



Release Notes for Device Fault Manager 2.0.3 on Solaris

Revised: 3 October 2006

These release notes are for use with Device Fault Manager (DFM) 2.0.3 running on a Solaris platform. Supported Solaris versions are Solaris 8 (Solaris 2.8) or Solaris 9 (Solaris 2.9).

Refer to the installation guides for software and hardware installation details.

These release notes provide the following information:

- [New Features, page 2](#)
- [Product Documentation, page 3](#)
- [Related Documentation, page 4](#)
- [Additional Information Online, page 5](#)
- [Known Problems, page 5](#)
- [Resolved Problems, page 22](#)
- [Obtaining Documentation, page 40](#)
- [Documentation Feedback, page 41](#)
- [Cisco Product Security Overview, page 42](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2004-2005 Cisco Systems, Inc. All rights reserved.

- [Obtaining Technical Assistance, page 43](#)
- [Obtaining Additional Publications and Information, page 46](#)

New Features

DFM 2.0.3 contains the following features.

New Features

DFM 2.0.3 contains all of the features that were introduced in DFM 2.0, which are described in the *User Guide for Device Fault Manager* (see [Product Documentation, page 3](#)).

Resolved Problems

In addition to all bug fixes provided through DFM 2.0 Service Pack 2, DFM 2.0.3 contains many new bug resolutions. A complete list of resolved problems is provided in [Resolved Problems, page 22](#).

Device Support

DFM 2.0.3 contains all device support provided through DFM 2.0 Service Pack 2. In addition, it contains support for the following devices:

- Cisco Content Networking—Cisco CSS 11500 Series Content Services Switches: 11501, 11503, 11506 (running WebNS 7.4)
- Cisco Routers—Cisco 800 Series Routers: 857 and 877 Integrated Services Routers

For a complete list of supported devices, see *Supported Devices for Device Fault Manager 2.0.3* (refer to [Product Documentation, page 3](#)).

Product Documentation


Note

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

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

Table 1 **Product Documentation**

Document Title	Available Formats
<i>Release Notes for Device Fault Manager 2.0.3 on Solaris</i>	<ul style="list-style-type: none"> Printed document that was included with the product. On Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps2421/prod_release_notes_list.html
<i>Installation and Setup Guide for Device Fault Manager 2.0.3 on Solaris</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps2421/prod_installation_guides_list.html Printed document available by order (part number DOC-7817165=).¹
<i>User Guide for Device Fault Manager, Software Release 2.0.3</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps2421/products_user_guide_list.html Printed document available by order (part number DOC-7817161=).¹
<i>Supported Devices for Device Fault Manager 2.0.3</i>	On Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps2421/products_device_support_tables_list.html

Table 1 Product Documentation (Continued)

Document Title	Available Formats
<i>Status of DFM Device Agent Bugs (DFM 1.x and DFM 2.x)</i>	On Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps2421/prod_release_notes_list.html
Context-sensitive online help	<ul style="list-style-type: none"> Select an option from the navigation tree, then click Help. Click the Help button in the dialog box.

1. See [Obtaining Documentation](#), page 40

Related Documentation



Note

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

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

Table 2 Related Documentation

Document Title	Description and Available Formats
<i>Quick Start Guide for LAN Management Solution 2.5.1</i>	<ul style="list-style-type: none"> Printed document that was included with the product. On Cisco.com at the following URL: http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html
<i>Data Migration Guide for LAN Management Solution 2.5.1</i>	<ul style="list-style-type: none"> Printed document that was included with the product. On Cisco.com at the following URL: http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html
<i>Release Notes for CiscoWorks Common Services 3.0.3 (Includes CiscoView) on Solaris</i>	<ul style="list-style-type: none"> Printed document that was included with the product. On Cisco.com at the following URL: http://www.cisco.com/en/US/products/sw/cscowork/ps3996/prod_release_notes_list.html

Table 2 Related Documentation (Continued)

Document Title	Description and Available Formats
<i>Installation and Setup Guide for Common Services 3.0.3 (Includes CiscoView) on Solaris</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com at the following URL: http://www.cisco.com/en/US/products/sw/cscowork/ps3996/prod_installation_guides_list.html • Printed document available by order (part number DOC-7817183=).¹
<i>User Guide for CiscoWorks Common Services 3.0.3</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com at the following URL: http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_list.html • Printed document available by order (part number DOC-7817182=).¹

1. See [Obtaining Documentation](#), page 40.

Additional Information Online

Service packs (formerly called incremental device updates or IDUs) contain the updated files necessary for the latest device support and fixes to known problems that are not available in DFM 2.0. If you are a registered user, you can download service packs for DFM from:

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

To determine which packages are installed on your CiscoWorks Server, from the Common Services home page, select **Software Center > Software Updates**.

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

Known Problems

Refer to these sections for information on known and resolved problems in this release:

- [Known Problems in DFM 2.0.3](#), page 6

- [Known Problems Inherited from DFM 2.0, page 20](#)

For information on DFM bugs that result from device bugs, see *Status of DFM Device Agent Bugs* at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dev_sup/index.htm.



Note

To obtain more information about known problems, access the Cisco Software Bug Toolkit at <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. (You will be prompted to log into Cisco.com.)

Known Problems in DFM 2.0.3

[Table 8](#) lists all problems that are specific to DFM 2.0.3. Note that known bugs from DFM 2.x service packs have been *rolled in* to this release.

Table 3 Known Problems in DFM 2.0.3

Bug ID	Summary	Additional Information
CSCsc68174	Local upgrade from LMS 2.5 LMS 2.5.1 should remove jar files from old image	<p>After performing a local upgrade to LMS 2.5.1 from LMS 2.5 (in other words, an upgrade from DFM 2.0), the DFM 2.0.3 image contains some jar files that should be removed. If not removed, these files may cause random problems when DFM Group Administration is used.</p> <p>The workaround is as follows:</p> <ol style="list-style-type: none"> 1. Stop the daemon manager. 2. Manually delete the following files from <i>NMSROOT/MDC/tomcat/webapps/triveni/WEB-INF/lib</i>: <ul style="list-style-type: none"> cogs1.3.jar ogs-client1.3.jar ogs-server1.3.jar ogs-sharedasa1.3.jar ogs-sharedgroup1.3.jar ogs-sqlasa1.3.jar ogs-testasa1.3.jar ogs-util1.3.jar 3. Restart the daemon manager.
CSCsa31846	Cannot resize Detailed Device View columns	Several columns in the DFM 2.x Detailed Device View are difficult to read because they are narrow and cannot be resized. There is currently no workaround.
CSCsa49471	Cannot configure user messages for the <code>ciscoEpmNotificationAlarm</code>	DFM CISCO-EPM-NOTIFICATION-MIB traps contain three user message fields: <code>cenUserMessage1</code> , <code>cenUserMessage2</code> , <code>cenUserMessage3</code> . However, the <code>varbinds</code> values are set to <code>um1</code> , <code>um2</code> , and <code>um3</code> , respectively, and cannot be reconfigured. There is no workaround.

