

# CiscoWorks2000 Fault Management Integration



AVVID Partner Program: Network and Service Management Solution  
 Device Fault Manager (DFM) provides real-time fault analysis for Cisco devices. Through a variety of data-collection and -analysis techniques, DFM generates “intelligent Cisco traps,” which can be forwarded to other multi-device, multi-vendor event-management systems installed in the network, sent to e-mail/pager gateways, or displayed in the DFM alarm window.

The following companies listed in the table below are integrating their products with DFM.

Company	Application
Aprisma	Aprisma SPECTRUM
Hewlett-Packard	HP OpenView Network Node Manager
Tivoli	Tivoli NetView
LOGEC Systems Inc.	LOGEC Event Correlation (for HP OpenView Network Node Manager users)
Atlantis Software	NotificationWorks Adapter for CiscoWorks2000 Device Fault Manager
SMARTS	InCharge Connectivity

Users can forward the intelligent Cisco traps from DFM to a third party fault management system by first editing the trap notifier file described in the “Configuring DFM Adapters” chapter of the Device Fault Manager User Guide at: [http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm1\\_0/user/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm1_0/user/index.htm). Users need to input the appropriate IP address of the management system in this file. Second, users must enable third party fault management systems to receive the traps. Instructions on enabling this feature in third-party applications are listed below.

When sending DFM traps to multiple trap recipients, please refer to the following release notes at [http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm1\\_0/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm1_0/index.htm).

- View AVVID Partners providing CiscoWorks2000 Fault Management Integration



## Aprisma SPECTRUM and CiscoWorks2000 DFM Integration

Aprisma Management Technologies, a leader in scalable e-business infrastructure management, is proud to announce its integration with the CiscoWorks2000 DFM. With this integration, SPECTRUM will assure reliable operation of the Cisco-based, business-critical networks through its advanced fault isolation, configuration management and root-cause analysis capabilities. The integration between SPECTRUM and CiscoWorks2000 DFM increases the sophistication of Spectrum's fault isolation capability by providing a more in-depth analysis of Cisco device performance, environmental conditions, forwarding errors and system resource availability.

By leveraging the Cisco intelligent traps from DFM within SPECTRUM, users gain more insight into the operational status of the managed Cisco devices within their network. The integration enables customers to monitor critical ports, understand device capacity limitations, detect when faults are occurring and finally, take action to rectify the problem. Customers will also experience a reduction in load on the SPECTRUM server because the impact of simple network management protocol (SNMP) polling queries are minimized by providing polling and thresholding for critical devices from a single source.

This is the adapter script for integrating Cisco DFM with Aprisma's SPECTRUM 6.0r0 and 6.0r1. This script will allow the Generic Device (GnSNMPDev) model type to recognize traps forwarded from the DFM. Users can download the adapter script at <http://www.aprisma.com/partners/developers/cisco/dfm.html>

### Requirements:

- Windows NT 4.0, Windows 2000, or Solaris 5.7
- SPECTRUM 6.0r0 or 6.0r1

### Installation Instructions:

1. Put dfmintegrate.jar into an empty (temporary) directory.
2. Open a shell window (ksh on Solaris, bash on Windows).
3. Become the root user on Solaris.
4. a) If this machine only has SpectroSERVER installed, run `./dfmintserv.sh`  
b) If this machine only has SpectroGRAPH installed, run `./dfmintgraph.sh`  
c) If this machine has both the SpectroSERVER and SpectroGRAPH installed, run `./dfmintegrate.sh`

### Instructions for use:

DFM traps will now be recognized by SPECTRUM. The SpectroSERVER or SpectroGRAPH must be restarted before DFM trap integration can be utilized. To see DFM traps in SPECTRUM, model the DFM server as a GnSNMPDev. DFM traps will appear in the EventLog, attached to the model of the DFM server.

For additional support, contact the SPECTRUM hotline:

Email: [spectromail@aprisma.com](mailto:spectromail@aprisma.com)

Phone: 603-334-2700



## HP OpenView NNM and CiscoWorks2000 DFM Integration

CiscoWorks2000 DFM integrated with HP OpenView NNM brings you even more intelligence in managing your Cisco environment the smart way. Now you can take advantage of the new DFM information with HP OpenView Network Node Manager 6.1.

With the HP OpenView free integration package, saving users time and money in creating an integrated solution, HP OpenView NNM now receives Cisco product-specific, intelligent traps from CiscoWorks2000 DFM. These intelligent traps bring a new level of granularity to managing Cisco events. Now you can get in-depth, trap data that only Cisco can provide on its own devices.

With richer information, now the event correlation technology of NNM can give users an even more complete picture of the enterprise network. As the network becomes more and more pivotal to service availability, understanding the root cause of events across the infrastructure is more important than ever. With the expert help text of NNM applied to these Cisco alarms, users can quickly and easily diagnose problems, allowing them to maintain service availability and proactively avoid network service disruptions.

