Release Notes for Cisco Router and Security Device Manager Version 2.1.1

May2, 2005

These release notes support Cisco Router and Security Device Manager version 2.1.1. They should be used with the documents listed in the "Related Documentation" section. These release notes are updated as needed.

Contents

This document contains the following sections:

- Introduction, page 1
- System Requirements, page 2
- New and Changed Information, page 9
- Restrictions and Limitations, page 12
- Important Notes, page 12
- Caveats, page 15
- Related Documentation, page 24
- Obtaining Documentation, page 25
- Documentation Feedback, page 26
- Cisco Product Security Overview, page 26
- Obtaining Technical Assistance, page 27
- Obtaining Additional Publications and Information, page 28

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

Copyright © 2003-2004 Cisco Systems, Inc. All rights reserved.

Introduction

Cisco Router and Security Device Manager (SDM) is a web-based configuration tool that allows you to configure LAN and WAN interfaces, routing, Network Address Translation (NAT), firewalls, Intrusion Prevention System (IPS), Virtual Private Networks (VPNs), and other features on the router. SDM version 2.1 and later can be installed on a PC, or in router memory. Earlier versions of SDM can be installed only in router memory. If you have a router listed in the "Hardware Supported" section on page 2, SDM may be preinstalled in router memory, or may be shipped on a CD with the router.

System Requirements

This section contains SDM system requirements.

Memory Requirements

A minimum of 6 MB of free router memory is required to support Cisco SDM files. 2 MB of router memory is required to support Cisco SDM Express files. The Wireless Management application requires an additional 1.7 MB.

Cisco SDM installed on a PC requires 6 MB of memory.

Table 2 on page 9 lists the files that are included with Cisco SDM, Cisco SDM Express, and the Wireless Management application.

Hardware Supported

This section lists the hardware that SDM supports.

Cisco Routers

SDM is supported on the following Cisco SB100 series routers.

- Cisco SB101
- Cisco SB106
- Cisco SB107

SDM is supported on the following Cisco 800 series routers:

- Cisco 831
- Cisco 836
- Cisco 837
- Cisco 851
- Cisco 857
- Cisco 871
- Cisco 876
- Cisco 877

- Cisco 878

SDM is supported on the following Cisco 1700 series routers:

- Cisco 1701
- Cisco 1710
- Cisco 1711
- Cisco 1712
- Cisco 1721
- Cisco 1751
- Cisco 1751-v
- Cisco 1760
- Cisco 1760-v

SDM is supported on the following Cisco 1800 series routers:

- Cisco 1801
- Cisco 1802
- Cisco 1803
- Cisco 1811
- Cisco 1812
- Cisco 1841

SDM is supported on the following Cisco 2600 series routers:

- Cisco 2610XM
- Cisco 2611XM
- Cisco 2620XM
- Cisco 2621XM
- Cisco 2650XM
- Cisco 2651XM
- Cisco 2691

SDM is supported on the following 2800 series routers:

- Cisco 2801
- Cisco 2811
- Cisco 2821
- Cisco 2851

SDM is supported on the following Cisco 3600 series routers:

- Cisco 3620
- Cisco 3640
- Cisco 3640A
- Cisco 3661
- Cisco 3662

SDM is supported on the following Cisco 3700 series routers:

- Cisco 3725
- Cisco 3745

SDM is supported on the following Cisco 3800 series routers:

- Cisco 3825
- Cisco 3845

SDM is supported on the following Cisco 7000 series routers:

- Cisco 7204VXR
- Cisco 7206VXR
- Cisco 7301

Supported Network Modules, WICs, Port Adapters, and Service Adapters

SDM supports configuration on the following network modules:

- NM-1E
- NM-4E
- NM-4T
- NM-2W
- NM-1E2W
- NM-1FE2W
- NM-2E2W
- NM-2FE2W
- NM-2FE2W-V2
- NM-1FE-FX
- NM-1FE-TX
- NM-4A/S (synchronous only)
- NM-8A/S (synchronous only)
- NM-CIDS-K9
- NM-16ESW
- NM-36ESW

SDM supports only Ethernet configuration on the following network modules:

- NM-1E1R2W
- NM-1FE1R2W
- NM-1FE1CE1U
- NM-1FE2CE1B
- NM-1FE1CE1B
- NM-1FE2CE1U
- NM-1FE1CT1

- NM-1FE2CT1
- NM-1FE1CT1-CSU
- NM-1FE2CT1-CSU

SDM supports the following WAN interface cards:

- WIC-1T
- WIC-2T
- WIC-2A/S (Frame Relay, PPP, HDLC, no asynchronous)
- WIC-1DSU-T1
- WIC-1ADSL
- WIC-1ENET
- WIC-1SHDSL
- WIC-1DSU-T1-V2
- WIC-1B-S/T
- WIC-1B-S/T-V3
- WIC-1AM
- WIC-2AM
- WIC-4ESW
- WIC-1SHDSL-V2

SDM supports the following high-speed wan interface cards (HWICs):