Table 3 Known Problems in DFM 2.0.3 (Continued)

Bug ID	Summary	Additional Information
CSCsb04678	DFM 2.0 displays bogus device info for selected alerts	When a user clicks an Alert ID for a given device, sometimes DFM occasionally displays alerts that are for different devices. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsb04914	DFM helpdesk user should not be able to manage/unmanage devices and interfaces	A user with the helpdesk role can manage and unmanage devices and interfaces (from either the Detailed Device View or by editing polling parameters from Configuration > Polling Parameters). A helpdesk user should not have this privilege. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsb05350	Cannot customize e-mail notification subject	Users cannot customize the subject of e-mail notifications. There is currently no workaround.
CSCsb82140	DFM does not handle ifOperStatus values correctly	DFM is capable of handling ifOperStatus values up(1) and down(2), but it does not recognize the dormant state. There is currently no workaround.
CSCsa48916	AA Detail page only refreshes events when they clear or recur	The Alerts and Activities Detail page only refreshes an event's status when the event is cleared, or when the event surpasses a threshold. However, even if the event repeatedly surpasses the threshold, DFM does not refresh the value. There is currently no workaround.
CSCsb38137	DFM 2.x discovery may hang (in Learning state) indefinitely	DFM 2.x discovery may hang (in Learning state). The conditions are unknown. This bug is under investigation. There is currently no workaround.

Table 3 Known Problems in DFM 2.0.3 (Continued)

Bug ID	Summary	Additional Information
CSCsb82889	DFM does not generate alerts when another application subsequently takes port 162	<p>If DFM is listening for traps at port 162, and another application subsequently takes that port, DFM will not receive any traps nor will it generate alerts.</p> <p>The workaround is as follows:</p> <ol style="list-style-type: none"> 1. Change the trap receiving port in DFM. 2. Use (or configure) a remote installation of the HPOV-NetView adapter, in which the remote machine is listening for traps on port 162. 3. Configure the remote machine to forward all traps to DFM at the listening port configured in Step 1.
CSCsb87408	If an interface goes down, DFM generates two interface Unresponsive events	When a device interface goes down, DFM generates two interface Unresponsive events for the same interface. This happens because DFM generates one event for the interface and another event for the underlying SNMP object. No workaround is currently available. Ignore the duplicate event.
CSCsc38566	DFM should not create virtual interface objects	DFM creates objects for virtual interfaces, but it should not. This is problematic for networks containing routers that have large numbers of virtual interfaces (because the objects, which contain little information, use system resources and discovery time). This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsb96943	In device name, dot is missing between name and domain	After importing devices from the DCR to DFM, a device may occasionally go to the Questioned state because the dot in the device name (between the name and domain) disappears. The name may be displayed correctly in the DCR. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).

Table 3 Known Problems in DFM 2.0.3 (Continued)

Bug ID	Summary	Additional Information
CSCsc13884	Device Selector page gives JSP error after upgrade from DFM 2.0 to DFM 2.0.3	After upgrading DFM 2.0 to DFM 2.0.3 (using the CD), if the user selects Device Management > Device Selector , the page occasionally displays a JSP error. This was observed on one machine. There is currently no workaround.
CSCsc41746	Intermittent problems when editing DFM user-defined groups	Occasionally, a user will not be able to edit user-defined groups. This happens intermittently. The workaround is to restart the daemon manager.
CSCsc44902	DFM devices are deleted when restricted license number exceeded	When more than 300 devices are added to a DFM server running with a restricted license, all devices are deleted from DFM. After some time, some of the devices may be automatically re-added. There is no workaround.
CSCsc46279	Solaris: Local upgrade hangs because sm_server is not registered with broker	When upgrading LMS 2.2 to LMS 2.5.1 on Solaris, a local upgrade may intermittently fail during the migration phase. This is because the sm_server does not register with the DFM broker. The workaround is to stop the sm_server and brstart processes using kill -9 .
CSCsc60557	Local upgrade to DFM 2.0.3 proceeds without running required migration script	When performing a local upgrade from DFM 1.2.x to DFM 2.0.3, the upgrade sometimes proceeds without running the required migration script. The workaround is as follows: <ol style="list-style-type: none"> 1. Check the installation log for the pertinent error. 2. Perform the procedures for migrating your data for a remote upgrade, as documented in the installation guides (see Product Documentation, page 3).

Table 3 Known Problems in DFM 2.0.3 (Continued)

Bug ID	Summary	Additional Information
CSCsc61715	Device Selector page gives DCRAdapter.log error after upgrade from DFM 1.2.x to DFM 2.0.3	<p>After upgrading DFM 1.2.x to DFM 2.0.3, if the user selects Device Management > Device Selector, the page intermittently displays the following message:</p> <p>An exception has occurred. Please check the DCRAdapter.log file.</p> <p>The workaround is as follows:</p> <ol style="list-style-type: none"> 1. Stop the daemon manager. 2. Verify that ports 43501 to 43508 are free (not in Listen or Timed_wait state). If they are not yet free, wait 3-4 minutes. 3. Restart the daemon manager.
CSCsa79086	Cannot create MSFC user-defined or customizable groups	DFM users cannot create user-defined or customizable groups for MSFCs. This is because the Group Administration user interface does not list the MSFCs in the Objects Matching Membership Criteria list, even though the MSFCs match the rule. As a result, the user cannot adjust polling and threshold settings or priorities for MSFCs. There is no workaround.
CSCsb36438	LMS 2.5 may not work properly with HP NIC-Teaming environment	If DFM is running on a server with multihomed HP NIC-Teaming (fail-on-fault) environment, devices in the DFM inventory are listed as Unresponsive. This was observed on a Windows server. The workaround is to disable NIC-Teaming, and then reinstall Common Services, DFM, and any other required LAN Management Solution applications.

Table 3 Known Problems in DFM 2.0.3 (Continued)

Bug ID	Summary	Additional Information
CSCsa58553	Fault History search screens are nonintuitive and may not work properly	<p>Fault History screens have the following limitations:</p> <ul style="list-style-type: none"> • The Search by Device page does not have an object selector. (This selector is helpful when the user does not know the device name.) • The Search by Event ID and Search by Alert ID pages do not list ID object selectors. (These selectors are helpful when the user does not know the IDs.) <p>To find a device with an unknown name, use the Search by Group page, which provides a device object selector.</p> <p>To find relevant event or alert IDs, start the Alerts and Activities display, and locate the event or alert ID for which you want to search. Use that ID in the Fault History search field.</p>
CSCsb48643	Cannot disable ICMP polling in DFM	DFM 2.x does not allow users to disable ICMP polling so software can function across a firewall. (Users could disable polling in earlier DFM versions.) There is currently no workaround.
CSCsb16311	Alerts and Activities display alarm not updated when most severe event is cleared	When the most severe event associated with an alert is cleared, DFM does not update the Alerts and Activities display to show the current status of all the events. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsb16307	Fault not attached when user selects Notify in Alerts and Activities Detail display	When a user clicks Notify from the Alerts and Activities Detail page, an e-mail is sent, but with no alert information. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).