This integration is only part of the HP OpenView Smart Way to Manage Your Cisco Environment solution, helping you to quickly take control of your Cisco network. For more information visit: <http://www.openview.hp.com/smartway>.

## Tivoli NetView and CiscoWorks2000 DFM Integration

Tivoli NetView is a heterogeneous network management solution that enables users to discover TCP/IP networks, display network topologies, correlate and manage events and SNMP traps, monitor network health, and gather performance data. Tivoli NetView now integrates with CiscoWorks2000 DFM. This integrated solution enables a singular focus on networking problems.

To enable Tivoli NetView to receive the DFM specific traps, follow the steps listed below on each Tivoli NetView server.

Note: The procedures are the same on Unix and NT, but the scripts are slightly different.

1. Download the integration script from the Tivoli DFM page on the Tivoli NetView Web site (<http://www.tivoli.com/products/index/netview/>). Click on the DFM integration link and download the appropriate file. Dfm.bat (NT)/dfm.sh (Unix).
2. As root, run the downloaded script
3. On the CiscoWorks2000 server machine, which is running DFM, a few changes need to be made:
  - Under CW2000\_ROOT/objects/smarts/conf/notifier, edit the file trap\_notify.conf. Add a recipient entry for each of your NetView servers that should receive these traps. The entries are in the form of ("hostname," TRAP\_PORT, "1") where TRAP\_PORT is normally 162 and hostname is the host name of the NetView server.
  - Under the CW2000 main page, click on CiscoWorks2000 server>>Administration>>Process Management>>Start Process. Select Dfm TrapNotifier and click finish.
4. Done. DFM traps should now be visible in the event window in NetView.

For additional information please visit the Tivoli NetView web site at: <http://www.tivoli.com/products/index/netview/>



## LOGEC Event Correlation and CiscoWorks2000 DFM Integration

LOGEC Systems provides event-correlation software, analyzing messages captured by NNM and suppressing and prioritizing them to highlight the most important that require action.

LOGEC Correlation software for NNM is able to accept and correlate the new DFM intelligent traps. The intelligent traps will enable the correlations to provide more pertinent information to NNM administrators. In addition, you can use the LOGEC correlations to relate the intelligent traps to other OpenView-generated traps for improved error reporting. Using LOGEC's Cisco Syslog Converter, you can also correlate Cisco router syslog information with the DFM traps to provide problem resolution.

LOGEC Systems has developed a "Cisco Starter Pack," designed specifically to complement CiscoWorks2000 and HP OpenView for managing Cisco devices in an enterprise network environment. The Cisco Starter Pack consists of two types of software integration solutions:

The LOGEC Syslog Converter reads Cisco router information from the syslog file and converts selected messages to SNMP traps. These converted traps are then forwarded to NNM, making them available for event correlation or any other application. This setup not only makes router information available for any older devices that may not have an option to broadcast SNMP traps, but also allows the LOGEC Syslog Converter user to control (that is, limit) which classes of messages are converted to SNMP traps. It also sets trap priorities based on event type.

The second is a set of commonly used event-correlation software products to manage the flood of messages captured by NNM and convert them into a flow of information to identify, correlate, and prioritize messages for network administrators to effectively manage their networks. The LOGEC Cisco Starter Pack incorporates three correlation products that reduce the alarms generated within NNM based on duplicates, transients (that is, intermittent problems), or specific field values. The "Cisco Starter Pack" is downloadable at <http://www.logec.com>. For additional information please email [support@logec.com](mailto:support@logec.com).

## Atlantis Software NotificationWorks and CiscoWorks2000 DFM Integration

Atlantis Software Inc., a leader in network management notification, is proud to announce its integration with the CiscoWorks2000 DFM. All NotificationWorks modules can integrate with DFM, enabling customers to forward alarms to pagers, e-mails, and cell phones, vocalize alarms through sounds cards, or escalate alarms when an event is not handled by the assigned technician within the scheduled time. NotificationWorks is modular based, allowing customers to purchase only those modules they need. NotificationWorks is modular based, allowing customers to purchase only those modules they need. The scheduling and filtering of alarms is very comprehensive; alarms can be scheduled and filtered based on hour of the day, day of the week, alarm name, affected node, alarm message content, even duplication alarms can be filtered, and much more. See the list of the NotificationWorks modules at

<http://www.atlantissoftware.com/products.shtml>.

