Cisco Router and Security Device Manager (SDM), Version 2.2 User Guide for the Cisco 7000 Family

September, 2005

Note This *User Guide* covers the Cisco 7204VXR, the Cisco 7206VXR, and the Cisco 7301 routers. For information on additional SDM supported platforms, go to: http://www.cisco.com/go/sdm.

Cisco Router and Security Device Manager (SDM), Version 2.2, is an intuitive Java-based device-management tool that lets you configure LAN interfaces, routing, Network Address Translation (NAT), firewalls, Virtual Private Networks (VPNs), and other features without knowledge of the Cisco command-line interface (CLI).

Note SDM does not support the following features on the Cisco 7000 family: SDM Reset, WAN configuration; therefore, you will need to use CLI commands to support these functions. The SDM Express Wizard is not supported on the Cisco 7000 family.

SDM is preinstalled on your router Flash Disk or CompactFlash Disk when you order a security bundle comprising a Cisco 7204VXR, Cisco 7206VXR, or Cisco 7301 router. http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm.

Because SDM uses a GUI interface, it requires that you access it from a PC using a supported web browser. For the supported browsers, see the "Cisco IOS Software Requirements" section on page 7.

This guide includes the following topics:

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

Overview

You can configure secure network access on your Cisco 7204VXR, Cisco 7206VXR, or Cisco 7301 router using both the SDM management tool and CLI commands.

You launch SDM using a supported browser on a PC. SDM allows you to configure supported security features, such as VPNs and firewalls, on interfaces that must be configured using CLI commands, such as token ring. SDM attempts to read any configurations added through CLI commands, but unsupported features are displayed as read-only or unsupported.

Although multiple users can concurrently use SDM to monitor a router, it is not recommended that multiple users concurrently modify the configuration; results may be inconsistent.

Features

Cisco SDM Version 2.2 New Features

Table 2 lists the key features of SDM, Version 2.2.

Table 1 SDM 2.2 New Features

Feature	Benefits
Collaborative Security Solutions	
Incident Control Services (ICS) • Support Trent Micro signatures	• Rapid deployment and customization of signatures for day-zero protection against new attacks
Network Admission Control (NAC) • Configuration wizard and client security posture management	• Simple and fast integration of NAC into existing network infrastructure

Table 1 SDM 2.2 New Features (continued)

Feature	Benefits
Application Level Security	
Application Firewall • Advanced firewall wizards, policy views, inspection rule editors and log views • P2P applications: BitTorrent, Kazaa, Gnutella, eDonkey • Instant Messaging: Yahoo, MSN, AOL • Protocol Conformance: HTTP & Email (SMTP/POP3/IMAP)	• Application level control and unified threat management for accelerated security policy deployment • Protocol anomaly detection services • High, Medium, Low firewall policy settings for accelerated and easy deployment
Granular Protocol Inspection • Pre-defined Application names • User customizable application to port (or port range) mapping	• More granular application inspection and control over TCP and UDP ports
Threat-based Intrusion Protection • Threat based signature categories to ease IPS deployments • Signature creation wizards, event viewer	• Easier and more intelligent signature selection based on threat types • Real time reporting of IPS events, and status
Easy VPN Server and Remote Enhancements • Advanced wizards, remote config update, web intercept, dial backup and QoS support	• Scalable, easy to manage, secure remote access for teleworkers or small offices on hub routers or branch office access routers
Dynamic DNS • HTTP and IETF based updates • Integration with existing WAN interface configuration wizard	• Scalable, remote management of dynamically addressed routers
Usability Improvements	• Ability to view in real-time SDEE alarms from IPS signature engines • Layer 3 and above Firewall Policy templates • Application Firewall Alarm log • NAT wizards to simplify IP Address management • Search toolbar for SDM UI pages, features and wizards

Cisco SDM Features

Table 2 lists the key features of SDM.

