

How is DFM 2.x Different from DFM 1.2.x?

The differences between DFM 2.x and DFM 1.2.x are listed in the following sections:

- [What's New in DFM?](#), page B-1
- [Behavior Changes](#), page B-2
- [User Interface Changes](#), page B-3
- [Terminology Changes](#), page B-6
- [Device Group Changes](#), page B-6
- [Protocol Support Updates](#), page B-8

What's New in DFM?

DFM 2.x provides a completely new user interface and many new features:

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

DFM 2.x also introduces Search by Group; in addition to searching Fault History by device and by alert or event ID, you can search by device group.

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

More detailed notification messages—When an alert occurs, DFM generates an SNMP trap using CISCO-EPM-NOTIFICATION-MIB. The SNMP trap format includes the attributes of the alert and the events that caused the alert. For more information, see Appendix C, “Notification MIB,” in *User Guide for Device Fault Manager 2.0.6*.



Note The SNMP Trap Notifier MIB is no longer used.

- **Easier notification configuration**—You can fully configure e-mail notification and trap notification from the DFM user interface without the need to modify the configuration on the management server.
- **SYSLOG notification**—DFM adds SYSLOG notification.
- **Additional security**—DFM supports:
 - SSL protocol between the client and the server.
 - SNMP V3 protocol (authNoPriv) between the server and the device.
 - Integration with Cisco Secure Access Control Server (ACS).
- **Automatic device import**—DFM integrates with the Common Services Device and Credentials Repository (DCR) and, by default, automatically imports devices from DCR.
- **Integration with Device Center**—Common Services Device Center is a device troubleshooting tool. DFM integrates with Device Center so that from Device Center, you can:
 - View active fault details: If there is an active fault, the alert ID is displayed on Device Center. You can click the alert ID to open a display with event details, alert status, description, duration, and the date and time the alert was last updated.
 - Launch a Fault History report for the device.

Behavior Changes

Discovery

- DFM now pings a device before performing discovery. This has the following effects:
 - Discovery fails if a device is using a proxy IP. Reconfigure the device access level to use ICMP only.
 - Discovery fails if a device's IP is a virtual IP. Reconfigure the device to use a valid IP address.
- Discovery of device cards is enhanced because DFM checks the cardTable attribute in OLD-CISCO-CHASSIS-MIB.
- DFM does not create interfaces of type ISDN, LAPD, and Other for Cisco Access Routers.
- After you upgrade DFM, you will see an increase in the number of ports and interfaces that are managed for the following devices:
 - Cisco MDS 9000 Series Multilayer Switches
 - Cisco SN 5400 Series Storage Routers
 - Cisco Catalyst 2950 Series Switches (2950-ST-24-LRE, 2955C-12, 2955S-12, 2955T-12)
 - Cisco Catalyst 3550 Series Switches (3550-24-PWR-SMI and -EMI)
 - Cisco Catalyst 3750 Series Switches (3750-stack)

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

Additional MIB Support

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

User Interface Changes

The DFM 2.x user interface is quite different from that of DFM 1.2.x. To help you access the applications you need to use, [Table B-1](#) lists the click-by-click navigation paths you would use to access functions in DFM 1.2.x. Then it provides the comparable navigation paths to use in DFM 2.x.

Table B-1 DFM 1.2.x Navigation Compared to DFM 2.x Navigation

DFM 1.2.x	DFM 2.x	DFM 2.x Description
Device Fault Manager > Administration > Administration Console	Device Fault Manager > Alerts and Activities (From the DFM home page) Alerts (From the Alerts and Activities display, click a device to open a Detailed Device View.)	From the Detailed Device View, you can: <ul style="list-style-type: none"> • View device detail information • Manage and unmanage devices • Acknowledge alerts • Annotate events
	(From the CiscoWorks home page) Common Services > Device and Credentials > Device Management Device Fault Manager > Device Management > Device Selector (From the DFM home page) Device Selector	Device management, such as add, import, and delete. Note In DFM 2.x, you import devices into a Device and Credentials Repository (DCR) that is shared by CiscoWorks applications. You select devices from the DCR (or automatically synchronize devices with the DCR) for DFM to manage.
	Device Fault Manager > Device Management > Device Details (From the DFM home page) Device Details	View device inventory.
	Device Fault Manager > Configuration > Polling and Thresholds (From the DFM home page) Configuration > Polling and Thresholds	Configure polling parameters and manage thresholds.
	Device Fault Manager > Configuration > Polling and Thresholds > Polling parameters	Edit the polling parameters.
	Device Fault Manager > Configuration > Polling and Thresholds > Managing Thresholds	Edit the thresholds.
	Device Fault Manager > Configuration > Polling and Thresholds > Apply Changes	Apply the changes to use updated polling parameters and threshold values.

