polling**

The SNMP poller’s MIB variable poll list is driven by a Just-In-Time polling algorithm, which ensures that only those MIB variables needed for correlation are polled. When an element is re-enabled, or comes back up, the variables are automatically polled again.

**Consolidating Requests to Optimize Polling**

The SNMP poller consolidates as many attributes as possible into a single SNMP GET request. This consolidation is not restricted to variables from the same SNMP table. The poller continually adapts to changes in the MIB variable poll list.

If the SNMP poller encounters a nonfatal error while consolidating, the SNMP poller responds differently to an SNMP V1 agent than to an SNMP V2C or V3 agent. This is because an SNMP V1 agent will stop processing a request upon encountering an error, while an SNMP V2C or V3 agent continues processing a request upon encountering an error. (SNMP V2C or V3 agents handle errors on a per-OID basis.)

- If an SNMP V1 agent encounters a nonfatal error during a GET request seeking multiple variables, the SNMP poller suspends the polling of the affected variable. If it continued to poll that variable, the remainder of the request would have to be resent after receiving the error, which could impact SNMP V1 agent performance. The SNMP poller continues to poll the unaffected variables. (An affected variable is one that, for example, has become unavailable due to a configuration change.) This enables the SNMP poller to operate efficiently with an SNMP V1 agent during unexpected device configuration changes.
In contrast, if an SNMP V2C or V3 agent encounters a nonfatal error during a GET request seeking multiple variables, the SNMP poller continues to poll both the affected and unaffected variables.

Coordinating ICMP and SNMP Polling

DFM links its ICMP and SNMP pollers; the SNMP poller will not send requests to any SNMP agent IP address that the ICMP poller has determined is unreachable. These IP addresses are added to a do not poll list, which the SNMP poller checks before sending SNMP requests. It does not send requests to addresses on this list.

If the SNMP agent has multiple IP addresses, the SNMP poller checks for each address in the do not poll list:

- If an address does not appear on the list, the SNMP poller sends a request to it.
- If all addresses for an agent are on the list, the SNMP poller considers the agent unreachable and temporarily suspends sending SNMP requests to it. As soon as an agent’s IP address becomes responsive (per the IMCP poller), the address is removed from the list, and SNMP polling resumes.

How DFM Calculates ICMP Polling Intervals

DFM calculates ICMP polling intervals for a system (for example, a switch or router) as an offset of the reachability setting’s polling interval for a system. System reachability is monitored using a combination of ICMP (Ping) requests for IP status and SNMP requests for interface, port, and card status. If a device does not respond to an ICMP poll, it is placed on a “do not poll” list.

DFM calculates ICMP polling intervals as an offset of the reachability setting’s polling interval for a system. The following is an example of a calculation based on the default value of 240 seconds.
1. DFM calculates the offset using this formula:
   
   ```
   offset = 60;
   if (offset > pollingInterval * 0.5) {
       offset = pollingInterval * 0.5;
   }
   ```

2. DFM calculates the ICIM polling interval using this formula:

   ```
   icimPollingInterval = pollingInterval - offset
   ```

Thus, the default polling intervals are as follows:

- ICMP polling interval is 3 minutes.
- SNMP polling interval is 4 minutes.
How DFM Calculates ICMP Polling Intervals
How DFM Calculates Repeated Restarts and Flapping

Device Fault Manager (DFM) uses similar calculations to diagnose both repeated restarts and flapping. DFM considers a system to be restarting repeatedly when it performs too many cold or warm starts over a short period of time. Table F-1 lists the elements, traps, and user-defineable parameters that DFM uses to calculate repeated restarts.