Table 2 SDM Features

Feature	Description
PC-Based SDM • SDM installed on Windows-based PC instead of router Flash	• No extra Flash space required on router for SDM • Great tool to manage the installed base of Cisco routers
Task-Based SDM UI • Newly designed home page, single starting point for key security tasks, better navigation between related tasks	• Faster and easier configuration of security configurations—IPSec VPNs, firewall, ACLs, IPS, etc.
Easy VPN Server and Remote • Wizard-based configuration and real-time monitoring of remote-access VPN users; integration with on-router or remote AAA server	• Scalable, easy to manage, secure remote access for teleworkers or small offices on hub routers or branch office access routers
Intrusion Prevention (IPS) • Dynamic signature update, quick deployment of default signatures, ability to customize signatures, validation of router resources before signature deployment	• Network-based protection against worms, viruses, and OS/protocol exploits • Customizable signatures for day-zero protection against new variants of worms and viruses
Role-Based Access • Factory-default profiles: Admin, read-only, firewall, Easy VPN Remote	• Secure, logical separation of router between NetOps, SecOps, end users • SPs can offer a graphical read-only view of the CPE services to end customers
QoS Policy • Three predefined categories: Real Time, Business Critical, Best Effort	• Easily and effectively optimize WAN/VPN bandwidth and application performance for different business needs (voice/video, enterprise applications, Web, etc.)
NBAR • Application traffic performance monitoring	• Real-time validation of application usage of WAN/VPN bandwidth against predefined service policies

Table 2 SDM Features (continued)

Feature	Description
SSHv2 • Automatically use SSHv2 for all encrypted communication between SDM and router	• Secure management between PC and Cisco router
SSHv2 • Automatically use SSHv2 for all encrypted communication between SDM and router • Security Audit • Automatically use SSHv2 for all encrypted communication between SDM and router	
Digital Certificates	• Highly scalable, more secure solution than preshare keys; easy to use and deploy with the combination of SDM, Cisco IOS CA, and SPD
IPS Provisioning Improvements • 2 new Cisco tuned signature files	• Allows rapid deployment of IPS signatures specific to router model

Comprehensive Cisco IOS Feature Support

Table 3 lists the Cisco IOS features.

Table 3 Cisco IOS Features

Feature	Description
VPN	Easy VPN Server, Easy VPN Remote, IPSec, GRE over IPSec, DMVPN (full mesh or hub-spoke), V3PN, digital certificates, VPN monitor, and troubleshooting
Firewall	Stateful Inspection, application firewall, granular protocol inspection, DMZ, firewall log, policy table
Intrusion Prevention (IPS)	Automatic Signature provisioning, Dynamic signature update and signature customization, event viewer, signature creation wizards, threat based signature categories
Routing	OSPF, EIGRP, RIPv2, Static
Interfaces	10/100/1000 Ethernet
Advanced Configuration	NAT wizards, ACL, VLAN, CLI preview mode, DHCP server, date/time, NTP, DNS, SSHv2, management access policy, Dynamic DNS

System Requirements

Refer to the following sections to determine the requirements for SDM support:

Memory Requirements

SDM Version 2.2 requires at least 7 MB of free Flash Disk or CompactFlash Disk on the router. Note that the Cisco IOS software requires approximately 20 MB of Flash Disk space.

Note Flash Disks and CompactFlash Disks provide from 48 MB to 356 MB of storage space. Flash Disks and CompactFlash Disks are supported on Cisco 7000 products that have PC card slots—formerly called Personal Computer Memory Card International Association (PCMCIA) slots.

Hardware Requirements

SDM requires a PC running a Pentium III processor or faster, with a supported browser, and one of the following supported Cisco 7000 routers (see Table 4):

Table 4 Supported Hardware

Supported Routers	Supported Processors	Supported Service Adapters[1]	Supported Port Adapters
Cisco 7204VXR	NPE-225, NPE-400, NPE-G1, NSE-1	VAM, VAM2, VAM2+	PA-2FE-TX PA-2FE-FX PA-8E PA-4E
Cisco 7206VXR	NPE-225, NPE-400, NPE-G1, NSE-1	VAM, VAM2, VAM2+	
Cisco 7301	—	VAM2, VAM2+	

1. The Integrated Services Adapter (ISA) module is not supported with SDM.

Note SDM requires a PC with a Pentium III or higher processor.

