



Readme for Device Fault Manager 2.0 Service Pack 2 on Windows

5 July 2005

This Readme file is for Device Fault Manager (DFM) 2.0 Service Pack 2 on Windows. This Readme contains the following sections:

- [Description, page 2](#)
- [Related Documentation, page 3](#)
- [New Device Support, page 3](#)
- [Hardware and Software Requirements, page 8](#)
- [Downloading the Service Pack, page 9](#)
- [Installing the Service Pack, page 9](#)
- [Known DFM/Service Pack Problems, page 11](#)
- [Resolved DFM Problems, page 16](#)



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

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

**Note**

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

Description

DFM 2.0 Service Pack 2 is a collection of updated files. Like all service packs, Service Pack 2 is cumulative and contains:

- All of the device support provided by Service Pack 2 and Patch/IDU 2.0.1, which is listed in the [New Device Support, page 3](#).
- All of the bug fixes provided by Service Pack 2 and Patch/IDU 2.0.1, which are listed in [Resolved DFM Problems, page 16](#).
- Information on the new CISCO-DEVICE-EXCEPTION-REPORTING-MIB pass-through trap, `cdcrMonitoredExceptionEvent`. See the online help by clicking the Help button and selecting **Device Fault Manager > Processed and Pass-Through Traps, and Unidentified Traps and Events > Pass-through SNMP Unidentified Traps**.
- New functions and online help provided in Patch/IDU 2.0.1, which includes information on the new script for listing ports and interfaces according to their type, name, group membership and managed status. For more information, see the online help by selecting **Device Fault Manager > Using Device Management > Getting Started with Device Management > Listing Ports and Interfaces in the DFM Inventory**.

**Caution**

You cannot remove Service Pack 2 after installing it; to return to your original configuration, you will have to uninstall and reinstall DFM. Therefore, you should save your configuration before installing this service pack as described in [Installing the Service Pack, page 9](#).

Service Pack 2 contains only the updated files, not a complete DFM image.

Related Documentation

Information about DFM 2.0 is available from Cisco.com. Go to <http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/index.htm>.

**Note**

For the status of DFM bugs that are due to device-specific problems, refer to *Status of DFM Device Agent Bugs (DFM 1.x and 2.x)* on Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dev_sup/index.htm. That document is updated whenever a service pack is released.

**Note**

You should print out and read this document before installing Service Pack 2.

New Device Support

This section lists the device support provided by this service pack. The object identifiers (OIDs) for all devices are provided in the device support table for DFM 2.0. You can view this table on Cisco.com by going to http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dev_sup/dfm2_0.htm.

**Note**

Unless otherwise noted, these devices run the Cisco IOS operating system.

Service Pack 2 provides the following new device support:

- Cisco Content Networking Devices:
 - Cisco 500 Series Content Engines: CE511 (running ACNS)
- Cisco Interfaces and Modules:
 - Cisco Service Modules: RPM-XF (for MGX 8800 Series Switches)
- Cisco Routers:
 - Cisco Small Business Routers: SB101, SB106, SB107
 - Cisco 12000 Series Routers: GSR 12010

- Cisco Storage Networking:
 - Cisco MDS 9200 Series Multilayer Fabric Switches: MDS 9216A (running SAN-OS)
- Cisco Switches and Hubs:
 - Cisco Ethernet Switching Network Modules: Cisco Gigabit Ethernet Switch Module (CGESM, for HP Blade Server)
- Cisco Voice and IP Communications:
 - Cisco IP Contact Center products: IPCC (running ICM)
- Cisco Wireless:
 - Cisco Aironet 1130 AG Series: AP 1130

Table 1 Device Support Provided in DFM 2.0 Service Pack 2

Device	DFM 2.0	
	SP2	IDU 2.0.1
Cisco Broadband Cable		
Cisco UBR900 Series Cable Access Routers		
uBR 905	X	X
Cisco Content Networking Devices		
Cisco 500 Series Content Engines		
CE-511	X	
Cisco 4600 Series Content Distribution Managers		
CDM-4630	X	X
CDM-4650	X	X
Cisco Interfaces and Modules		
Cisco 2600 Series Content Engine Module CE 2636	X	X
Cisco Network Analysis Module for 2600/3600/3700 Series	X	X
Cisco 3201 Wireless Mobile Interface Card (WMIC) for Cisco 3200 Series Mobile Access Routers	X	X

