Cisco Router and Security Device Manager (SDM) User Guide for the Cisco 7200 VXR and Cisco 7301 Routers

October, 2006

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) 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 7200 VXR or Cisco 7301 routers: 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.

SDM can also be purchased and installed on an existing Cisco 7204VXR, Cisco 7206VXR, or Cisco 7301 router. See "Installing SDM (Optional)" section on page 6 for instructions on downloading and installing 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 4.

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, firewalls, and digital certificates. Interfaces that SDM does not support, such as token ring, must be configured using CLI commands. SDM attempts to read any configurations added through CLI commands, but unsupported features are displayed as read-only in the SDM user interface.

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

For SDM feature information, see the Security Device Manager Release Notes Page at http://www.cisco.com/en/US/products/sw/secursw/ps5318/prod_release_notes_list.html

System Requirements

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

Memory Requirements

SDM Version 2.3.1 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 1):

Table 1 Supported Hardware

Supported Routers	Supported Processors	Supported Service Adapters[1]	Supported Port Adapters
Cisco 7204VXR	NPE-225, NPE-400, NPE-G1, NPE-G2, NSE-1	VAM[2], VAM2[2], VAM2+	PA-2FE-TX PA-2FE-FX PA-8E PA-4E
Cisco 7206VXR	NPE-225, NPE-400, NPE-G1, NPE-G2, NSE-1	VAM[2], VAM2[2], VAM2+	
Cisco 7301	—	VAM2[2], VAM2+	

1. The Integrated Services Adapter (ISA) module is not supported with SDM.
2. The VAM and VAM2 products are no longer being sold.

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

Browser and Java Requirements

For browser and Java requirements, see the Security Device Manager Release Notes at http://www.cisco.com/en/US/products/sw/secursw/ps5318/prod_release_notes_list.html

PC Operating System Requirements

For PC operating system requirements, see the Security Device Manager Release Notes at http://www.cisco.com/en/US/products/sw/secursw/ps5318/prod_release_notes_list.html

Cisco IOS Software Requirements

Table 2 lists the SDM minimum supported Cisco IOS software for your router.

Table 2 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.

Restrictions

The following restrictions apply to SDM running on Cisco 7204VXR, 7206VXR, and 7301 routers:

- The SDM Express application is not supported.
- WAN configuration is not supported. SDM supports configuration of Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces.
- The SDM Reset feature is not available.
- No SDM-default configuration file is supplied.

Determining if SDM Is Installed

Use the following method to determine if SDM is installed on your router:

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,attack-drop.sdf, 128MB.sdf, 256MB.sdf, home.shtml, home.tar, common.tar.

If SDM ins not installed on your router, and you wish to download and install it, go to "Installing SDM (Optional)" section on page 6.

This completes the procedure for determining if SDM is installed on your router. Go to "Configuring Your Router to Support SDM" section on page 5.

Configuring Your Router to Support SDM

You can install and run SDM on a router that is already in use without disrupting network traffic, but you must ensure that a few configuration settings are present in the router configuration file.

Access the CLI using Telnet or the console connection to modify the existing configuration before installing SDM on your router.

Step 1 Enable the HTTP and HTTPS servers on your router by entering the following commands in global configuration mode:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# ip http server

Router(config)# ip http secure-server

Router(config)# ip http authentication local

Router(config)# ip http timeout-policy idle 600 life 86400 requests 10000
```

If the router supports HTTPS, the HTTPS server will be enabled. If not, the HTTP server will be enabled. HTTPS is supported in all images that support the Crypto/IPSec feature set, starting from Cisco IOS release 12.25(T).

Step 2 Create a user account defined with privilege level 15 (enable privileges). Enter the following command in global configuration mode, replacing username and **password** with the strings that you want to use:

```
Router(config)# username username privilege 15 secret 0 password
```

For example, if you chose the username tomato and the password vegetable, you would enter:

```
Router(config)# username tomato privilege 15 secret 0 vegetable
```

You will use this username and password to log in to SDM.

Step 3 Configure SSH and Telnet for local login and privilege level 15. Use the following commands:

```
Router(config)# line vty 0 4

Router(config-line)# privilege level 15

Router(config-line)# login local

Router(config-line)# transport input telnet ssh

Router(config-line)# exit
```

If your router supports 16 vty lines, you can add the following lines to the configuration file:

```
Router(config)# line vty 5 15

Router(config-line)# privilege level 15

Router(config-line)# login local

Router(config-line)# transport input telnet ssh
```

```
Router(config-line)# exit

Router(config)#
```

Step 4 (Optional) Enable local logging to support the log monitoring function. Enter the following command in global configuration mode:

```
Router(config)# logging buffered 51200 warning
```

Step 5 Enter the **end** command to leave configuration mode:

```
Router(config)# end

Router#
```

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/pcgi-bin/tablebuild.pl/sdm.

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

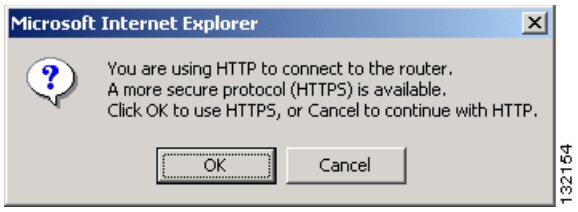
https://*router_interface_IP_address*

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.

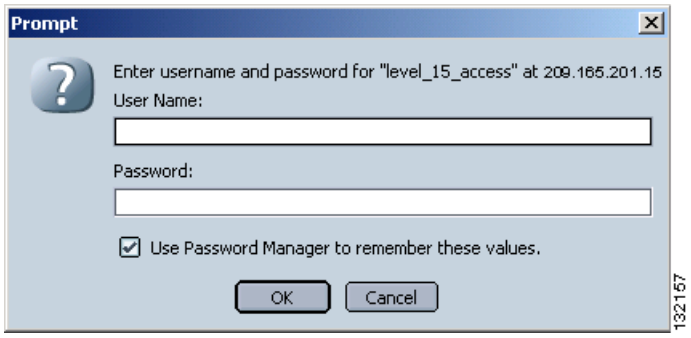
If you do not enter **https://** and you are using Windows IE, you will receive a message, warning you that you are not in secure mode. Click **OK** to configure in secure mode, or click **Cancel** to continue using http (see Figure 1).

Figure 1 Microsoft Internet Explorer Screen