Table F-1  Elements, Traps, and Parameters Used to Calculate Repeated Restarts

<table>
<thead>
<tr>
<th>Elements</th>
<th>SNMP Traps</th>
<th>Threshold Category</th>
<th>Parameter</th>
<th>Parameter Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>All elements except ports and interfaces</td>
<td>Cold Start, Warm Start</td>
<td>Reachability Settings</td>
<td>Restart trap threshold</td>
<td>Minimum number of SNMP traps required in a user-defined period of time to trigger an event.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Restart trap window</td>
<td>User-defined period within which minimum number of traps must be received to trigger an event.</td>
</tr>
</tbody>
</table>

DFM considers a network adapter to be flapping when it fluctuates between the Up and Down states too often over a short period of time. Table F-2 lists the elements, traps, and user-defineable parameters DFM uses to diagnose flapping.
After DFM generates a Repeated Restarts event or a Flapping event, DFM computes the stable time (the amount of time that must elapse without further traps before DFM declares the element stable again). The stable time is at least as long as the time the element was at fault, and at least as long as the trap window; however, it can be no longer than one hour.

Figure F-1 illustrates how a system is diagnosed as performing repeated restarts, or how a network adapter is diagnosed as flapping.

Table F-2  Elements, Traps, and Parameters Used to Calculate Flapping

<table>
<thead>
<tr>
<th>Elements</th>
<th>SNMP Traps</th>
<th>Threshold Category</th>
<th>Parameter</th>
<th>Parameter Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports and Interfaces</td>
<td>Link Up</td>
<td>Interface/port flapping settings</td>
<td>Link trap threshold</td>
<td>Minimum number of SNMP traps required in a user-defined period of time to trigger an event.</td>
</tr>
<tr>
<td></td>
<td>Link Down</td>
<td></td>
<td>Link trap window</td>
<td>User-defined period within which minimum number of traps must be received to trigger an event.</td>
</tr>
</tbody>
</table>

After DFM generates a Repeated Restarts event or a Flapping event, DFM computes the stable time (the amount of time that must elapse without further traps before DFM declares the element stable again). The stable time is at least as long as the time the element was at fault, and at least as long as the trap window; however, it can be no longer than one hour.

Figure F-1 illustrates how a system is diagnosed as performing repeated restarts, or how a network adapter is diagnosed as flapping.
In Figure F-1, the trap window (Restart trap window or Link trap window parameter) has a value of 30 seconds, and the trap threshold (Restart trap threshold or Link trap threshold parameter) has a value of 2. DFM performs the following actions:

1. As soon as DFM receives a Link Down Trap from a physical port or interface (or a Warm Start/Cold Start Trap from a system), DFM begins counting.

2. When DFM receives 2 or more traps within 30 seconds, it considers the network adapter or system to be at fault and DFM generates a Repeated Restarts event or a Flapping event. The minimum traps parameter (set by the Link trap threshold or Restart trap threshold parameter) determines the number of traps DFM must receive (2) within the trap window (30 seconds, set by the Link trap window or restart trap window parameter) before it considers an element at fault.

3. DFM continues to receive traps for 80 seconds after the initial trap, resulting in a stable time of 80 seconds.

   The stable time is the amount of time that DFM waits before it clears the Repeated Restarts event or Flapping event.
CiscoWorks Navigation Changes

This appendix contains a list of the navigation differences between DFM 2.0 and DFM 1.2.x. For a list of navigation changes in Common Services, refer to User Guide for CiscoWorks Common Services.

Note: Along with the new features listed in What’s New in DFM 2.0?, page 1-3, DFM 2.0 includes other changes that DFM 1.x users will notice. For detailed information on these behavioral differences between DFM 2.0 and DFM 1.2.x, refer to Installation and Setup Guide for Device Fault Manager.

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 G-1 lists the click-by-click navigation paths you would use to access functions in DFM 1.2.x. Then, Table G-1 provides the comparable navigation paths to use in DFM 2.0.
### Table G-1  DFM 1.2 Navigation Compared to DFM 2.0 Navigation