Table 1 Device Support Provided in DFM 2.0 Service Pack 2

Device	DFM 2.0	
	SP2	IDU 2.0.1
Cisco Interfaces and Modules (continued)		
Cisco Catalyst 6500 & Cisco 7600 Series Communications Media Module (WS-SVC-CMM)	X	X
Cisco Service Modules: RPM-XF for MGX 8800 series switches	X	
Cisco Network Management		
Cisco Wireless LAN Solution		
Cisco Wireless LAN Solution Engine 2.8	X	X
CiscoWorks for Wireless LAN Solution Engine		
1030	X	X
1130	X	X
Cisco Optical Networking		
Cisco ONS 1540 Series		
ONS-15454	X	X
Cisco Routers and Routing Systems		
Cisco SOHO 70 Series		
SOHO 76	X	X
SOHO 77H	X	X
Cisco Small Business Routers		
SB101	X	
SB106	X	
SB107	X	
Cisco 1800 Series Integrated Services		
1841	X	X
Cisco MWR 1900 Mobile Wireless Routers		
MWR 1900	X	X

Table 1 Device Support Provided in DFM 2.0 Service Pack 2

Device	DFM 2.0	
	SP2	IDU 2.0.1
Cisco Routers and Routing Systems (continued)		
Cisco 2800 Series Integrated Services		
2801	X	X
2811	X	X
2821	X	X
2851	X	X
Cisco 3800 Series		
3825	X	X
3845	X	X
Cisco 12000 Series (Gigabit Switch)		
12010 GSR	X	
Cisco Security and VPN		
Cisco VPN 3000 Series Concentrators		
VPN 3002	X	X
Cisco 7100 Series VPN Routers		
7140-2FE	X	X
Cisco Storage Networking		
Cisco MDS 9200 Series Multilayer Fabric Switches		
MDS-9216A	X	
Cisco Switches and Hubs		
Cisco Catalyst 3560 Series		
3560G-24PS (IOS)	X	X
3560G-24TS (IOS)	X	X
3560G-48PS (IOS)	X	X
3560G-48TS (IOS)	X	X

Table 1 Device Support Provided in DFM 2.0 Service Pack 2

Device	DFM 2.0	
	SP2	IDU 2.0.1
Cisco Switches and Hubs (continued)		
Cisco Catalyst 3750 Metro Series		
ME-3750-24TE-MA AC switch (IOS)	X	X
ME-3750-24TE-MD DC switch (IOS)	X	X
Cisco Catalyst 4000 Series		
Catalyst 4948 (IOS)	X	X
Cisco Catalyst G-L3 Series Switches		
4908G-L3 (IOS)	X	X
Cisco Catalyst 6500 Series		
6509-NEBA (IOS)	X	X
Cisco Systems Intelligent Gigabit Ethernet Switch Module (IGESM) for IBM eServer BladeCenter	X	X
Cisco Gigabit Ethernet Switch Module (CGESM) for HP Blade Server	X	
Cisco Voice and IP Communications		
Cisco IAD 2400 Series Integrated Access Devices		
IAD 2420	X	X
IAD 2431-T1/E1	X	X
Cisco 7800 Series Media Convergence Servers		
7825H	X	X
7835H	X	X
7845I	X	X
Cisco IP Contact Center		
IPCC	X	

Table 1 Device Support Provided in DFM 2.0 Service Pack 2

Device	DFM 2.0	
	SP2	IDU 2.0.1
Cisco Wireless		
Cisco Aironet 340 Series		
AP340 (VxWorks)	X	X
Cisco Aironet 1130 Series		
AP 1130	X	

Hardware and Software Requirements

Service Pack 2 can be installed on a system running:

- DFM 2.0 (with or without Common Services 3.0 Service Pack 1)
- DFM 2.0 running with Patch/IDU 2.0.1 (with or without Common Services 3.0 Service Pack 1)

In addition to the hardware and software requirements needed for the initial installation of DFM 2.0, you must also install the Common Services MDF Package Version 1.2 or higher (see [Installing the Service Pack, page 9](#)). If you have installed Common Services 3.0 Service Pack 1, you have the required MDF package.

For information on installing DFM 2.0, refer to *Installing and Setting Up Device Fault Manager on Windows*. You can view this documentation on Cisco.com by going to:

<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm20/install/windows/index.htm>.

Downloading the Service Pack

Service Pack 2 files are downloaded in a compressed form. To prevent overwriting of files in existing directories as well as ensure that adequate disk space is available, users should download the files to a temporary working area of their server, and then uncompress the files.



Note

You can also use the Common Services Device Update function to download the service pack. For more information, from the Common Services home page, select **Software Center > Software Update** and click **Help**.

Step 1 Make sure you have adequate free space, then, from the DFM download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>, click the link to `cwdfm2_0_2_win.zip`, and follow the instructions to download the zip file to a temporary working area of your server.