Table 3 Known Problems in DFM 2.0.3 (Continued)

Bug ID	Summary	Additional Information
CSCsb14294	DFM polls MSFC 15.1/16.1 internal interfaces	Device Fault Manager 2.0 polls the 6506 MSFC internal interfaces 15/1 and 16/1. It should not. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsb73377	Bogus ExcessiveFragmentation alerts for 6503 CatOS LargestFreeBuffer	DFM generates bogus ExcessiveFragmentation events for the Catalyst 6503 catOS LargestFreeBuffer. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5). Delete and re-add the device to remove any previously-existing bogus events.
CSCsb83127	Cannot edit customizable group by ifType	DFM does not allow the user to edit customizable groups so that ifType has a unique value. There is currently no workaround
CSCsc02403	Alerts and Activities Detail page information not propagated	When a user clicks an Alert ID in the Alerts and Activities display, the Alerts and Activities Detail page will open, but occasionally no event details are displayed (or it may take up to 30 minutes to display the information). The problem maybe due to DBexceptions caused by attempts access a large dfmepm.db database. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsc21691	Cannot clear UnidentifiedTrap alert	When an unmanaged device sends a pass-through trap, the event is added to the UnidentifiedTrap bucket. If that device is then added as a managed device before the event is cleared from UnidentifiedTraps, there is no way to clear that event manually. There is currently no workaround.
CSCsa97721	120dpi font resolution renders Alerts and Activities display unreadable	Setting font resolution to 120 dpi on a high resolution monitor renders the Alerts and Activities display unreadable. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).

Table 3 Known Problems in DFM 2.0.3 (Continued)

Bug ID	Summary	Additional Information
CSCsa67346	3560-48PS, Metro 3750: Collision Rate event info shows null value	<p>When a user opens an event details page to check collision rate information, the value of SingleCollisionFramesP is displayed as null, as follows:</p> <pre>OutputPacketRate 3333333.2 PPS CollisionPct 12.0 % SingleCollisionFramesP null</pre> <p>This was observed on the 3560-48PS switch and the Metro 3750 series switches. There is no workaround.</p>
CSCsa86901	MDS-9216A: DDV does not display FibreChannel interfaces	<p>The MDS-9216A Detailed Device View does not display the device's FibreChannel interfaces. The MDS-9216A has 18 interfaces (17 are ifType fibreChannel(56) and one is ifType fastEther(62)). Only the FastEthernet port is shown in the DDV; no interface components are listed.</p> <p>This is due to a problem with the DFM engine. There is no workaround.</p>
CSCsa85670	MDS-9216A: DDV does not display memory information	<p>The Detailed Device View does not display memory components for the MDS-9216A, even though the device supports memory components.</p> <p>This is due to a problem with the DFM engine. There is no workaround.</p>
CSCsa81033	GSR-12010: DFM generates discovery error messages	<p>When attempting to discover the GSR-12010 (OID 1.3.6.1.4.1.9.1.348), DFM generates error messages and device fans are not discovered.</p> <p>This is due to a problem in the DFM engine. There is no workaround.</p>

Table 3 Known Problems in DFM 2.0.3 (Continued)

Bug ID	Summary	Additional Information
CSCsa66807	DDV has meaningless redundancy-related information	<p>The following redundancy-related information was displayed on the Detailed Device View for the CE-2636, CDM-4650, CE-511, and WLSE 2.8:</p> <p>RedundancyState LastSwitchOverTime LastSwitchOverReason</p> <p>This information should not be listed, since it is meaningless for these devices. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).</p>
CSCin86757	DFM does not generate fault when SNMP agent gives null response	DFM does not report SNMPAgent Unresponsive symptoms when it receives a NULL response from an SNMP agent. This is misleading to users, since the agent is actually responding to SNMP queries with an invalid value, but DFM never detects this. DFM neither polls the device nor reports there is a device polling problem.
CSCin86753	Issue regarding duplicate IP address in ITM 2.0	When different IP addresses belonging to the same device are added as separate devices, due to a timing issue, they are discovered and listed as separate devices. This is incorrect and causes invalid DuplicateIP alarms.
CSCsb64944	DFM 2.0.3: DDV displays blank page	When a DFM 2.0.3 user opens a Detailed Device View using Device Management > Select Devices , DFM occasionally displays a blank page in addition to the normal page. This has only been observed on one client machine. The workaround is to close the blank window. This bug is under investigation.

Table 3 Known Problems in DFM 2.0.3 (Continued)

Bug ID	Summary	Additional Information
CSCsb21975	Ca t2924CXLv: DDV shows LargestFreeBuffer value as not available	<p>When a user launches a Detailed Device View for the Catalyst 2924CXLv, DFM occasionally fails to collect the value of LargestFreeBuffer. The following was displayed:</p> <pre>LargestFreeBuffer = ciscoMemoryPoolLargestFree / 1024 Unable to generate the alarm for Excessive fragmentation</pre> <p>There is no workaround.</p>
CSCsd33287	Device rediscovery hangs at 10%	DFM 2.x discovery may hang at 10% due to a communication problem between the inventory service and collector. This problem is under investigation. There is currently no workaround.
CSCsd38823	INVDbEngine process hogs CPU, rendering the system unusable	<p>The DFM INVDbEngine process can hog the CPU. This was observed when DFM was installed with other contents of the LAN Management Solution, the DCR was managing 9,000 devices, and DFM attempted to import all of the devices.</p> <p>The workaround is to use manual DFM/DCR synchronization to selectively add devices to the DFM inventory. (In the Device Selector page, make sure the synchronization checkbox is not checked.)</p>
CSCsd42055	Devices not getting managed when imported in bulk	<p>When 1,500 devices were added to DFM in a bulk import, most of the devices are put in the Questioned state and finally time out. The behavior differed between Solaris and Windows as follows:</p> <ul style="list-style-type: none"> On Windows, the workaround is to rediscover the devices in question. On Solaris, the problem remained after increased the SNMP timeout and retries to their maximum. There is no workaround for Solaris.

Table 3 Known Problems in DFM 2.0.3 (Continued)

Bug ID	Summary	Additional Information
CSCsd46213	Backup succeeds, but incorrect DFM version listed in restorebackup.log	<p>DFM 2.0.4 can be successfully backed up and restored, However, the restorebackup.log lists the following message:</p> <p>Version of DFM available in the backup is 2.0</p> <p>Ignore the log message.</p>
CSCsd46224	Device management states not preserved after data is restored	<p>After a user backs up and restores DFM data, DFM does not preserve the original management state of the devices. For example, a device that was suspended is moved to managed.</p> <p>The workaround is to manually change the managed state of the device from the Detailed Device View.</p>
CSCsd46279	Notification group management states not preserved after the groups are edited	<p>After a user edits a notification group, DFM does not preserve the original management state. For example, a suspended notification group is moved to running. The workaround is to manually change the management state using Notification Services.</p>
CSCsd64086	New user defined groups not reflected in Fault History unless users logs out and in	<p>After creating a new user defined group in DFM, the group is not displayed in Fault History. The user must log out and back in to CiscoWorks to see the new group in Fault History. The workaround is to log out and back in to CiscoWorks.</p>
CSCsd65361	Trap recipient entries deleted when they follow a duplicate	<p>If a user lists the same trap recipient twice, any recipients listed after the duplicate are deleted. For example, dfmpc3 and dfmpc4 would be deleted from the following list of hostnames:</p> <p>dfmpc1, dfmpc2, dfmpc1, dfmpc3, dfmpc4</p> <p>There is no workaround.</p>