<table>
<thead>
<tr>
<th>DFM 1.2.x</th>
<th>DFM 2.0</th>
<th>DFM 2.0 Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Fault Manager &gt;</td>
<td>Device Fault Manager &gt;</td>
<td>Alarm display from which you can:</td>
</tr>
<tr>
<td>Monitoring Console</td>
<td>Alerts and Activities</td>
<td>- Launch tools, such as Fault History and Common Services Device Center</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Export data to a PDF file or a comma-separated-values file</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Print data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can also change the display to show the information that interests you most, as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Select and create views, groups of device groups; use a view that contains the device groups of interest to you.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Filter the display to show alerts based on their severity, status, and originating device.</td>
</tr>
</tbody>
</table>
### Table G-1  DFM 1.2 Navigation Compared to DFM 2.0 Navigation (continued)

<table>
<thead>
<tr>
<th>DFM 1.2.x</th>
<th>DFM 2.0</th>
<th>DFM 2.0 Description</th>
</tr>
</thead>
</table>
| Device Fault Manager > Administration > Administration Console | Device Fault Manager > Alerts and Activities | From the Detailed Device View, you can:  
- View device detail information  
- Manage and unmanage devices  
- Acknowledge alerts  
- Annotate events |
| (From the CiscoWorks home page) Common Services > Device & Credentials Administration > Device Management | Device management, such as add, import, and delete. **Note** In DFM 2.0, you import devices into a Device Credentials Repository (DCR) that is shared by CiscoWorks applications. You select devices from the DCR (or automatically synchronize devices with the DCR) for DFM to manage. |
| Device Fault Manager > Device Management > Device Selector | View device inventory. |
| Device Fault Manager > Device Management > View Device Details | Configure polling parameters and manage thresholds. |
| Device Fault Manager > Configuration > Polling and Thresholds | Reconfigure DFM to use updated polling parameters and threshold values. |
## Table G-1  DFM 1.2 Navigation Compared to DFM 2.0 Navigation (continued)

<table>
<thead>
<tr>
<th>DFM 1.2.x</th>
<th>DFM 2.0</th>
<th>DFM 2.0 Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Fault Manager &gt; Administration &gt; Device Discovery &gt; Change Probe</td>
<td>Device Fault Manager &gt; Device Management &gt; Device Selector</td>
<td>Select devices manually or configure DFM to automatically synchronize device inventory with Device Credentials Repository (DCR).</td>
</tr>
<tr>
<td><strong>Note</strong> The change probe process is obsolete in DFM 2.0.</td>
<td><strong>Note</strong> Applications on different servers can use the same master DCR. For more information, see <em>User Guide for CiscoWorks Common Services</em>.</td>
<td></td>
</tr>
</tbody>
</table>
| **Device Fault Manager > Administration > Device Discovery > Rediscovery Schedule** | **Device Fault Manager > Configuration > Other Configurations > Rediscovery Schedule** | • Edit the default rediscovery schedule.  
• Create additional rediscovery schedules. |
| **Device Fault Manager > Administration > Trap Configuration > Trap Receiving** | **Device Fault Manager > Configuration > Other Configurations > SNMP Trap Receiving** | Change the port number that DFM uses to listen for SNMP traps. |
| **Note** Although the SNMP trap adapter file used in DFM 1.2 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. |
| **Note** 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
Configure e-mail notifications for alarms.

**Note** 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
Configure trap notifications for alarms.

**Note** 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
Trim the Fault History database.

**Note** DFM 2.0 keeps 31 days of history and trims the database daily at the time you specify.

<table>
<thead>
<tr>
<th>DFM 1.2.x</th>
<th>DFM 2.0</th>
<th>DFM 2.0 Description</th>
</tr>
</thead>
</table>
| Device Fault Manager > Administration > Fault Notification > Mail Notifier | Device Fault Manager > Notification Services > E-Mail Notification | Configure e-mail notifications for alarms.  
**Note** Although the mail notifier 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.  
**Note** 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.  
**Note** DFM 2.0 keeps 31 days of history and trims the database daily at the time you specify. |
### Table G-1  DFM 1.2 Navigation Compared to DFM 2.0 Navigation (continued)