- HWIC-4T
- HWIC-4A/S
- HWIC-8A/S-232
- HWIC-4ESW
- HWICD-9ESW
- HWIC-AP-G-X
- HWIC-AP-AG-X

SDM supports the following advanced integration modules (AIMs):

- AIM-VPN/BP
- AIM-VPN/BP II
- AIM-VPN/BPII-PLUS
- AIM-VPN/HP
- AIM-VPN/HP II
- AIM-VPN/HPII-PLUS
- AIM-VPN/EP
- AIM-VPN/EP II
- AIM-VPN/EPII-PLUS

SDM supports the following port adapters on Cisco 7000 routers:

- PA-2FE-TX

- PA-2FE-FX
- PA-8E
- PA-4E

SDM supports the following service adapters on Cisco 7000 routers:

- SA-VAM
- SA-VAM2
- SA-VAM2+

SDM also supports the MOD-1700VPN.

PC System Requirements

SDM is designed to run on a personal computer that has a Pentium III or faster processor.

Software Supported

This section describes SDM software requirements.

Cisco IOS Images

SDM is compatible with the Cisco IOS images listed in Table 1.

Note SDM supports the IOS Intrusion Prevention System (IPS). In order to be able to use SDM to configure IOS-IPS, the router must run an IOS image of Release 12.3(8)T4 or later.

Table 1 SDM-Supported Routers and Cisco IOS Releases

SDM-Supported Routers	SDM-Supported Cisco IOS Releases
Cisco SB101 Cisco SB106 Cisco SB107	• 12.3(8)YG
Cisco 831 Cisco 837	• 12.2(13)ZH or later • 12.3(2)XA or later • 12.3(2)T or later
Cisco 836	• 12.2(13)ZH or later • 12.3(2)XA or later • 12.3(4)T or later
Cisco 851 Cisco 857	• 12.3(8)YI
Cisco 871 Cisco 876 Cisco 877 Cisco 878	• 12.3(8)YI

Table 1 SDM-Supported Routers and Cisco IOS Releases (continued)

SDM-Supported Routers	SDM-Supported Cisco IOS Releases
Cisco 1701	• 12.2(13)ZH or later • 12.3(2)XA or later (SDM does not support Cisco IOS release 12.3(2)XF.) • 12.3(4)T or later
Cisco 1711 Cisco 1712	• 12.2(15)ZL or later • 12.3(2)XA or later (SDM does not support Cisco IOS release 12.3(2)XF.)
Cisco 1710 Cisco 1721 Cisco 1751 Cisco 1751-v Cisco 1760 Cisco 1760-v	• 12.2(13)ZH or later • 12.3(2)XA or later (SDM does not support Cisco IOS release 12.3(2)XF.) • 12.2(13)T3 or later • 12.3(2)T or later • 12.3(1)M or later • 12.2(15)ZJ3 (not available for the Cisco 1710 or Cisco 1721)
Cisco 1801 Cisco 1802 Cisco 1803 Cisco 1811	• 12.3(8)YI
Cisco 1812	• 12.3(8)YH or later
Cisco 1841	• 12.3(8)T4 or later
Cisco 2610XM Cisco 2611XM Cisco 2620XM Cisco 2621XM Cisco 2650XM Cisco 2651XM Cisco 2691	• 12.2(11)T6 or later • 12.3(2)T or later • 12.3(1)M or later • 12.3(4)XD • 12.2(15)ZJ3
Cisco 2801 Cisco 2811 Cisco 2821 Cisco 2851	• 12.3(8)T4 or later
Cisco 3640 Cisco 3661 Cisco 3662	• 12.2(11)T6 or later • 12.3(2)T or later • 12.3(1)M or later • 12.3(4)XD • 12.2(15)ZJ3
Cisco 3620	• 12.2(11)T6 or later • 12.3(1)M or later

Table 1 SDM-Supported Routers and Cisco IOS Releases (continued)

SDM-Supported Routers	SDM-Supported Cisco IOS Releases
Cisco 3640A	• 12.2(13)T3 or later • 12.3(2)T or later • 12.3(1)M or later • 12.3(4)XD • 12.2(15)ZJ3
Cisco 3725 Cisco 3745	• 12.2(11)T6 or later • 12.3(2)T or later • 12.3(1)M or later • 12.3(4)XD • 12.2(15)ZJ3
Cisco 3825 Cisco 3845	• 12.3(11)T or later
Cisco 7204VXR Cisco 7206VXR	• 12.3(2)T or later • 12.3(1)M or later SDM does not support B, E, or S train releases on the Cisco 7000 routers.
Cisco 7301	• 12.3(2)T or later • 12.3(3)M or later SDM does not support B, E, or S train releases on the Cisco 7000 routers.