Browser and Java Requirements

Note SDM does not support Windows 2000 Advanced Server.

SDM can be used with the following browsers and Java software:

- Netscape version 7.1 and 7.2 (not supported on Windows 98)
- Internet Explorer version 5.5 and later on all operating systems
- Java plug-in (SUN Java Runtime Environment (JRE) Version 1.4.2_08 or later)

PC Operating System Requirements

SDM can be run on a PC running any of the following operating systems:

- Microsoft Windows XP Professional
- Microsoft Windows 2003 Server (Standard Edition)

Note Microsoft Windows 2000 Advanced Server is not supported.

- Microsoft Windows 2000 Professional (Service Pack 4 or later)
- Microsoft Windows NT 4.0 Workstation (Service Pack 4 or later)
- Microsoft Windows ME
- Microsoft Windows 98 Second Edition

Cisco IOS Software Requirements

Table 5 lists the SDM minimum supported Cisco IOS software for your router.

Table 5 Minimum Supported Cisco IOS Software for Use with SDM

Platform	Minimum Cisco IOS Software
Cisco 7204VXR Cisco 7206VXR Cisco 7301	Cisco IOS Software Release 12.3(2)T or later, or 12.3(3)M or later; no support for B, E, and S trains

Connectivity Requirements

You can connect to SDM via a PC or server using any of the following methods: HTTP and HTTPS; Telnet, SSH, and SSHv2.

Note Cisco SDM has negligible impact on router DRAM or CPU.

Determining if SDM Is Installed

Use one of the following methods to determine if SDM is installed on your router:

- Enter **https://***router_IP_address* in a web browser and see if SDM starts.
- Using the CLI, enter the **dir all-filesystems** or the **show flash** command, and check to see if the SDM file set is present: sdm.tar, ips.tar, home.shtml, home.tar, common.tar.

This completes the procedure for determining if SDM is installed on your router. Go to "Configuring Your Router to Support SDM" section on page 8.

Configuring Your Router to Support SDM

Note Before you download/upgrade SDM, your router Ethernet interfaces must be configured. See the appropriate installation and configuration guide for your router. For Cisco 7200VXR routers, see the *Cisco 7200 VXR Installation and Configuration Guide*, and for the Cisco 7301 router, see the *Cisco 7301 Installation and Configuration Guide* for more information.

Before installing SDM on your router, modify the existing configuration using the CLI to include the following configuration information:

- Enable HTTP/HTTPS server, using the following Cisco IOS software commands:

```
ip http server
ip http secure-server
ip http authentication local
```

- Configure your router to have a user account with level 15 privileges, by typing the **username** command:

```
username cisco privilege 15 password 0 cisco
```

Note By default, privilege level 15 is enabled on the router.

For security purposes, the user account defined should be different from the default one used in the preceding example.

- Enable SSH and Telnet for local login by typing the following commands:

```
line vty 0 15
 privilege level 15
 login local
! The next line only for the image does not support SSH
 transport input telnet
! The next line for the image supports SSH
 transport input telnet ssh
```

- (Optional) Enable local login to support the log monitoring function by typing the following command:

```
logging buffered 51200 warning
```

Note This completes the procedure for configuring your router to support SDM. If SDM is preinstalled on your router, go to the "Launching SDM" section on page 9.

Installing SDM (Optional)

SDM comes preinstalled on the Flash Disk or CompactFlash Disk as part of your Cisco 7204VXR, Cisco 7206VXR, or Cisco 7301 router. You can also download/upgrade SDM free of charge from the Software Center on Cisco.com at: http://www.cisco.com/public/sw-center/index.shtml.

For instructions on installing SDM, see *Downloading and Installing Cisco Router and Security Device Manager* at http://www.cisco.com/en/US/products/sw/secursw/ps5318/tsd_products_support_series_home.html

Launching SDM

To start SDM on your router using a PC browser to access SDM, follow these steps:

Step 1 Access the router CLI using the Telnet connection or the console port.