<table>
<thead>
<tr>
<th>DFM 1.2.x</th>
<th>DFM 2.0</th>
<th>DFM 2.0 Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Fault Manager &gt; Fault History:</strong></td>
<td><strong>Device Fault Manager &gt; Fault History:</strong></td>
<td><strong>Device Fault Manager &gt; Fault History:</strong></td>
</tr>
<tr>
<td>• Search by Devices</td>
<td>• Alert Filtering</td>
<td>Generate a 31-day Fault History report based on search criteria.</td>
</tr>
<tr>
<td>• Search by Fault Conditions</td>
<td>• Search Alarm ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Search by Device</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Search by Group</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Event Filtering</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Search by Event ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Search by Device</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Search Alert ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Search by Group</td>
<td></td>
</tr>
<tr>
<td><strong>Device Fault Manager &gt; Alerts and Activities &gt; Tools &gt; Fault History</strong></td>
<td><strong>Device Fault Manager &gt; Alerts and Activities &gt; Tools &gt; Fault History</strong></td>
<td>Generate a 24-hour Fault History report for all alerts in your current view.</td>
</tr>
<tr>
<td><strong>Device Fault Manager &gt; Alerts and Activities</strong></td>
<td><strong>Device Fault Manager &gt; Alerts and Activities</strong></td>
<td>Generate a 24-hour Fault History report for all events on a device component.</td>
</tr>
<tr>
<td>Click an alert ID. The Alerts and Activities Detail display appears. In the Tools column next to the device component of interest, select <strong>Fault History</strong>.</td>
<td>Click an alert ID. The Alerts and Activities Detail display appears. In the Tools column next to the device component of interest, select <strong>Fault History</strong>.</td>
<td></td>
</tr>
</tbody>
</table>
### A

- **access, user**: 11-27 to 11-28
- **Access Control Server (see ACS)**
- **access ports**
  - customizable groups: 8-8
  - defined: 4-5
  - listing by name, type, group, state: 4-5 to 4-7
  - overriding groups: 10-10
  - polling and thresholds: 10-2, 10-11
  - polling categories: 10-18 to 10-25
  - system defined groups: 8-6
  - threshold categories: 10-31 to 10-41
  - viewing thresholds: 10-26
- **acknowledging alerts**: 3-30
- **ACS**: 11-7, 11-8 to 11-12
  - Alerts and Activities display and: 3-2, 3-8, 3-10, 3-14, 9-2
  - device-based filtering: 11-11
  - Device Management pages and: 4-3
  - DFM in ACS mode: 11-9
  - Fault History pages and: 6-3, 6-7, 6-13, 6-15
  - Group Administration and: 8-4
  - modifying roles and privileges: 11-11

### Alerts

- **Notification Services and**: 5-9
- **Polling and Thresholds pages and**: 10-18, 10-26
- **registering with**: 11-9
- **users, configuring**: 11-8
- **versions supported**: 11-9
- **views and**: 9-2

### Alerts

- **acknowledging**: 3-30
- **annotating**: 3-30
- **defined**: 1-8
- **e-mail response**: 3-31
- **getting details about**: 3-6
- **stored Fault History information**: 6-6
- **Alerts and Activities Details page**: 3-12 to 3-17
- **acknowledging alerts**: 3-30
- **annotating alerts**: 3-30
- **e-mail response**: 3-31
- **event details, obtaining**: 3-11
  - **event properties, viewing**: 3-19
  - **events associated with an alert, viewing**: 3-17
  - **layout**: 3-14
  - **starting**: 3-12
Alerts and Activities display 3-1 to 3-32
  ACS and 3-2, 3-8, 3-10, 3-14, 9-2
  customizing 3-10 to 3-11
Fault History, starting from 6-3
layout 3-4, 3-7
log file 11-19
overview 1-8, 3-1
starting 3-2, 3-12
tool buttons on 3-5
views 9-1 to 9-7
alias devices 4-18
annotating alerts 3-30
Apply Changes page 7-4
audience for this document xv

B
backing up databases 11-14
BackupActivated D-2

C
CASUSER, DFM file owner 11-3
cautions
  significance of xvi
changing event names 5-5
CiscoView 3-18