Table 3 Known Problems in DFM 2.0.3 (Continued)

Bug ID	Summary	Additional Information
CSCsd70989	Empty Alerts and Activities page exits when saved to PDF	If the user displays an Alerts and Activities page that has no alerts, and exports the window to PDF, the Alerts and Activities page exits. There is no workaround.
CSCsd72607	Solaris: Deleted devices not removed from notification groups	After deleting devices from the DFM inventory, the devices still appear in existing notification groups. (The devices do not appear when creating a new notification group.) There is no workaround.
CSCsd78100	WLSE: Switchover events not generated when added through VIP in NAT	When a WLSE device is added to DFM using VIP, and the device is configured with a NAT address, DFM does not generate any switchover events or traps after services are started or stopped. There is no workaround.
CSCsd79639	User cannot search Fault History for devices deleted in last 31 days	If a device is deleted from DFM, users cannot search for historical device information from Fault History, even if the Fault History database contains information on the device. There is no workaround.
CSCsd81235	Alerts and Activities Details page displays two Tools drop-down lists	The Alerts and Activities Detail page occasionally displays two Tools drop-down lists for one event. This was observed when two events occurred on the same device, and one of the events is cleared. There is no workaround.
CSCsd73739	DFM 2.0.3 stops sending notifications for very large networks	When the number of managed instances approaches or exceeds the DFM maximum, DFM stops sending notifications for new events. There is no workaround.
CSCin86752	DFM does not discover 4604 Access Gateway card in Catalyst 4506	DFM 1.2.x did not discover 4604 Access Gateway cards in Catalyst 4506 switches. This problem has been fixed. However, although DFM 2.0 discovers the parent switch and card successfully, it does not display any card details in the Detailed Device View. There is currently no workaround.

Table 3 Known Problems in DFM 2.0.3 (Continued)

Bug ID	Summary	Additional Information
CSCsa63869	WLSE: VIP not being rediscovered after switchover	When the virtual interface (VIP) of a WLSE device is added and a switchover occurs, the VIP is not rediscovered by DFM. This is because after a switchover, the VIPs become unreachable for a short period of time, and if this coincides with when the polling is performed, no rediscovery is performed. The workaround is to manually rediscover the VIP.
CSCsa58587	ONS-15454 not moved to Known unless group selected	While being discovered, the ONS-15454 may get stuck in the Learning state if a group is not selected. The workaround is to select a group.
CSCsc63868	CSS devices: Device is listed as Unknown device type	When a CSS 11501, 11503 or 11506 device running WebNS 7.4 or later is added to DFM, it is listed as an Unknown device type. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsb78524	CSS devices: DDV does not list all interfaces/ports	The Detailed Device View does not list all of the ports and interfaces on the CSS 11501, 11503 or 11506 devices running WebNS 7.4 or later. There is currently no workaround.
CSCsc41119	CSS devices: DFM does not report processor and memory events	DFM does not report processor and memory HighUtilization events on CSS 11501, 11503 or 11506 devices running WebNS 7.4 or later. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsg03702	SIP 200 card: DDV lists card status as Not Available	When the Detailed Device View is launched on a Cisco 7609 router that has a SIP 200 card, the card is listed as Not Available. There is no workaround.
CSCsg13511	6504-E: Temperature OutOfRange event not generated	DFM does not generate a temperature OutOfRange event for the 6504-E. There is no workaround.

Known Problems Inherited from DFM 2.0

Table 4 lists all known problems that were inherited from the DFM 2.0 release.

Table 4 *Known Problems Inherited from DFM 2.0*

Bug ID	Summary	Additional Information
CSCsa50314	DFM group administration windows should not show Common Services groups	DFM Group Administration allows users to create groups that contain Common Services groups, but users cannot perform any actions on those groups. The Common Services groups should therefore not be listed. This is due to a Common Services problem. A bug against Common Services has been opened (CSCsa50290). There is no workaround.
CSCef60937	Fault History and Notification Services do not list groups from other LMS applications	In the Fault History and Notification Services windows, DFM does not display groups from other LMS applications (such as Campus Manager and Resource Manager Essentials). This is due to a Common Services problem. A bug against Common Services has been opened (CSCef59702). There is no workaround.
CSCsa48916	Alerts and Activities Detail page only refreshes events when they are cleared or they recur	The Alerts and Activities Detail page only refreshes event status when the event is cleared or when the event surpasses a threshold. If the event already surpassed the threshold, it is not refreshed if the value (still above the threshold) changes again. There is no workaround.

Table 4 Known Problems Inherited from DFM 2.0 (Continued)

Bug ID	Summary	Additional Information
CSCeg34129	Sybase database error causes occasional lag in SNMP and e-mail notification delivery	<p>A Sybase problem occasionally causes Notification Services to delay in delivering SNMP and e-mail notifications, with a delay up to five minutes. This occurs when the Solaris server is running in a heavy load environment (for example, when 50 events are received every polling cycle, and the polling cycle is every 4 minutes). It may be observed every 30 minutes.</p> <p>The Sybase database error that causes this problem is being tracked through a Common Services 3.0 defect (CSCef37746). There is currently no workaround.</p>
CSCsa50045	Memory ExcessiveFragmentation event not generated for some switches	By default, DFM generates memory ExcessiveFragmentation events for routers. For switches, the event is generated only when the enableFragmentAnanalysis flag is set to true. In DFM 1.2.x, users could enable this flag using the UI, but there is no mechanism to do this in DFM 2.0. There is no workaround.
CSCsa61612	Need UI for bulk unmanage	DFM needs a function for performing bulk manage and unmanage operations, so that access ports (and other components) can be easily managed or unmanaged. The workaround is to manually manage or unmanage each component.
CSCsa49793	Need popup message to remind user when to select Apply Changes	When a device or device component is resumed (or managed) after being suspended (or unmanaged), users must select Configuration > Apply Changes to resume polling. Although this is explained in the documentation, DFM should also display a popup message that reminds users to do this.

Table 4 *Known Problems Inherited from DFM 2.0 (Continued)*

Bug ID	Summary	Additional Information
CSCsb51729	DFM shows error message when creating group	<p>When a user tries to create a group using DFM Group Administration, DFM sometimes displays the following error:</p> <pre>Error evaluating rule in Group Administration Server.: :DFM:VASA:DFMObject:Device.IP.Address contains "10.77" (Application error: ASAResponderException: Could not fetch instances of VoiceAndTelephonyBecause:com.cisco.nm.inchar gelib.InchargeWrapperException: Not currently attached)</pre> <p>This bug is under investigation. There is no workaround.</p>

Resolved Problems

These sections contain tables that list the problems resolved in this release:

- [Problems Resolved in DFM 2.0.3, page 23](#)
- [Problem Resolutions Inherited from DFM 2.0 Service Pack 2, page 29](#)
- [Problem Resolutions Inherited from DFM 2.0 Service Pack 1, page 30](#)
- [Problem Resolutions Inherited from DFM 2.0, page 33](#)

Problems Resolved in DFM 2.0.3

Table 5 lists all problems that are resolved in DFM 2.0.3.