Step 2 Open a web browser on a PC, and enter the following URL:

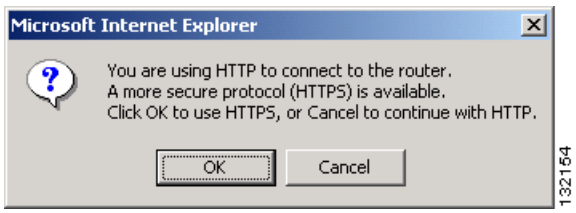
`https://router_interface_IP_address`

where *router_interface_IP_address* is the router IP address.

Note **https://...** specifies that the Secure Sockets Layer (SSL) protocol be used for a secure connection. **http://...** can be used if SSL is not available.

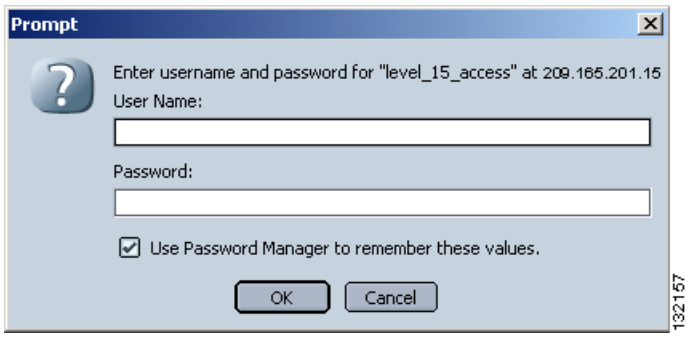
If you do not enter **https://** and you are using Windows IE, you will receive a message, warning you that you are not in secure mode. Click **Yes** to configure in secure mode, or click **Cancel** to continue using http (see Figure 1).

Figure 1 Microsoft Internet Explorer Screen



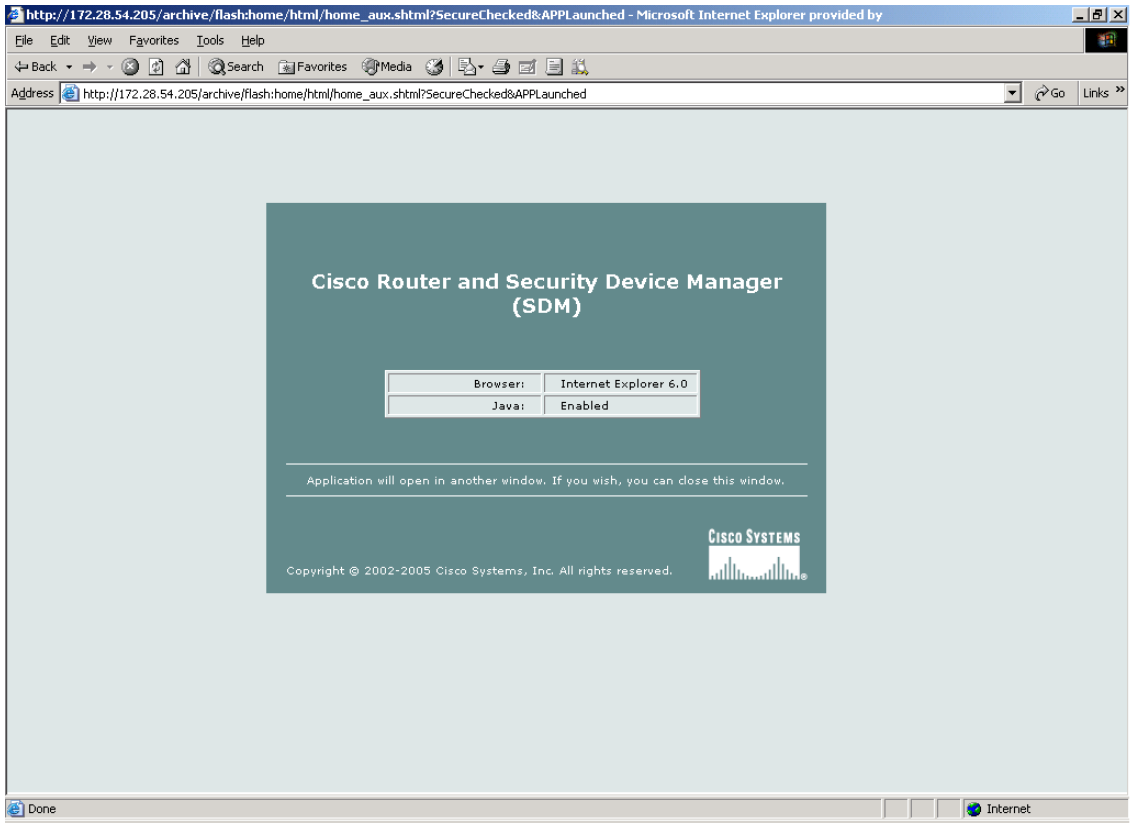
Step 3 At the Netscape **Prompt** screen, enter your user ID and password (see Figure 2), and check the 'Use Password Manager to remember these values' box to remember your user ID and password in the future. Then, click **OK**.