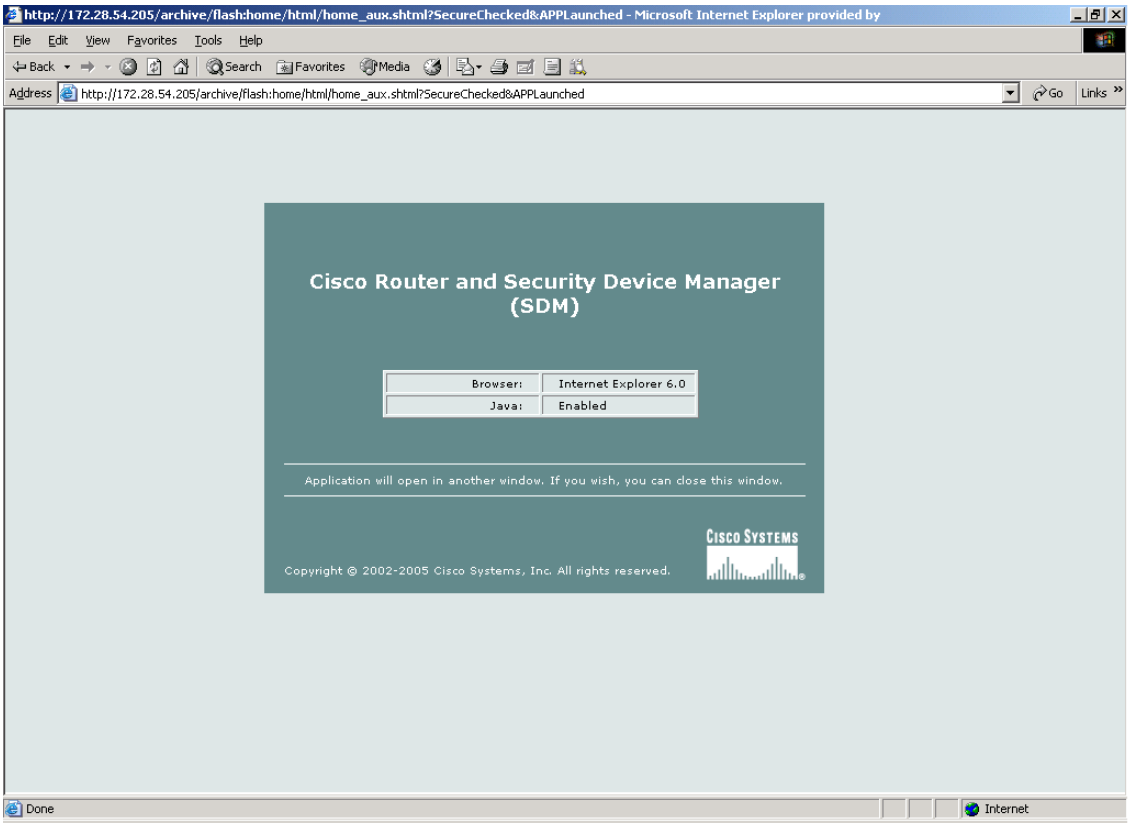
Step 2 At the Netscape **Prompt** screen, enter your user ID and password (see Figure 2), and check the 'Use Password Manager to remember these values' box to remember your user ID and password in the future. Then, click **OK**.

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 3 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

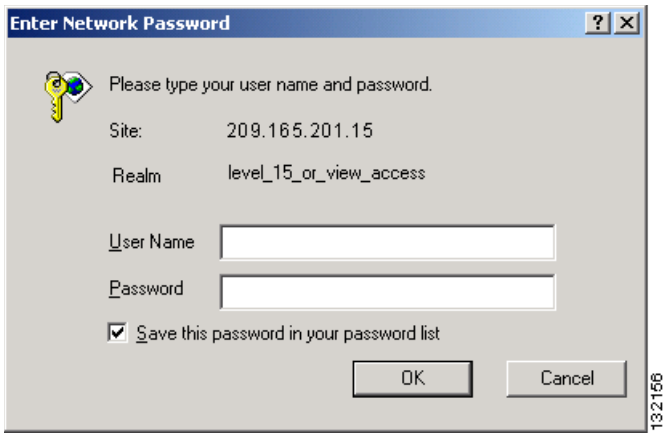
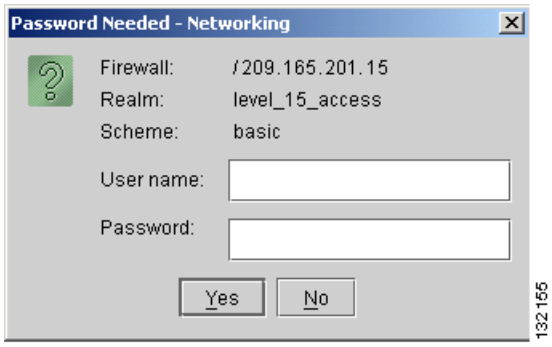


Figure 5 Netscape - Enter Network Password Screen



Step 4 At the Security Alert screen (see Figure 6), click **Yes** to continue.

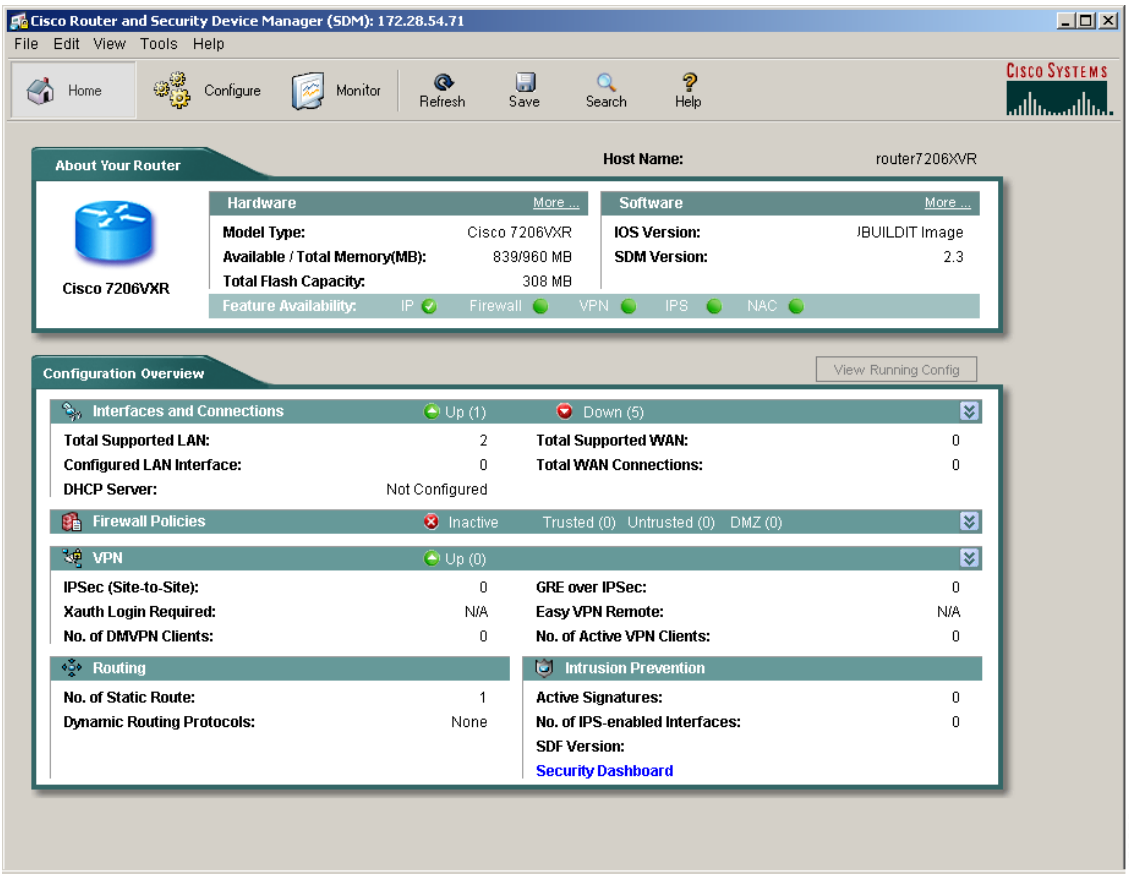
Figure 6 Security Alert Screen

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.

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

Note Figure 7 shows an example of one version of Security Device Manager launch screen. Details may vary depending on the Security Device Manager version you are running.

Figure 8 Router Home Page



Note Figure 8 provides an example of a Router Home Page. Details may vary depending on the Security Device Manager version you are running.

Step 5 Click **Configure** and then click on e of the feature buttons on the left side to begin configuring your router. **(**See *Downloading and Installing Cisco Router and Security Device Manager* for detailed instructions.)

This completes the procedure for launching SDM.

Upgrading SDM

SDM uses an installation wizard to guide you through the process of installing the newer software. To see step-by-step instructions for the installation wizard, refer to “Task 4:Install the SDM Files” in *Downloading and Installing Cisco Router and Security Device Manager*.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

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

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

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

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

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 will find information about how to do the following:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—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.

- For 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 (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key 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.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

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 Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This 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.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

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)—An existing 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 operations 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 the network is impaired while 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.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

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

- 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

- *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 where networking professionals 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

- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- 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