Table 5 Problems Resolved in DFM 2.0.3

Bug ID	Summary	Explanation
CSCsa70833	dfmValidateUpgrade fails to validate a DFM 1.2 CD-ROM	The dfmValidateUpgrade script failed to validate a DFM 1.2 CD-ROM. It now validates the CD correctly.
CS Csa72836	DFM12x-DFM20-upgrade.pl should be integrated with restorebackup.pl	When upgrading to DFM 2.0, the user had to run a separate DFM12x-DFM20-upgrade.pl script to perform an upgrade (unlike other applications in the LAN Management Solution). The script is now integrated with restorebackup.pl, a script which is used by LMS 2.5.1 applications.
CSCsa97915	Solaris: Installation on Solaris sometimes fails	Sometimes, while installing DFM on Solaris, the installation script displayed dependency handling errors and stopped. This was because there were special characters in the CD mount path. This has been fixed and the installation now proceeds correctly.
CSCsa80715	Notification Services hangs after 2 weeks	Trap recipients did not receive traps from Notification Services; also, there was no response when a user clicked a link on the Notification Services tab. This happened after the NOSServer process had been running continuously for about two weeks. This problem no longer occurs.
CSCsb40243	sm_server and brstart are not terminated when daemon manager stops	The sm_server and brstart processes are not terminated when the CiscoWorks daemon manager stops. If the daemon manager is restarted, two instances of both sm_server and brstart will be running, and the CPU will hang around 100%. The workaround is as follows: <ol style="list-style-type: none"> 1. Stop the daemon manager. 2. Kill or stop any remaining sm_server and brstart processes. 3. Restart the daemon manager.

Table 5 Problems Resolved in DFM 2.0.3 (Continued)

Bug ID	Summary	Explanation
CSCsa91950	restorebackup.pl displays incorrect instructions	If a user performed a remote upgrade to DFM 2.0 and ran the restorebackup.pl command, the command displayed upgrade instructions that were not up-to-date and not correct. The messages have been updated and corrected.
CSCsa97047	Remote upgrade completion message unclear	When performing a remote upgrade using the DFMRestore.pl command from the DFM 2.0 Upgrade Kit, the upgrade script generated an error message and the upgrade appeared to fail due to a problem with the DFM Broker. This problem no longer occurs.
CSCsa97839	Fatal errors when migrating polling/threshold data	Fatal errors were sometimes displayed while running the DFM12x-DFM20-upgrade.pl command and migrating polling and threshold data. This seemed to happen after migrating Resource Manager Essentials data. This problem no longer occurs.
CSCsa97928	E-Mail and Trap Notifier data is migrated but not displayed	Although Mail and Trap Notifier data was migrated from DFM 1.2.x to DFM 2.0, the data was not displayed by DFM 2.0. This was because TRAP_DEFAULT_FILE and EMAIL_DEFAULT_FILE were not defined in the <i>NMSROOT/object/nos/config/nos.properties</i> file. These are now defined and the data is displayed.
CSCsa98010	sm_ov_fwd does not run after remote HPOV-NV adapters installed	After installing the HPOV-NetView adapters on a remote host, sm_ov_fwd would not run. The process now runs correctly after the adapters are installed.
CSCsb04458	Changing homepage server name breaks DFM groups	If a user changed the homepage name to a value other than the hostname, DFM groups would break. This problem no longer occurs.
CSCsb06357	TCP port 8888 is not listed as used port in the documentation	DFM uses port 8888 for the DFMLogServer, but the port was not listed in the table of ports in the user guide and online help. This information has been added.
CSCsb14204	Solaris: DFM polling and threshold settings cannot be saved in Mozilla	Polling and Threshold values could not be saved when using a Mozilla-based browser (such as Mozilla or Netscape) on Solaris. The values are now saved.

Table 5 Problems Resolved in DFM 2.0.3 (Continued)

Bug ID	Summary	Explanation
CSCsb71371	Print and Export to PDF links in DDV do not work	If the user tried to Print or Export to PDF from the Detailed Device View, the links did not work. The links now work.
CSCsb75934	Solaris: Uninstall of HPOV-NetView Adapter alone is not possible	On Solaris, the user was not offered the option of uninstalling only the HPOV-NetView Adapter (which is useful on remote machines). This option is now displayed.
CSCsb76225	sm_nv_fwd does not run after remote HPOV-NV adapters installed	After installing the HPOV-NetView adapters on a remote host, sm_nv_fwd would not run. The process now runs correctly.
CSCsb77987	DFM prompts for license even if license was already provided	DFM prompted the user for a valid license even after a license had already been provided. This problem no longer occurs.
CSCsb89994	Trap recipients information is skipped after five entries	If a user tried to migrate more than five trap recipients (IP/hostnames) during an upgrade, after the upgrade, DFM displayed only the first five entries. The other information was lost. All recipient information is now migrated and displayed.
CSCsc12761	Remote upgrade license validation from 1.2.x fails	When validating an upgrade license on a remote server, the validation failed. This problem has been fixed.
CSCsc24189	E-Mail and Trap Notification data not displayed after remote upgrade	When upgrading from DFM 1.2.x to DFM 2.0.3, E-Mail and Trap Notification data was not migrated. The data is now migrated.
CSCsc28680	Local upgrade should not ask for proof of purchase	After a local (inline) upgrade to DFM 2.0.3, even if the user supplied the upgrade license information, DFM would nag the user for proof of purchase. This problem no longer occurs.
CSCsc53405	After migration, DFM times out waiting for DFM server process	After migrating data, DFM would time out when waiting for the DfmServer process to register with the DfmBroker process. This problem no longer occurs.

Table 5 Problems Resolved in DFM 2.0.3 (Continued)

Bug ID	Summary	Explanation
CSCsb86237	Cannot customize thresholds for Interfaces and Modules group	When a user selected Polling and Thresholds > Managing Thresholds and tried to customize thresholds for Cisco Interfaces and Modules, the Customize Settings page opened but did not display any settings that could be changed. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsa79675	Cannot read Detailed Device View screen	Detailed Device View columns in DFM 2.x were not readable because they were too small. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsb59510	DDV displays error page	<p>DFM occasionally displayed an error page when a user opened a Detailed Device View, clicked the device IP address radio button, and then clicked either the Device Attribute or Information link (on the right side of the page). This error was displayed:</p> <pre>Problem with File /WEB-INF/screens/ddv.jsp!!!Cannot find bean ddvhtmltable in scope null</pre> <p>This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).</p>
CSCsc18405	Trap and Syslog Notification recipients are cleared	<p>Existing trap and syslog recipients were sometimes cleared when a user tried to edit them. This happened when the user edited an existing subscription, and did the following:</p> <ol style="list-style-type: none"> 1. On the Trap Recipients page (after viewing the existing recipients information), click Back. The Notification Group and Subscription Name page is displayed. 2. Click Next. The previously existing host, ports, and comments entries are cleared. <p>This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).</p>