Step 2 Unzip all files into the temporary working area.

Installing the Service Pack



Caution

You cannot remove Service Pack 2 after installing it; to return to your original configuration, you will have to uninstall and reinstall DFM. Therefore, you should save your configuration before installing this service pack as described in [Step 1](#).

Step 1 Make sure that you have a backup of your configuration, in case you need to revert back to it. (This service pack cannot be uninstalled.)

Step 2 Verify that Common Services MDF package version 1.2 (or higher) is installed: From the Common Services home page, select **Software Center > Device Update**.

- a. In the Products Installed table, click the CiscoWorks Common Services link. The Package Map page opens.

- b. Check the page under Patches Installed:
 - If MDF Package Version 1.2 (or higher) is listed, proceed to [Step 3](#).
 - If either MDF Package Version 1.2 (or higher) is not listed *or* no MDF package is listed, return to the Software Updates page, click **Help**, and follow the instructions to download the MDF package.

Step 3 Move to the directory in which the unzipped Service Pack 2 files reside, and run the installation script by double-clicking **cwdfm2_0_2_win.exe**.

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

- If you want to continue the installation (you will lose any ACS custom roles), click **Yes** and proceed to [Step 5](#).
- If you do not want to continue the installation (so you can change your AAA security mode to CiscoWorks Local and save any ACS custom roles), do the following:
 - Click **No**. (You will need to reset your mode to ACS after you have installed DFM, as described in [Step 9](#).) The installation will abort.
 - From the command prompt, run the following command:


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

Step 5 Follow the prompts in the installation script. The options displayed by the installation script depend on your configuration.

Step 6 When the installation is finished, click **Finish** to exit the installer.

Step 7 Verify the installation:

- a. From the Common Services home page, select **Software Center > Software Update**.
- b. In the Products Installed table, click the Device Fault Manager link. A page that lists all installed patches, packages, and applications is displayed.
- c. Verify that under Patches Installed, there is an entry for DFM2.0-SP2.

- Step 8** Rediscover the new devices using the DFM home page:
- If you are using automatic synchronization with the DCR, select **Device Management > Rediscover/Delete**.
 - If you are using manual synchronization with the DCR, select **Device Management > Device Selector** and add the devices to the DFM inventory. The devices will be rediscovered when they are added to DFM.
- Step 9** If you exited the installation in order to change your AAA security mode from ACS to CiscoWorks Local (in [Step 4](#)), reset your security role back to ACS. From the Common Services home page, select **Server > Security > AAA Mode Setup**, click **Help**, and follow the instructions.
- Step 10** Remove the distribution files from the temporary working area on your server.
-

Known DFM/Service Pack Problems

The following table describes the known problems in Service Pack 2. Unless otherwise specified, there is no workaround for these problems.



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.)

For a list of known problems in Device Fault Manager 2.0, go to http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm20/rel_note/win_rn.htm.



Note

For the status of other DFM bugs that are due to device-specific problems, refer to *Status of DFM Device Agent Bugs (DFM 1.x and 2.x)* on Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dev_sup/index.htm. That document is updated whenever a service pack is released.

Table 2 Known Problems in Service Pack 2

Bug ID	Summary	Explanation
CSCsb12653	Custom roles in ACS overwritten when application/Service Pack installed	<p>Custom ACS roles are overwritten when DFM 2.0 (or any DFM 2.0 service packs or patch/IDUs) are installed on a CiscoWorks machine that is configured to use ACS 3.3.x for its security mode. This is due to a Common Services defect (CSCsb07694).</p> <p>The installation software includes a warning message that explains the workaround, as follows:</p> <ol style="list-style-type: none"> Exit the installation and run the following command to reset the mode to CiscoWorks Local (the following command is one line): <pre style="margin-left: 40px;">NMSROOT/bin/perl NMSROOT/bin/ResetLoginModule.pl</pre> Restart the installation process. When the installation completes, reset the mode back to ACS from the Common Services home page (using Server > Security > AAA Mode Setup). <p>This information has been included in the service pack installation instructions (see Installing the Service Pack, page 9).</p>
CSCsa84962	DFM should not allow installation of Patch/IDU 2.0.1 on DFM SP2	If a user tries to install patch/IDU 2.0.1 on top of DFM 2.0 Service Pack 2, DFM should issue error messages, but it does not. There is no workaround.
CSCsa85635	DFM should allow installation of DFM 2.0 on DFM SP2	If a user tries to install DFM 2.0 on top of DFM 2.0 Service Pack 2, DFM issues an error and exits the installation. There is no workaround.