Table B-1 DFM 1.2.x Navigation Compared to DFM 2.x Navigation (continued)

DFM 1.2.x	DFM 2.x	DFM 2.x Description
Device Fault Manager > Monitoring Console	Device Fault Manager > Alerts and Activities (From the DFM home page) Alerts	Alarm display from which you can: <ul style="list-style-type: none"> • Launch tools, such as Fault History and Common Services Device Center • Export data to a PDF file or a comma-separated-values file • Print data You can also change the display to show the information that interests you most, as follows: <ul style="list-style-type: none"> • Select and create views or groups of device groups; use a view that contains the device groups of interest to you. • Filter the display to show alerts based on their severity, status, and originating device.
Device Fault Manager > Administration > Device Discovery > Change Probe	Device Fault Manager > Device Management > Device Selector (From the DFM home page) Device Selector Note The change probe process is obsolete in DFM 2.x.	Select devices manually or configure DFM to automatically synchronize device inventory with Device and Credentials Repository (DCR). Note Applications on different servers can use the same master DCR. For more information, see <i>User Guide for CiscoWorks Common Services 3.0.6</i> .
Device Fault Manager > Administration > Device Discovery > Rediscovery Schedule	Device Fault Manager > Configuration > Other Configurations > Rediscovery Schedule (From the DFM home page) Rediscovery Schedule	<ul style="list-style-type: none"> • Edit the default rediscovery schedule. • Create additional rediscovery schedules.
Device Fault Manager > Administration > Trap Configuration > Trap Receiving	Device Fault Manager > Configuration > Other Configurations > SNMP Trap Receiving	Change the port number that DFM uses to listen for SNMP traps. Note Although the SNMP Trap Adapter file used in DFM 1.2.x is still present in the DFM 2.x filesystem, DFM 2.x does not use it.
Device Fault Manager > Administration > Trap Configuration > Trap Forwarding	Device Fault Manager > Configuration > Other Configurations > SNMP Trap Forwarding	Configure hostnames and port numbers for trap forwarding. Note Although the SNMP Trap Adapter file used in DFM 1.2.x is still present in the DFM 2.x filesystem, DFM 2.x does not use it.
Device Fault Manager > Administration > Fault Notification > File Notifier	—	If you need to log events to a file, contact the Technical Assistance Center for the workaround for CSCsa83426.

Table B-1 DFM 1.2.x Navigation Compared to DFM 2.x Navigation (continued)

DFM 1.2.x	DFM 2.x	DFM 2.x Description
Device Fault Manager > Administration > Fault Notification > Mail Notifier	Device Fault Manager > Notification Services > E-Mail Notification (From the DFM home page) Notification Services > E-Mail Notification	Configure e-mail notifications for alarms. Note Although the Mail Notifier Adapter file used in DFM 1.2.x is still present in the DFM 2.x filesystem, DFM 2.x does not use it.
Device Fault Manager > Administration > Fault Notification > Trap Notifier	Device Fault Manager > Notification Services > Trap Notification (From the DFM home page) Notification Services > Trap Notification	Configure trap notifications for alarms. Note Although the Trap Notifier Adapter file used in DFM 1.2.x is still present in the DFM 2.x filesystem, DFM 2.x does not use it.
Device Fault Manager > Administration > Fault History Database Sizing	Device Fault Manager > Configuration > Other Configurations > Daily Purging Schedule	Trim the Fault History database. Note DFM 2.x keeps 31 days of history and trims the database daily at the time you specify.
Device Fault Manager > Fault History: <ul style="list-style-type: none">• Search by Devices• Search by Fault Conditions	Device Fault Manager > Fault History: <ul style="list-style-type: none">• Alert Filtering<ul style="list-style-type: none">– Search Alarm ID– Search by Device– Search by Group• Event Filtering<ul style="list-style-type: none">– Search by Event ID– Search by Device– Search Alert ID– Search by Group (From the DFM home page) Fault History	Generate a 31-day Fault History report based on search criteria.
	Device Fault Manager > Alerts and Activities > Tools > Fault History (From the DFM home page) Fault History	Generate a 24-hour Fault History report for all alerts in your current view.
	Device Fault Manager > Alerts and Activities Click an alert ID. The Alerts and Activities Detail display appears. In the Tools column next to the device component of interest, select Fault History . (From the DFM home page) Alerts	Generate a 24-hour Fault History report for all events on a device component.