Table 5 Problems Resolved in DFM 2.0.3 (Continued)

Bug ID	Summary	Explanation
CSCsc92186	DFM does not support SHA-1 SNMPv3 authentication algorithm	DFM 2.0.3 could not discover devices using SNMPv3 with SHA-1 as its hashing algorithm, because DFM considered SHA-1 an invalid SNMP protocol. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsd31511	Rediscovery Schedule displays 500 Server Error	When a user selected Configuration > Other Configuration > Rediscovery Schedule , the system sometimes displayed a 500 Internal Server error. Investigation showed that this occurred predominantly when DFM was installed with Resource Manager Essentials (RME), and RME was running several periodic system jobs (collection, polling, purging, and so forth). This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsc49794	DFM does not add device using correct IP address	When a switch with multiple IP addresses was added to DFM, DFM did not use the specified IP address when creating the object instance in the DFM engine. This caused the device to go to the Unknown discovery state. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsc05115	DFM does not discover MeetingPlace Express as Host	DFM did not discover the Cisco MeetingPlace Express (1.3.6.1.4.1.9.1.710) as a host. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsb21876	Cat 3750: Standalone switches (without stack) not supported	DFM reported all Catalyst 3750 switches with the same OID, because DFM assumed they would be used in a stack: 3750-24FS, 3750-24PS, 3750-24TS, 3750-48PS, 3750G-16TD, 3750G-24PS, 3750G-24TS1U, 3750G-48PS, and 3750G-48TS. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsb57090	CSS device no longer supported because sysObjectID changed	For CSS 11503 and 11506 devices running WebNS 7.4 or higher, DFM did not correctly discover the devices. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).

Table 5 Problems Resolved in DFM 2.0.3 (Continued)

Bug ID	Summary	Explanation
CSCsc76777	Sup720 and NAM cards: Correct names not displayed	The Detailed Device View did not display the correct names for the Sup720 and NAM cards. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsc76732	3750: Support stack MIB	DFM did not generate any alerts if a 3750 switch was removed from the stack because it did not support the following CISCO-STACKWISE-MIB pass-through traps: cswStackPortChange cswStackNewMaster cswStackMismatch cswStackRingRedundant cswStackMemberRemoved This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsc53019	ASL ERROR in DFM.log file	The DFM.log file sometimes contained ASL-ERROR messages. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsd31319	Running notifications not sent when DFM is restarted	If a user restarted DFM, previously existing notifications stopped running. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsd00991	DFM should not create async interfaces on Access Servers	DFM was creating and managing all Access Server async interfaces (SLIP itType=28), even though they are logical interfaces. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).
CSCsc91394	Notification subscriptions do not work after upgrade to DFM 2.0.3	Notification subscriptions stopped working after upgrading to DFM 2.0.3. This was due to an NOSServer registration problem. This problem has been fixed in DFM 2.0.4 (see Additional Information Online, page 5).

Problem Resolutions Inherited from DFM 2.0 Service Pack 2

Table 5 lists all problems that were resolved in DFM 2.0 Service Pack 2.

Table 6 Problem Resolutions Inherited from DFM 2.0.2

Bug ID	Summary	Explanation
CSCsb12653	Custom roles in ACS overwritten when application/Service Pack installed	Custom ACS roles were overwritten when DFM 2.0 (or any DFM 2.0 service packs or patch/IDUs) were installed on a CiscoWorks machine that is configured to use ACS 3.3.x for its security mode. The roles are no longer overwritten.
CSCsa58207	Solaris: Warning says Solaris 2.9 not supported	When Patch/IDU 2.0.1 was installed on a Solaris 2.9 machine, CiscoWorks warned the user that the operating system was not supported. This was a spurious message and has been removed.
CSCsa57904	Device center and CV launched from AAD prompts for username/password	When the Device Center or CiscoView was launched from the Alerts and Activities display, CiscoWorks prompted the user for a username and password. This problem no longer occurs.
CSCsa66842	Interface utilization rate should be in % instead of bytes per sec	In the Detailed Device View, interface utilization was listed as bps. It is now listed as a percentage (%).
CSCsa45908	HighErrorRate event info is incomplete	The event details window of the HighErrorRate was incomplete. It did not display InputPacketErrorPct or ErrorPct. It now displays all information.
CSCsa67962	Rediscovery scheduler-error in log file	When a user configured a rediscovery schedule, the Rediscovery.log might report an error, and no rediscovery was performed. In addition, the Common Services Job Browser did not list the job. These problems no longer occur.
CSCsa47044	Event details window is not descriptive for c3845	The event details window for Cisco 3845 network adapter alarms did not display any information. The information is now displayed.

Table 6 *Problem Resolutions Inherited from DFM 2.0.2 (Continued)*

Bug ID	Summary	Explanation
CSCsa47936	Alerts and Activities Detail tools fail if SSL is enabled on DFM server	If SSL was enabled on the DFM server, any of the tools that were launched from the Tools drop-down list (on the Alerts and Activities Detail page) would fail. This was because the tools path was hard-coded to http, and if SSL were enabled, the proper path would be through https. This problem no longer occurs.
CSCsa58213	WLSE: Switchover trap not supported	When a WLSE switchover occurred (from standby to active), DFM did report an event but the switchover trap was not reported. This problem is fixed.
CSCsa58970	Online Help: Syslog listening port number is not correct	The online help incorrectly listed the listening port for syslog notifications as 512. It is 514. This has been corrected.

Problem Resolutions Inherited from DFM 2.0 Service Pack 1

[Table 5](#) lists all problems that were resolved in Service Pack 1 (also called Patch/IDU 2.0.1).

Table 7 *Problem Resolutions Inherited from DFM 2.0.1*

Bug ID	Summary	Explanation
CSCsa50868	Device takes too long to move to Known state	DFM sometimes required more than 30 minutes to move a device from Learning to Known. This was due to the following: <ul style="list-style-type: none"> • A problem with the DFM engine. • A communication glitch. This problem no longer occurs.

Table 7 Problem Resolutions Inherited from DFM 2.0.1 (Continued)

Bug ID	Summary	Explanation
CSCsa49406	Cannot launch drop-down tools from Alerts and Activities Detail page	When a remote instance of Cisco View or Campus Manager was registered with the CiscoWorks home page, and local versions of those applications were already registered, CiscoWorks could not launch tools from the Alerts and Activities Detail drop-down list. This was because CiscoWorks tries to open the remote link rather than the local link. This problem no longer occurs.
CSCsa41661	Solaris: Sun JDK problem causes some applications (Notification Services) to dump core file and quit after three days	<p>On Solaris machines, a Java problem occasionally caused Notification Services to dump core and quit after three days of notification forwarding. This occurred when the Solaris server was running in a heavy load environment (for example, when 50 events were received every polling cycle, and the polling cycle was every 4 minutes). The Alerts and Activities display and Fault History were not affected.</p> <p>The Sun JDK defect that caused this problem was tracked through a Common Services 3.0 bug (CSCeg26913). Sun recommends launching JVM with two options:</p> <ul style="list-style-type: none"> -server: Launches JVM as server JVM (rather than client JVM) -Djava.compiler=NONE: Creates meaningful stack trace for future troubleshooting
CSCsa45329	Solaris: DFM hogs CPU when DCR contains more than 5,000 devices	When the DCR contains more than 5,000 devices, the DFMOGSServer may hog CPU cycles due to processing issues. The CPU hogging may occur for four hours or more. This problem is less noticeable in dual CPU machines.
CSCsa45235	Port analysis is provided even when analysis is disabled	If a port was connected to a Layer 3 device (a router) and a user then disabled analysis on the port, DFM continued to analyze the port. This was due to an internal engine issue. This problem no longer occurs.