Figure 2 Netscape Prompt Screen



The SDM application screen opens (see Figure 3).

Figure 3 SDM Application Screen



Note You must disable your active popup blocker for SDM to function. An error message will appear if you have not disabled your browser's popup blockers.

Step 4 At the IE **Enter Network Password** window (see Figure 4), enter your user ID and password, then click **OK**. Check the box 'Save this password in your password list' if you want the system to remember your password.

At the Netscape **Password Needed Networking** screen (see Figure 5), enter your user name and password, then click **OK**.

Figure 4 Microsoft Internet Explorer - Enter Network Password Screen

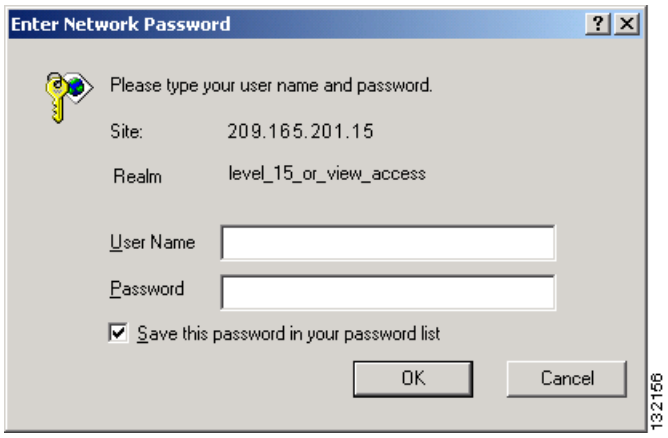
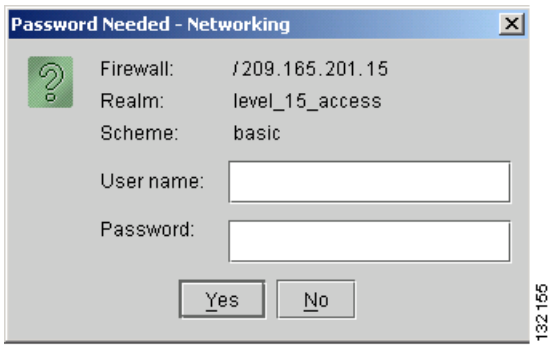


Figure 5 Netscape - Enter Network Password Screen



Step 5 At the Security Alert screen (see Figure 6), click **Yes** to continue.