Integration with DFM is accomplished by using our NotificationWorks Adapter for CiscoWorks2000 DFM. This module converts the "intelligent Cisco traps" from DFM and translates them into over 50 specific alarms. Each alarm can then be handled using any NotificationWorks module. For instance, if you would like to have the alarms forwarded to pagers with scheduling that is comprehensive and granularly then you would also use our PageManager Pro module. Together these two modules will provide the ability to be notified via pagers, e-mails, and cellular phones for all of the "intelligent Cisco traps."

**Requirements for NotificationWorks:**

- Windows NT 4.0, Windows 2000
- NotificationWorks Adapter for CiscoWorks2000 Device Fault Manger
- For Paging, E-Mail notification—NotificationWorks' PageManager Pro Module
- For Alarm Vocalizing—NotificationWorks' Alarm Vocalizer Pro Module
- For Escalation Tracking and Accountability—NotificationWorks' Escalation Manager

Note: CiscoWorks2000 DFM can run on NT or Solaris. Users can run the two applications on separate servers and still enable integration.

**Installation Instructions:**

1. Configure the CiscoWorks2000 Trap Notifier Adapter to forward traps to the IP address of the PC running NotificationWorks
2. On the PC running NotificationWorks, enable the Windows NT/2000 SNMP trap service.
3. Install NotificationWorks by running setup. When prompted for which modules to install, select Adapter for CiscoWorks2000 DFM module and the other NotificationWorks modules you would like to use. For instance, if you would like paging notification, then also select the PageManager Pro module.
4. Schedule the CiscoWorks2000 DFM alarms by consulting that module's documentation.

**Instructions for use:**

CiscoWorks2000 DFM traps will now be recognized by NotificationWorks. The scheduling of the traps is dependent on the NotificationWorks module being used. Consult the appropriate module documentation.

For additional support, contact the Atlantis Software:

Email: [asinfo@atlantissoftware.com](mailto:asinfo@atlantissoftware.com)

Support Forum: <http://www.atlantissoftware.com/support.shtml>

Phone: 510-796-2180

**SMARTS InCharge Connectivity and DFM**

SMARTS InCharge software solutions isolate multi-vendor root-cause network, system, service and application failures and identify their effects on other parts of the IT infrastructure. The InCharge product family, including InCharge Connectivity for Networks is designed to interoperate and leverage CiscoWorks2000 DFM, enabling users to deploy both CiscoWorks2000 and InCharge solutions in the same network. By using both solutions customers will understand what the problems are that affect Network and Application availability with InCharge, and will have an in-depth understanding of how individual Cisco devices are performing by using DFM.

To integrate DFM analysis into the SMARTS Connectivity products is a two-step process. The first is to start the InCharge Connectivity Console, and the second is to attach and configure that same console to the DFM server to receive DFM notification. Below find the details of each step.

**Step One:**

- Start the InCharge monitoring console.
- When the console is started an attach server dialog will be displayed first prompting the user to attach to a domain manager.
- The attach dialog has two fields Broker and Domain.
- The Broker field should contain the value <host>:426 where <host> is the host where InCharge was installed.
- Select a domain manager from the pull down list in the Domain field.
- Click Apply to attach.

## Step Two:

- From the Domain menu option choose Attach.
- An attach server dialog will be displayed prompting the user to attach to a domain manager.
- Now change the broker field to specify the host where DFM is installed. The Broker field should contain the value <host>:426 where <host> is the host where DFM was installed and 426 is the standard broker port for DFM 1.0.
- Once the broker field is changed click on the domain field and select the DFM server of your choice from the pull down list.
- Click OK to attach to the domain.

If the user wishes to perform administrative functions for the InCharge or DFM application, they should use the Administration console installed for each of the products separately. The Administration Console is not designed to be interoperable between DFM and InCharge applications.

For additional information please email [support@smarts.com](mailto:support@smarts.com)



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

European Headquarters  
Cisco Systems Europe  
11, Rue Camille Desmoulins  
92782 Issy-les-Moulineaux  
Cedex 9  
France  
[www.cisco.com](http://www.cisco.com)  
Tel: 33 1 58 04 60 00  
Fax: 33 1 58 04 61 00

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems Australia, Pty., Ltd  
Level 9, 80 Pacific Highway  
P.O. Box 469  
North Sydney  
NSW 2060 Australia  
[www.cisco.com](http://www.cisco.com)  
Tel: +61 2 8448 7100  
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

**Cisco.com Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic

Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel  
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal  
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden

All contents are Copyright © 1992-2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement. Printed in the USA. AccessPath, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, CiscoLink, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Discover All That's Possible, Fast Step, Follow Me Browsing, FrameShare, FormShare, GigaStack, IGX, IP/VC, IQ Breakthrough, IQ Expertise, IQ FastTrack, IQ logo, IQ Net Readiness Scorecard, Internet Quotient, MGX, the Networkers logo, Packet, PIX, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company (0101R) 02/01 BWXXXX