Table 7 Problem Resolutions Inherited from DFM 2.0.1 (Continued)

Bug ID	Summary	Explanation
CSCsa45801	DFM reports IF OperationallyDown events even when analysis is disabled	If a user disabled all interface/port analysis (using the Disable All Threshold Settings check box), DFM occasionally continued to provide interface fault information. This was because DFM applies reachability settings after applying connector port and interface settings. This problem no longer occurs.
CSCsa15285	DFM displays MPLS type as GENERIC	DFM displays Multiprotocol Label Switching (MPLS) interfaces as TYPE=GENERIC. (MPLS interfaces have an ifType=166.) These interfaces are now correctly displayed.
CSCin86754	DFM does not provide a way to list managed access ports	DFM did not provide the capability for listing all managed access ports. A script is now provided for listing ports and interfaces according to their type, name, group membership and managed status. Refer to the online version of <i>User Guide for Device Fault Manager</i> ; see Product Documentation, page 3 .
CSCin86756	Add TrafficRate attribute to UI	On some DFM devices, CurrentUtilization was listed as an exponential number. Users could not interpret this meaning, since the TrafficRate attribute was not listed. The attribute is now listed.
CSCsa49933	Broken help links in Group Administration	In the Group Administration windows, some of the Help links were broken. These are now working correctly.

Problem Resolutions Inherited from DFM 2.0

Table 8 lists all problems that were resolved in the DFM 2.0 release.

Table 8 Problem Resolutions Inherited from DFM 2.0

Bug ID	Summary	Explanation
CSCdx32239	Incorrect duplexity shown for router and switch interfaces and ports	<p>DFM did not always report correct duplexity for router and switch interfaces. One reason this happened was because of assumptions DFM made when port or interface duplexity was UNSPECIFIED. DFM now uses DuplexMode to specify the duplexity (UNSPECIFIED, by default) and DuplexSource to track the source of setting duplexity (NONE by default). DFM now uses this new algorithm to determine duplexity:</p> <ol style="list-style-type: none"> 1. DFM checks the portDuplexity MIB attribute in the CISCO-STACK-MIB, and: <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 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. <p>(continued)</p>

Table 8 *Problem Resolutions Inherited from DFM 2.0 (Continued)*

Bug ID	Summary	Explanation
CSCdx32239 (continued)	Incorrect duplexity shown for router and switch ifs and ports	<p>3. DFM checks the <code>cdpCacheDuplex</code> MIB attribute in the CISCO-CDP-MIB, and:</p> <ul style="list-style-type: none"> a. If the value is set to either half duplex or full duplex, DFM uses that setting for <code>DuplexMode</code> (for both local and remote ports), and sets <code>DuplexSource</code> to <code>NEIGHBOR_MIB</code>. b. If the value is unknown, DFM proceeds to Step 4. <p>4. If DFM cannot correctly determine the duplex mode (because it was not set manually or set by MIBs), DFM will set <code>DuplexSource</code> to <code>ASSUMED</code> and do the following:</p> <ul style="list-style-type: none"> 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 <code>Type="*ETHER*"</code> and its <code>MaxSpeed=10000000</code>.) b. For all other interfaces, DFM will assume the setting is full duplex.
CSCed27739	DFM manages MPLS logical interfaces, causing duplicate alarms	<p>DFM generated duplicate alarms for Multiprotocol Label Switching (MPLS) interfaces. This occurred because DFM managed logical interfaces, and MPLS logical interfaces have a separate <code>ifIndex</code>.</p> <p>Logical interfaces with <code>ifType:166</code> (MPLS) are now unmanaged by default.</p>

Table 8 Problem Resolutions Inherited from DFM 2.0 (Continued)

Bug ID	Summary	Explanation
CSCsa03104	DFM uses wrong OID to poll CPU utilization on PIX	<p>DFM did not report CPU utilization for PIX Firewalls because the algorithm used by DFM created the proper instrumentation when:</p> <ul style="list-style-type: none"> • cpmCPUTotalPhysicalIndex was nonzero, or • The OLD-CISCO-CPU-MIB was supported <p>For PIX Firewalls, cpmCPUTotalPhysicalIndex is always 0, and PIX Firewalls does not support OLD-CISCO-CPU-MIB.</p> <p>DFM still polls cpmCPUTotalPhysicalIndex, but the value of cpmCPUTotalIndex is verified instead. cpmCPUTotalIndex is used as the index.</p>
CSCea80669	ovtrapd cannot start after reboot because DFM occupies port 162	<p>If a user installed HP OpenView before DFM, HP OpenView used port 162 and DFM used port 9000. This is the correct behavior. However, if the user rebooted the device, the HP OpenView ovtrapd process could not start because DFM occupied port 162 as well as port 9000.</p> <p>Now, if DFM detects that HP OpenView or NetView is installed, DFM will only use port 9000. (However, if you want DFM to always use port 162 upon reboot—for example, if you remove HP OpenView and NetView—you can use the --privopen option to do so. Refer to the online version of <i>User Guide for Device Fault Manager</i>; see Product Documentation, page 3.)</p>
CSCeb12662	Layer 3 device port/interface handling is incorrect	<p>When an IP address was assigned to a port on the Catalyst 4506 running Cisco IOS (with Sup III), DFM displayed it as both a port and an interface.</p> <p>All multilayer switch ports, to which IP addresses are assigned, are now properly modeled as interfaces.</p>

Table 8 Problem Resolutions Inherited from DFM 2.0 (Continued)

Bug ID	Summary	Explanation
CSCdx64809	DFM should unmanage voice interfaces/ports	<p>In Cisco IOS devices running the Survivable Remote Site Telephony (SRST) feature, a VoiceEncapPeer interface (in ifTable) exists for each phone supported by SRST. These interfaces were operationally DOWN by default, since they were not being used while the local IP phones could reach their remote call manager. DFM generated an OperationallyDown event for these interfaces, which was incorrect, since this was the normal and expected state.</p> <p>DFM no longer generates an OperationallyDown event for these interfaces.</p>
CSCea11383	DFM should not treat voice dial peers as regular interfaces	DFM treated dial peer interfaces as physical interfaces and was managing them. These interfaces are now not managed because DFM recognizes them (by their ifType) as voice interfaces.
CSCdy43753	DFM cannot discover third power supply in Cat4000 switches	DFM could not discover the third power supply in Catalyst 4000 switches, even though the snmpwalk verified that the power supply was operational. DFM now correctly discovers the power supply.
CSCeb41000	DFM should suppress flapping if device restarts	When a device restarted, all associated interfaces sent link up and link down traps. If the number of restarts exceeded the Link Trap threshold, DFM reported excessive restarts and flapping (depending on the interface type) for all associated interfaces. The flapping event is now suppressed if the device restarts.
CSCdz14890	1% error threshold is too high for critical interfaces	The minimum for the error threshold (ifInerror) in DFM was 1% of the total number of packets, which was too high for high-bandwidth interfaces (such as Gbic and other WAN interfaces). The threshold can now be changed, because DFM 2.0 adds a new ErrorTraffic threshold. Refer to the online version of <i>User Guide for Device Fault Manager</i> ; see Product Documentation, page 3 .

