



Preface

This preface describes the audience, organization, and conventions of the *Cisco MDS 9000 Family Fabric Manager User's Guide*. It also provides information on how to obtain related documentation.

Audience

This guide is for system administrators who intend to use the Cisco Fabric Manager to configure and monitor the switches that build the network fabric.

You should be familiar with the basic concepts and terminology used in internetworking, and understand your network topology and the protocols that the devices in your network can use. You should also have a working knowledge of the operating system on which you are running Fabric Manager, such as Microsoft Windows, Linux, or Solaris.

Organization

This document contains the following chapters:

- **“New and Changed Information”**—Summarizes the new and changed features for the *Cisco MDS 9000 Family Fabric Manager Switch Configuration Guide*.
- **Chapter 1, “Product Overview”**—Presents an overview of the Cisco MDS 9000 Family of multilayer switches and directors.
- **Chapter 2, “Getting Started with Cisco Fabric Manager”**—Provides a brief overview of Fabric Manager components and capabilities, and information on installation and launching the applications.
- **Chapter 3, “Overview of Fabric Manager”**—Provides in-depth descriptions of GUIs and capabilities for Fabric Manager Client, Fabric Manager Server, Device Manager, and Performance Manager.
- **Chapter 4, “Before You Begin”**—Discusses some things to be aware of before installing your switch.
- **Chapter 5, “Obtaining and Installing Licenses”**—Provides information on the Cisco MDS 9000 Family licensing model, license concepts, and license installation and management.
- **Chapter 6, “Initial Configuration”**—Provides initial switch configuration options and switch access information.

- **Chapter 7, “Configuring High Availability”**—Provides details on the high availability feature including switchover mechanisms.
- **Chapter 8, “Software Images”**—Describes how to upgrade Cisco MDS 9000 Family switches, install software image files, use the Flash file system on the supervisor engine, and recover a corrupted bootflash image.
- **Chapter 9, “Managing Modules”**—Explains how to display and analyze the status of each module and specifies the power on and power off process for modules.
- **Chapter 10, “Managing System Hardware”**—Provides details on switch hardware inventory, power usage, power supply, module temperature, fan and clock modules, and environment information.
- **Chapter 11, “Configuring and Managing VSANs”**—Describes how virtual SANs (VSANs) work, explains the concept of default VSANs, isolated VSANs, VSAN IDs and attributes, and provides details on how to create, delete, and view VSANs.
- **Chapter 12, “Configuring Interfaces”**—Explains port and operational state concepts in Cisco MDS 9000 Family switches and provides details on configuring ports and interfaces.
- **Chapter 13, “Configuring Trunking”**—Explains TE ports and trunking concepts.
- **Chapter 14, “Configuring PortChannels”**—Explains PortChannels and load balancing concepts and provides details on configuring PortChannels, adding ports to PortChannels, and deleting ports from PortChannels.
- **Chapter 15, “Configuring and Managing Zones”**—Defines various zoning concepts and provides details on configuring a zone set and zone management features.
- **Chapter 16, “Configuring Inter-VSAN Routing”**—Describes Inter-VSAN Routing.
- **Chapter 17, “Managing FLOGI, Name Server, FDMI, and RSCN Databases”**—Provides name server and fabric login details required to manage storage devices and display registered state change notification (RSCN) databases.
- **Chapter 18, “Configuring Switch Security”**—Discusses the AAA parameters, user profiles, RADIUS authentication, SSH services, and SNMP Security options provided in all switches in the Cisco MDS 9000 Family and provides configuration information for these options.
- **Chapter 19, “Configuring Fabric Security”**—Describes how to configure and manage fabric security.
- **Chapter 20, “Configuring Port Security”**—Provides details on port security features that can prevent unauthorized access to a switch port in the Cisco MDS 9000 Family.
- **Chapter 21, “Configuring Fibre Channel Routing Services and Protocols”**—Provides details and configuration information on Fibre Channel routing services and protocols.
- **Chapter 22, “Configuring IP Services”**—Provides details on IP over Fibre Channel (IPFC) services and provides configuring IPFC, virtual router, and DNS server configuration information.
- **Chapter 23, “Configuring FICON”**—Provides information on configuring and managing FICON with the Cisco MDS 9000 Family.
- **Chapter 24, “Configuring IP Storage”**—Provides details on extending the reach of Fibre Channel SANs by connecting separated SAN islands together via IP networks using FCIP, and allowing IP hosts to access FC storage using the iSCSI protocol.
- **Chapter 25, “Configuring Call Home”**—Provides details on the Call Home service and includes information on Call Home, event triggers, contact information, destination profiles, and e-mail Options.

- **Chapter 26, “Configuring Domain Parameters”**—Explains the Fibre Channel domain (fcdomain) feature, which includes principal switch selection, domain ID distribution, FC ID allocation, and fabric reconfiguration functions.
- **Chapter 27, “Configuring Traffic Management”**—Provides details on the quality of service (QoS) and Fibre Channel Congestion Control (FCC) features.
- **Chapter 28, “Configuring System Message Logging”**— Describes how to configure system message logging on the Cisco MDS 9000 Family switches.
- **Chapter 29, “Discovering SCSI Targets”**—Describes how the SCSI LUN discovery feature is started and displayed.
- **Chapter 30, “Monitoring Network Traffic Using SPAN”**—Describes the switched port analyzer (SPAN), identifies SPAN sources, specifies filters, explains SPAN Sessions, SD port characteristics, and configuration details.
- **Chapter 31, “Advanced Features and Concepts”**—Describes the advanced configuration features—time out values, fctrace, fabric analyzer, world wide names, flat FC IDs, loop monitoring, and interoperating switches.
- **Chapter 32, “Configuring Fabric Configuration Servers”**—Describes how the fabric Configuration Server (FCS) feature is configured and displayed.
- **Chapter 33, “Monitoring System Processes and Logs”**—Provides information on displaying system processes and status. It also provides information on configuring core and log files, HA policy, heartbeat and watchdog checks, and upgrade resets.
- **Chapter 34, “Troubleshooting the Fabric”**—Provides information on using Fabric Manager to troubleshoot your fabric.
- **Chapter 35, “Troubleshooting Fabric Manager Issues”**—Describes some common issues you may experience while using Cisco Fabric Manager, and provides solutions.

Conventions

This document uses the following conventions:

Item	Convention
Commands, keywords, special terminology, and options that should be selected during procedures	boldface font
Variables for which you supply values and new or important terminology	<i>italic</i> font
Displayed session and system information, paths and file names	<code>screen</code> font
Information you enter	boldface screen font
Variables you enter	<i>italic screen</i> font
Menu items and button names	boldface font
Indicates menu items to select, in the order you select them.	Option > Network Preferences



Tip

Identifies information to help you get the most benefit from your product.



Note

Means *reader take note*. Notes identify important information that you should reflect upon before continuing, contain helpful suggestions, or provide references to materials not contained in the document.



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage, loss of data, or a potential breach in your network security.



Warning

Identifies information that you must heed to prevent damaging yourself, the state of software, or equipment. Warnings identify definite security breaches that will result if the information presented is not followed carefully.

Obtaining Documentation

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

Cisco.com

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

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Documentation DVD

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

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to mdsfeedback-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
- Nonemergencies—psirt@cisco.com



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 that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

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

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

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

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

<http://www.ciscopress.com>

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

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

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

- World-class networking training is available from Cisco. You can view current offerings at this URL:

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