CiscoWorks
  home page 2-2
  processes and DFM 11-21
Common Services groups 8-2
Configuration page 1-11, 7-2
credentials, editing device 4-26
customizable groups 8-8, 10-3
  access port 8-8
device 8-8
  editing 8-11
  interface 8-8
  overview 8-3
  restrictions 8-8
  trunk port 8-8
  (see also groups)

do
den manager, registering
  processes 11-24 to 11-29
Daily Purging Schedule
  log file 11-19
  managing 7-6
database
  backing up and restoring 11-14
  passwords 11-16
  purging 7-5, 7-6
Index

DCR  4-8 to 4-10
    automatic import into DFM  4-15
    changes, effect on DFM  4-29
    credentials, editing  4-26
    deleted devices and  4-30
    devices not in DFM  4-17
    DFM discovery and  4-29
    log file  11-20
    manual import into DFM  4-16
    masters  4-10
    slaves  4-10
    synchronization with DFM  4-9

DDV  3-20 to 3-29
    ACS and  4-3
    examples  3-24
    layout  3-23
    log file  11-19
    starting  3-20, 4-32
    suspending or resuming devices and elements  3-26 to 3-29
    VLANs and  3-20
    deleting devices  4-30
    Detailed Device View (see DDV)
    Device Aliases page  4-18
    Device and Credentials Repository (see DCR)
    Device Center
        Alerts and Activities Details and  3-18
        Fault History and  6-2
    Device Details page  4-32
    device groups
        polling settings  10-18 to 10-25
        threshold categories  10-31 to 10-41
        viewing thresholds  10-26
    device groups, managing  8-3, 8-11
        ACS and  4-3
        customizable  8-8
        deleting groups  8-31
        group membership  8-30
        polling and thresholds  10-2
        rules  8-20 to 8-26

Device Management page  1-8
    devices
        DDV  3-20 to 3-29
        overriding groups  10-9
        polling and thresholds  10-11
        resuming  3-26 to 3-29
        states  4-11
        suspending  3-26 to 3-29
        viewing with DDV  3-24
    devices, importing  4-12 to 4-23
        aggregate devices  4-13
        alias (duplicate) devices  4-18
        DCR
            automatic  4-15
            manual  4-16
        device names  4-12
Index

devices, importing (continued)
  discovery status 4-19
  troubleshooting 4-12, 4-20
  verifying 4-19

devices, managing 4-1 to 4-35
  ACS and 4-3
  ACS device-based filtering 11-11
  aggregate devices 4-13
  contained and containing devices 4-13
  credentials, editing 4-26
  DDV 3-20 to 3-29
  deleting devices 4-30
  device details, viewing 4-32
  Device Details display, understanding 4-33
  device states 4-11
  device support 11-5
  device types managed by DFM 4-3
  exporting 4-24 to 4-25
  forwarding traps to DFM 7-11
  groups (see groups)
  importing (see devices, importing)
  interfaces managed by DFM 4-5
  limits, device 2-13
  log files 11-20
  naming 4-12
  ports managed by DFM 4-5
  rediscovering 4-29
  SNMP timeout and retries, modifying 4-34
  (see also DCR)

Device Selector page 4-16, 4-17
Device Summary page 4-10
device support 11-5

DFM
  1.x and 2.x differences 1-3
  changing event names 5-5, D-1
  day-to-day operations 1-7
  device limits 2-13
  device types managed by 4-3
  home page 2-2
  interfaces managed by 4-5
  introduction 1-1, 1-11 to 1-16
  operational overview 1-13
  ports managed by 4-5
  security alerts 2-12
  servers, additional 11-6
  setting up 1-5 to 1-6, 1-11
  user interface overview 2-1 to 2-13

DFM home page
  CiscoWorks home page and 11-6
  introduction 2-2
  registering additional DFM servers 11-6