Table 8 Problem Resolutions Inherited from DFM 2.0 (Continued)

Bug ID	Summary	Explanation
CSCdz86886	Cannot change PacketErrorRate threshold	The PacketErrorRate threshold could not be modified. The threshold can now be changed, because DFM 2.0 adds a new ErrorTraffic threshold. Refer to the online version of <i>User Guide for Device Fault Manager</i> ; see Product Documentation, page 3 .
CSCec42667	CSS11150 and CSS11050 switches generate incorrect memory exception	On CSS11150 and CSS11050 switches, DFM generated erroneous memory exceptions because instead of monitoring only the SCFM module, it was monitoring other modules (such as the EPIF module). DFM no longer monitors any modules besides the SCFM module.
CSCec77687	Filter out pass-through traps which are not related to managed devices	Whenever pass-through traps were received from unmanaged devices, they were displayed in the Monitoring Console. Pass-through traps for unmanaged devices are no longer displayed in the Monitoring Console.
CSCec30981	VLAN for L3 switches not displayed	DFM did not display VLAN information for Catalyst 4500 switches that perform Layer 3 routing. DFM now displays the VLAN information.
CSCea30379	DFM incorrectly reports CSS-11506 free memory	DFM reported insufficient memory alarms for the blades of some Content Switches because the cards are internal and had no memory on them. DFM will not report these errors (by unmanaging the cards) if it finds that no memory is configured in the module. This applies to modules 7 and 8 on the CSS11506 and module 4 on the CSS11503.
CSCdz71499	DFM reports Catalyst 6000 IDSM blade as undiscovered	When a Catalyst 6000 with an IDSM blade was added to DFM, DFM reported the blade as Undiscovered. This error occurred because IDSM blades do not support SNMP. DFM no longer tries to discover the IDSM blade, which is shown as a card in the parent switch.
CSCea11379	Memory not polled for 2948G	DFM did not poll memory components on the Catalyst 2948G. Memory components are now polled on the Catalyst 2948G.

Table 8 Problem Resolutions Inherited from DFM 2.0 (Continued)

Bug ID	Summary	Explanation
CSCdw23386, CSCdy83378, CSCdv53038, CSCdw91367	Improve ISDN modeling	These problems have been fixed through the improved ISDN interface model provided with DFM 2.0. Refer to the online version of <i>User Guide for Device Fault Manager</i> ; see Product Documentation, page 3 .
CSCea17909, CSCea15555	Interfaces incorrectly displayed	<p>When a port on a device that supports both Layer 2 and Layer 3, such as a Sup card running Cisco IOS, was assigned an IP address, it was displayed in the DFM Administration Console under both Interface and Port. It is now displayed under Interface.</p> <p>This fix also applies to the following devices:</p> <ul style="list-style-type: none"> • Catalyst C2955C-12 • Catalyst C2955T-12 • Catalyst C4506-with-Sup • Catalyst C4507-with-Sup • Catalyst C4503-with-Sup • Catalyst C3550-24-PWR • Catalyst C2955S-12 • WS-C2950ST-24-LRE
CSCdz09981	DFM Name Resolution fails if devices are in different DNS domain	DFM was not using the fully qualified domain name entered in the Essentials Inventory Device Name and Domain Name fields for name resolution. This problem no longer occurs.
CSCdw19930	DFM reports HSRP implementation as duplicate IP message	HSRP virtual IP addresses are no longer reported as duplicate IP addresses.

Table 8 Problem Resolutions Inherited from DFM 2.0 (Continued)

Bug ID	Summary	Explanation
CSCdx56957	Cat IOS devices: interfaces shown in both port and interfaces	<p>After adding a Catalyst device running Cisco IOS, Gigabit Ethernet GE1/1 and GE1/2 interfaces were displayed in both the Interface and Port groups.</p> <p>This behavior occurred because when you assigned an IP address to a port on a Catalyst switch, and the Catalyst switch was running the Cisco IOS operating system, DFM created an object in both the Port and Interface classes. The object in the Interface class represented a logical entity that DFM used to maintain connectivity information.</p> <p>This behavior has been fixed. Now, when a port has an IP address assigned to it, DFM will only display it in the Interface group. It will not be displayed in the Ports group.</p>
CSCdv88878	PPP interfaces are always classified as Backup and cannot be unmanaged	<p>DFM always classifies the PPP interfaces as Dial-on-Demand and thus generates a max-uptime event. DFM 2.0 provides a GUI feature through which users can disable interface and port analysis, thus suppressing event generation. Refer to the online version of <i>User Guide for Device Fault Manager</i>; see Product Documentation, page 3.</p>
CSCdz49270	DFM translates sysConfigChangeTime as date and time	<p>In sysConfigChange traps, DFM was incorrectly translating the sysConfigChangeTime, sometimes showing dates instead of a length of time since the last configuration change.</p> <p>Because there is currently no function that can map the MIB attribute SysConfigChangeTime to a time format consisting of hours/minutes/seconds, DFM will no longer display this MIB attribute in the sysConfigChange trap.</p>
CSCea24977	3725 SystemObjectID is incorrect	<p>The SystemObjectID was incorrect for the 3725. The OID has been corrected.</p>

Table 8 *Problem Resolutions Inherited from DFM 2.0 (Continued)*

Bug ID	Summary	Explanation
CSCdy27270	DFM 1.2.1 shows false PowerSupplyException for Cat3550	DFM displayed a power supply OperationalException for the Catalyst 3550, even though running the 'sh env all' command confirms that the power supply does not have any problems. DFM no longer displays this exception.
CSCdy77106	DFM needs to add support of Layer 3 Cat4006-SUP3 (WS-X4014)	DFM did not support the Cisco Catalyst Supervisor Engine III on the Catalyst 4006. DFM 2.0 adds this support.

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

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

Ordering Documentation

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

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

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

Documentation Feedback

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

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com

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

- Nonemergencies—psirt@cisco.com

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

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



Tip

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

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

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

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

Obtaining Technical Assistance

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

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

Cisco Technical Support & Documentation Website

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

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

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

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



Note

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

Submitting a Service Request

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

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

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

<http://www.ciscopress.com>

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

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions.
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

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

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

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


- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the “Product Documentation” section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2006 Cisco Systems, Inc.
All rights reserved.

 Printed in the USA on recycled paper containing 10% postconsumer waste.