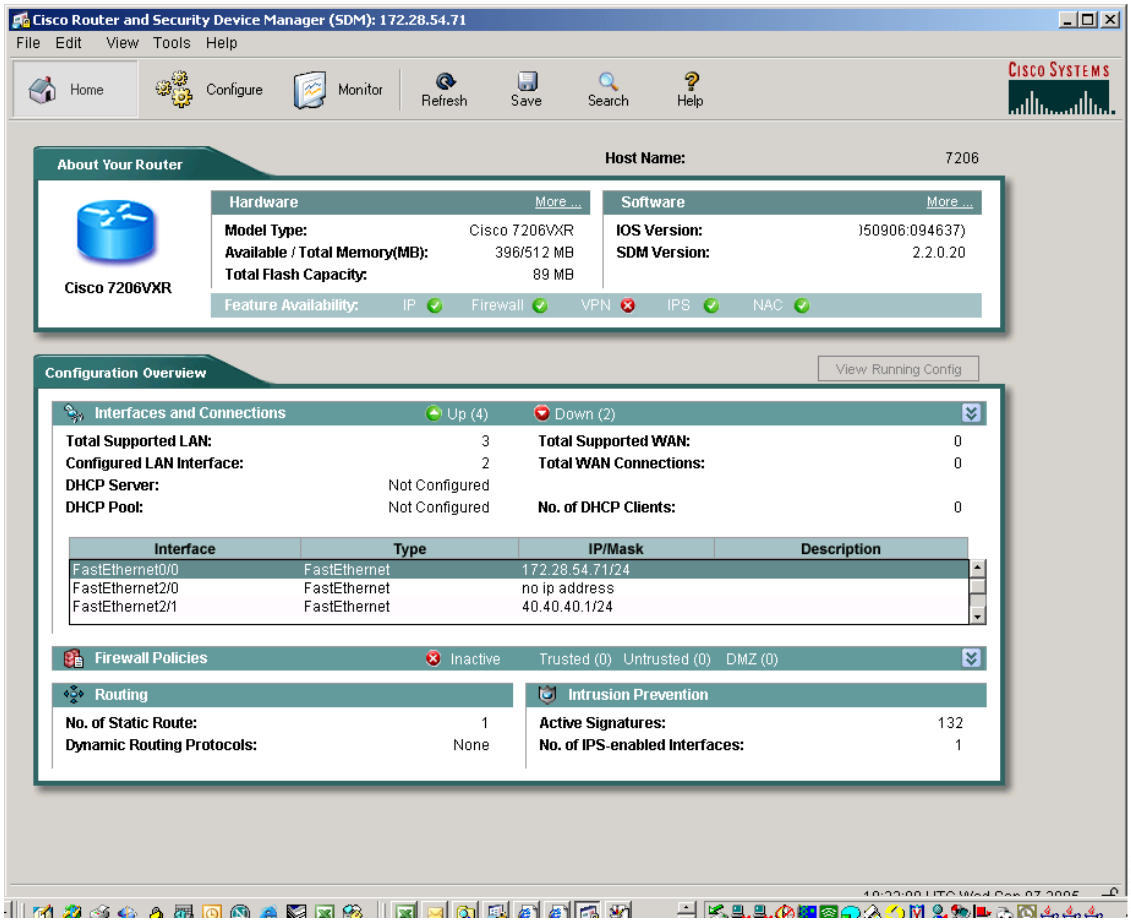
Figure 6 Security Alert Screen

The Cisco Router and Security Device Manager (SDM) Launch screen appears (see Figure 7) in the background. Leave this window open and wait for the next window.

Note Do not close this window (Figure 7) until you log out from SDM, as it will close SDM.

Figure 7 Cisco Router and Security Device Manager (SDM) Launch Screen

Figure 8 Router Home Page



Step 6 Click **Configure** to begin configuring your router for VPN secure access. See *Downloading and Installing Cisco Router and Security Device Manager 2.2* for detailed instructions.

Note The WAN configuration, and Reset to Factory Default wizards are not supported on the Cisco 7000 routers.

This completes the procedure for launching SDM.

Upgrading SDM

If SDM is already configured on your router, you can upgrade SDM using the Tools main menu.

Select from one of the following:

- Tools>Update SDM>Upgrade from Cisco.com
- Tools>Update SDM>From Local PC

For instructions on upgrading SDM, see *Downloading and Installing Cisco Router and Security Device Manager*.

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. You can access iQ Magazine at this URL:

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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *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