Discovery
  aggregate devices 4-13
  alias (duplicate) devices 4-18
  DCR synchronization and 4-29
  device states 4-11
  events that trigger 4-29
  log file 11-20
discovery (continued)
  rediscovery 4-29
  Rediscovery Schedule 4-29, 7-7
status 4-19
troubleshooting 4-12, 4-20
Discovery Status page 4-19
documentation xvi
  additional online xix
  audience for this xv
  related to this product xviii
typographical conventions in xv
duplexity, interface 8-23, 10-36 to 10-37, D-6
DuplexMode 10-36 to 10-37
DuplexSource 10-36 to 10-37
duplicate (alias) devices 4-18
Duplicate (event) D-2

generating details about 3-11, 3-19
log files
  Event Processing Adapters 11-19
  Event Promulgation Module 11-19
stored Fault History information 6-9
thresholds and 10-40
Event sets (see Notification Services)
ExceededMaximumUptime 10-40, D-2
ExcessiveFragmentation 10-41, D-2
exporting devices 4-24 to 4-25

F
FAT partitions 11-3
Fault History 6-1 to 6-16
  ACS and 6-3, 6-7, 6-13, 6-15
  alerts, searches 6-6 to 6-8
  Alerts and Activities display 6-12
  Device Center and 6-2
events, searches 6-9 to 6-12
Events display 6-14
introduction 1-10
log file 11-19
overview 6-1
starting 3-18, 6-3
file ownership 11-3
Flapping 10-41, D-3, F-1 to F-3

e-mail
  notifications (Notification Services) 5-3,
    5-16 to 5-22
  response to alert 3-31
  SMTP server 7-15
event properties, viewing 3-19
events
  changing names 5-5, D-1
defined 1-8
Index

G

groups  8-1 to 8-31
  ACS and  8-4
  Common Services, overview  8-2
creating  8-11, 8-16 to 8-20
customizable  8-7, 8-8, 10-3
  editing  8-11
  overview  8-3
  restrictions  8-8
deleting  8-31
details  8-27
DFM, overview  8-2
editing  8-11, 8-12 to 8-15
interfaces, unmanaging  4-5
managing, overview  8-9
membership  8-26, 8-29, 8-30
overriding (polling and thresholds)  10-4 to 10-11
ports, unmanaging  4-5
rules  8-20 to 8-26
summaries  8-26
system defined  8-4
  Common Services  8-3
  DFM  8-6
  overview  8-3
user defined
  editing  8-11
  overview  8-3

H

help
  online documentation  xix
HighBackplaneUtilization  10-41, D-3
HighBroadcastRate  10-40, D-3
HighBufferMissRate  10-41, D-4
HighBufferUtilization  10-41, D-4
HighCollisionRate  10-40, D-4
HighDiscardRate  10-40, D-5
HighErrorRate  10-40, D-5
HighQueueDropRate  10-40, D-6
HighUtilization  10-40, 10-41, D-6
HP OpenView  7-12

I

ICMP polling
  intervals  E-4
  overview  E-1
SNMP polling and  E-4
IDUs (Incremental Device Updates)  11-5
InformAlarm  D-6
InsufficientFreeMemory  10-41, D-7
interfaces
  customizable groups  8-8
  listing by name, type, group, state  4-5 to 4-7
  managed by DFM  4-5
  overriding groups  10-10
interfaces (continued)
   polling and thresholds  10-11
   polling categories  10-18 to 10-25
   system defined groups  8-6
   threshold categories  10-31 to 10-41
   unmanaging  4-5
   viewing thresholds  10-26

inventory
   DCR devices not in DFM  4-17
   DCR synchronization with  4-9
   effect of DCR changes  4-29
   log files
      Inventory Collector  11-19
      Inventory Interactor  11-19
      Inventory Service  11-20
   inventory collection  4-29
   log file  11-20
   (see also discovery)

K

Known device state  4-11

L

Learning device state  4-11

logs
   backups  11-18
   configuring  11-17
   DFM log files  11-19
   log file (for Logging Services)  11-19
   maintaining  11-18
   sizes  11-18