Table 2 Known Problems in Service Pack 2 (continued)

Bug ID	Summary	Explanation
CSCsa90722	Windows: Fatal messages in uninstallation log	When a Windows user uninstalls CiscoWorks by selecting Uninstall All, although the installation is successful, several fatal messages are written to the Ciscoworks_setup log. You should ignore the messages.
CSCsa56549	No prompt when patch/IDU or service pack is installed and user reinstalls	If the user tries to reinstall a patch/IDU or service pack that is already installed, DFM does not ask for confirmation that the user really wants to perform the reinstallation. On Solaris, a message informs the user that the patch/IDU or service pack is already installed and continues with the reinstallation. On Windows, DFM proceeds with the reinstallation without notifying the user of the existing installation. There is no workaround.
CSCsa66717	Patch/IDU or service pack install log summary message misleading	<p>Although a patch/IDU or service pack installation will correctly abort if an outdated MDF package is installed, the installation software will display the following message:</p> <pre>Possible Warnings/Errors Encountered- ===== No Errors were encountered during installation.</pre> <p>The Windows installation log will describe the problem (“MDF PSU package is not installed”), but the Solaris installation log will not.</p> <p>You should ignore the final message and install the appropriate MDF package from:</p> <p>http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-cd-one</p>

Table 2 Known Problems in Service Pack 2 (continued)

Bug ID	Summary	Explanation
CSCsa67346	3560-48PS, Metro 3750: Collision Rate event info shows null value	<p>The event details windows for collision rate displays the value of SingleCollisionFramesP 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>
CSCsa82905	CE-511: Port/interface alerts not generated	<p>The CE-511 does not compute CurrentUtilization because HighCounter MIBs are not implemented for interfaces with speeds greater than 20 Mbps. A bug has been opened against the CE-511 (CSCeh60145). There is no workaround.</p>
CSCsa81033	DFM generates discovery error messages for GSR-12010	<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 2 Known Problems in Service Pack 2 (continued)

Bug ID	Summary	Explanation
CSCsa80319	IPCC: Port/interface alerts not generated	The IPCC does not compute CurrentUtilization because HighCounter MIBs are not implemented for ETHERNETCSMACD interfaces with speeds greater than 1,000 Mbps. A bug has been opened against the IPCC (CSCeh62329). There is no workaround.
CSCsa83484	SB101 does not implement high counter MIBs	The SB101 does not compute CurrentUtilization because HighCounter MIBs are not implemented for PPP interfaces with maxSpeed = 100000000. An agent bug will be opened. There is no workaround.
CSCsb03285	GSR12010 does not report RepeatedRestarts	The GSR 12010 does not support the RepeatedRestarts fault because the device does not generate cold start and warm start traps. A bug has been opened against the GSR 12010 (CSCsb09818). There is no workaround.
CSCsa66807	DDV has 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. There is no workaround.</p>

Table 3 *Known Problems Inherited from Patch/IDU 2.0.1*

Bug ID	Summary	Explanation
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.
CSCsa53657	1841: Port/IF alarms not generated	The Cisco 1841 does not implement HighCounter MIBs. The 1841 has two interfaces of type ethernetCsmacd(6) with speeds of 100,000,000; therefore, the network adapter-related events are not generated. An agent bug will be opened. There is no workaround.
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.

Resolved DFM Problems

The following table describes DFM problems that are resolved in Service Pack 2.

Table 4 *Problems Resolved in Service Pack 2*

Bug ID	Summary	Explanation
CSCsa64852	Windows: CW daemons not restarted after MDF package check	On Windows, if the software detected that the required MDF package was not installed, the installer terminated but did not restart the CiscoWorks daemons. The daemons are now restarted.

Table 4 Problems Resolved in Service Pack 2 (continued)

Bug ID	Summary	Explanation
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.
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 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.

Table 4 *Problems Resolved in Service Pack 2 (continued)*

Bug ID	Summary	Explanation
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 in the online help packaged with this patch/IDU, and in the Cisco.com documentation.

Table 5 *Problems Resolutions Inherited from Patch/IDU 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.
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.
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 5 Problems Resolutions Inherited from Patch/IDU 2.0.1

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. This patch/IDU provides a new script for listing ports and interfaces according to their type, name, group membership and managed status. For more information, see the online help by selecting Device Fault Manager > Using Device Management > Getting Started with Device Management > Listing Ports and Interfaces in the DFM Inventory.
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. This patch/IDU adds the TrafficRate attribute to the DFM user interface.
CSCsa49933	Broken help links in Group Administration	In the Group Administration windows, some of the Help links were broken. This patch/IDU fixes these broken links.