Terminology Changes

Terminology has changed since DFM 1.2.x as follows:

- *Symptom* is replaced by *event*. Events are rolled up into *alerts*.
- *Compound* is not used and there is no replacement. A compound differs from an alert; there could be multiple compounds on a single device, whereas an alert is a roll-up of all events for a device.
- Levels of device certification (*validated*, *certified*, *template*, *undiscovered*, *uncertified*) are replaced by new device states:
 - *Known*—The device is successfully imported and fully managed by DFM. (Corresponds to *validated* and *certified*).
 - *Learning*—DFM is discovering the device. This is the initial state, when the device is first added to DFM or is being rediscovered.
 - *Questioned*—DFM cannot manage the device. (Can sometimes correspond to *undiscovered*.)
 - *Pending*—The device is being deleted. DFM is waiting for confirmation from all of its data collectors before purging the device and its details.
 - *Unknown*—The device is not supported by DFM. (Corresponds to *unsupported* and *uncertified*).
- *Manage* is replaced by *Activate*; *unmanage* is replaced by *suspend*.
- When a DFM 1.2.x fault was *acknowledged*, it was removed from the Alarm Log. In DFM 2.x, when an event is *acknowledged*, it remains in the Alerts and Activities display.
- DFM 1.2.x assigned devices to groups based on *matching criteria*. DFM 2.x assigns devices to groups based on *group rules*.
- DFM 2.x eliminates the term *device class* and introduces *device type*.
- DFM 1.2.x displayed managed elements organized by *device class*—for example: *Bridge*, *Host*, *Hub*, *MSFC*, *Probe*, *Router*, *RSM*, *Switch*. DFM 2.x displays devices organized by *device group*:
 - Inventory device groups are organized by device state.
 - Polling and Threshold groups are organized by device type; for example, Routers, Switches and Hubs, and Voice and Telephony. (For more information, see *User Guide for Device Fault Manager 2.0.6*.)

Device Group Changes

In DFM 1.2.x, you could browse the device inventory by selecting a device class. In DFM 2.x, you can examine device groups.

Table B-2 Device Group Changes

DFM 1.2.x Device Classes	DFM 2.x Device Groups
Bridge	Wireless
Host	Cisco Interfaces and Modules
	Content Networking
	Network Management
	Voice and Telephony

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

DFM 1.2.x Device Classes	DFM 2.x Device Groups
Hub	Switches and Hubs
MSFC	Cisco Interfaces and Modules
Probe	Cisco Interfaces and Modules Network Management
Router	Broadband Cable Cisco Interfaces and Modules Content Networking Routers Security and VPN Switches and Hubs Universal Gateways and Access Servers Voice and Telephony Wireless
RSFC	Cisco Interfaces and Modules
RSM	Cisco Interfaces and Modules
Switch	Content Networking DSL and Long Reach Ethernet (LRE) Optical Networking Routers Storage Networking Switches and Hubs Wireless Voice and Telephony
Terminal Server	Universal Gateways and Access Servers

Protocol Support Updates

Table B-3 *Protocols*

Protocol	DFM 1.2.x	DFM 2.x
SSL	Not SSL-compliant	Uses SSL protocol between the server and the browser. You enable and disable SSL for the server. See <i>User Guide for Common Services 3.0.6</i> .
SNMP	<ul style="list-style-type: none"> • Supports SNMPv1 and SNMPv2 for polling and receiving traps • Forwards traps as SNMPv2 	<ul style="list-style-type: none"> • Supports SNMPv1 and SNMPv2 for polling and receiving traps. • Forwards traps as SNMPv2. • Partially supports SNMPv3: <ul style="list-style-type: none"> – Uses SNMPv3 protocol between the server and the device. – Supports the Authentication No Privacy (authNoPriv) option.