M

MajorAlarm  D-7

MIBs
   Notification MIB  C-1
   pass-through SNMP traps  B-3
      polled  G-1
      processed SNMP traps  B-1

MinorAlarm  D-7

MSFC  4-4, 4-13

MSM  4-4, 4-13

N

names, devices  4-12
NetView  7-12
NMS, integrating with DFM  7-12
NMSROOT  11-3
Notification Groups (see Notification Services)
Notification MIB  C-1
Notification Services  5-1 to 5-28
   ACS and  5-9
      configuring notifications, overview  5-6
      E-Mail Notifications  5-3, 5-16 to 5-22, 7-15
Index

Notification Services (continued)
  event names, customizing 5-5
  Event Sets 5-7
  introduction 1-9
  log file 11-20
  Notification Groups 5-8, 8-3, 8-11
  Notification MIB C-1
  SNMP Trap Notifications 5-3, 5-10 to 5-15
  subscriptions 5-2 to 5-5
  Syslog Notifications 5-3, 5-22 to 5-28
  VLANs and 5-1

Pending device state 4-11, 4-23
polling
  ACS and 10-18
  applying changes 10-23
  changing settings 10-13 to 10-17
  device groups 10-24
  editing settings 10-18 to 10-25
  how settings are applied 10-3
ICMP
  intervals E-4
  overview E-1
  SNMP and E-4
log files
  adapter 11-19
  database 11-20
  grouping services 11-20
  manager 11-20
  restoring default settings 10-23
  setting priorities 10-4 to 10-11
SNMP
  ICMP and E-4
  overview E-2
  versions supported by DFM E-2
  viewing settings 10-18 to 10-25
polling and thresholds 10-1 to 10-41
ACS and 10-26
  applying changes 10-23
  changing settings 10-13 to 10-17
  customizable groups and 10-3

online help, using 2-3
OperationallyDown D-8
OutOfRange D-8
OutofRange 10-40
overriding groups 10-4 to 10-11
  default 10-6
  devices 10-9
  interfaces 10-10
  port 10-10
  overview 4-29

pass-through SNMP traps B-3
passwords, database 11-16
polling and thresholds (continued)
log files
  adapter 11-19
  database 11-20
  grouping services 11-20
  manager 11-20
setting priorities 10-4 to 10-11
(see also polling)
(see also thresholds)
ports
  access ports 4-5, 4-5 to 4-7, 8-6, 8-8
  firewalls and 11-4
  managed by DFM 4-5
  overriding groups 10-10
  polling and thresholds 10-2
  privileged, using 11-28
  trunk ports 4-5, 4-5 to 4-7, 8-7, 8-8
  unmanaging 4-5
priorities (polling and thresholds) 10-4 to 10-11
processed SNMP traps B-1
processes
  CiscoWorks 11-21
  log file for multiple thread 11-19
  registering with daemon
  manager 11-24 to 11-29
  stopping and starting 11-21

Q

Questioned device state 4-11, 4-23

R

Rediscover/Delete (devices) page 4-20,
  4-26 to 4-31
rediscovery
  DCR synchronization and 4-29
  events that trigger 4-29
  log file 11-20
  Rediscovery Schedule 4-29, 7-5, 7-7
  (see also discovery)
  Rediscovery Schedule page 7-7 to 7-10
  (see also rediscovery)
RepeatedRestarts 10-41, D-9, F-1 to F-3
restoring databases 11-14
resuming device monitoring 3-26 to 3-29
RSFC 4-4, 4-13
RSM 4-4, 4-13
rules, group 8-20 to 8-26

S

security
  alerts 2-12
  file ownership and protection 11-3
  firewalls 11-4
  SNMPv3 11-4
  SSL 11-3
  user access 11-27 to 11-28
self-signed security certificates, creating 11-12
SMTP server, default 7-15
SNMP
  polling
    ICMP and E-4
  overview E-2
  SNMP versions supported by DFM E-2
  SNMPv3 11-4
  timeout and retries, modifying 4-34
SNMP Configuration page 4-35
SNMP traps
  cold start F-1
  integrating SNMP trap receiving with other NMS 7-12
  pass-through B-3
  processed B-1
  SNMP Trap Notifications 5-3, 5-10 to 5-15
  trap forwarding port 7-14
  trap receiving port 7-14
  warm start F-1
SSL 11-3
StateNotNormal D-9
states, devices 4-11
subscriptions (see Notification Services) support, device 11-5
suspending device monitoring 3-26 to 3-29
Syslog Notifications 5-3, 5-22 to 5-28
system administration 7-1 to 7-15
  backup and restore 11-14
  database passwords 11-16
  databases, purging 7-6
  devices from traps to DFM 7-11
  device support 11-5
  logging, configuring 11-17
  ports used 11-1
  processes, starting and stopping 11-21
  protocols used 11-1
  Rediscovery Schedule 7-7
  scheduled tasks 7-5
  security 11-3 to 11-5
  self-signed security certificates, creating 11-12
  SMTP default server 7-15
  SNMP trap forwarding port 7-14
  SNMP trap receiving port 7-14
  users, configuring 11-7 to 11-9
  system defined groups
    DFM 8-6
    overview 8-3
    (see also groups)

T
  tabular displays (see user interface)
  thresholds
    applying changes 10-23
    categories
      Backup Interface Support 10-34, 10-40
      Dial-on-Demand Interface Support 10-34, 10-40
      Environment 10-35, 10-40
thresholds (continued)
categories (continued)
  Generic Interface/Port Performance  10-35, 10-40
  Interface/Port Flapping  10-38, 10-41
  Processor and Memory  10-38, 10-41
  Reachability  10-39, 10-41
changing settings  10-13 to 10-17, 10-26 to 10-30
events triggered by  10-40
how settings are applied  10-3
log files
  adapter  11-19
  database  11-20
  grouping services  11-20
  manager  11-20
restoring defaults  10-30
setting priorities  10-4 to 10-11
values  10-40
viewing  10-26
traps
  forwarding from devices to DFM  7-11
  pass-through SNMP  B-3
  processed SNMP  B-1
  SNMP (see SNMP traps)
  unidentified traps  B-5
troubleshooting
  device discovery  4-20
  device import  4-12, 4-13, 4-20
trunk ports
  customizable groups  8-8
  defined  4-5
  listing by name, type, group, state  4-5 to 4-7
  overriding groups  10-10
  polling and thresholds  10-2, 10-11
  polling categories  10-18 to 10-25
  system defined groups  8-7
  threshold categories  10-31 to 10-41
  viewing thresholds  10-26
typographical conventions in this document  xv

U

unidentified traps and events
  DDV, and  3-20
  other  B-5
Unknown device state  4-11
Unresponsive  D-10
user access  11-27 to 11-28
user defined groups
  editing  8-11
  overview  8-3
  (see also customizable groups)
user interface
  DFM windows, working with  2-1
  dates and times displayed  2-3
  Enter key versus buttons  2-2
  Help, using  2-3
user interface (continued)
  DFM windows, working with (continued)
    multiple windows 2-2
    page not displayed, reasons for 2-2
  objects and groups, selecting 2-7
  tabular displays 2-4
    displays with more than 2,000 records 2-6
    exporting data from 2-6
    paging and sorting 2-5
    printing 2-7
  user roles, understanding 2-12
  users, configuring 11-7 to 11-9
  User Tracking (Campus Manager) 3-18

V

views
  ACS and 9-2
  activating and deactivating 9-4
  configuring 9-1 to 9-7
  creating 9-2
  default 9-2
  deleting 9-7
  log file 11-20
  maximum number 9-1
  modifying 9-5
  refresh cycle 9-1
  selecting for AAD 3-10
  view groups 8-3, 8-11

VLANs
  Alerts and Activities Detail page and 3-12
  Alerts and Activities display and 3-6, 4-4
  Detailed Device View and 3-20
  event properties page and 3-19
  Fault History and 6-3
  Notification Services and 5-1
  viewing details 3-19