Determining the Cisco IOS Software Version

To determine the Release of Cisco IOS software currently running on your Cisco router, log in to the router and enter the **show version** EXEC command. The following sample output from the **show version** command indicates the version number on the second output line:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (c1700-k8sv3y7-mz) Version 12.2(13)ZH
```

Web Browser Versions and Java Runtime Environment Versions

SDM can be used with the following browsers:

- Firefox version 1.0.3
- Internet Explorer version 5.5 and later
- Netscape version 7.1 and version 7.2

SDM requires Sun Java Runtime Environment (JRE) version 1.4.2_05 or later, or Java Virtual Machine (JVM) 5.0.0.3810.

PC Operating System Versions

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

- Microsoft Windows XP Professional
- Microsoft Windows 2003 Server (Standard Edition)
- Microsoft Windows 2000 Professional with Service Pack 4
- Microsoft Windows ME
- Microsoft Windows NT 4.0 Workstation with Service Pack 4

Note Windows 2000 Advanced Server is not supported.

Japanese, Simplified Chinese, French, German, Spanish and Italian language support is available on these operating systems:

- Microsoft Windows XP Professional with Service Pack 2 or later
- Microsoft Windows 2000 Professional with Service Pack 4 or later

New and Changed Information

This section contains information that is new or that has changed since the previous release.

New Features Supported in SDM Version 2.1.1

SDM version 2.1.1 supports the following new features:

- New Hardware Support—SDM supports the following new platforms: Cisco SB100 series, Cisco 850 series, Cisco 870 series, Cisco 180x routers, and Cisco 181x routers.
- Integrated Wireless Management—SDM Express lets you create a basic configuration for your wireless network. The web-based Wireless Management application allows you to customize the configuration and make security settings based on your site requirements.
- IPS Provisioning Improvement—IPS supports the new files 128MB.sdf and 256MB.sdf, enabling you to deploy signatures based on router capabilities.
- Support for two new HWICs—HWIC-AP-G-X and HWIC-AP-AG-X.

SDM File List

SDM version 2.1.1 uses the files listed in Table 2.

Table 2 SDM File List

File Name	Size	Description
sdm.tar	3 MB	SDM application file.
ips.tar	1.21 MB	Intrusion Prevention System (IPS) application file.
es.tar	762 KB	SDM Express application file.

Table 2 SDM File List

File Name	Size	Description
sdm.tar	3 MB	SDM application file.
wlanui.tar	1.8 MB	Wireless Application
home.tar	114 KB	SDM and SDM Express support file.
common.tar	821 KB	SDM and SDM Express support file.
home.shtml	2 KB	SDM and SDM Express support file.
attack-drop.sdf	91 KB	Signature Definition File (SDF) used by IPS.
128MB.sdf	493 KB	Signature Definition File (SDF) used by IPS.
256MB.sdf	732 KB	Signature Definition File (SDF) used by IPS.
sdmconfig-*modelnum*.cfg For example: sdmconfig-180x.cfg	2 KB	Default configuration file.

Installation Notes

This section contains important information regarding installation and upgrades to SDM.

Cisco 1700 Routers Running ITS/CCME and Cisco IOS Release 12.2(13)T

If you are installing SDM on a router that already has the Internet Telephony Service (ITS) or Cisco Call Manager Express (CCME) application installed in flash memory, you may exceed the number of files allowed in flash memory by installing SDM. Cisco 1700 routers using a Cisco IOS Release 12.2(13)T image cannot have more than 32 files in flash memory.

Before installing SDM, you must delete any unneeded files from flash memory. If no files can be deleted, do not install SDM on the router.

Downloading SDM from Cisco.com and Installing It on the Router

If SDM is not currently installed on the router, the document *Downloading and Installing Cisco Router and Security Device Manager (SDM)* explains how to download SDM from Cisco.com and install it on the router. To obtain this document, go to the following URL:

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

Upgrading to a New SDM Release

If a version of SDM later than version 1.0 is already installed on the router, you should use the SDM automatic update feature to install the latest files on the router. SDM automatically checks Cisco.com for more recent versions of SDM, downloads them to your PC, removes the old SDM files from memory, runs the **squeeze flash**: command if necessary, and copies the latest files to the router. The update feature is available from the Tools menu. Choose **Tools** > **Update SDM** > **Update from CCO**.

If you are currently using SDM version 1.0, you must download the file SDM-V*nn*.zip at the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/sdm

The document *Downloading and Installing Cisco Router and Security Device Manager (SDM)* explains how to install SDM and all related files on the router. This document is available at the following URL:

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

Uninstalling SDM Files

If you want to remove SDM from flash memory or from a router disk file system, you can do so by logging onto the router and completing the following steps in EXEC mode:

Step 1 Change to the directory in which the SDM files are located.

If the router has a flash file system, use the following command:

```
router# cd flash:
```

If the router has a disk file system, use the following command:

```
router# cd diskN
```

Replace *N* with the actual number of the disk. Use the **slot** keyword instead of the **disk** keyword if necessary.

Step 2 Use the **delete** command to remove the SDM files. The example below deletes the file sdm.tar:

```
router# delete sdm.tar
Delete filename [sdm.tar]?
Delete flash:sdm.tar? [confirm]
```

Press **Return** to confirm the deletion.

Step 3 Use the **delete** command to remove the remaining SDM files. The "SDM File List" section on page 9 lists the files used by SDM.

Step 4 Reclaim memory space by using the **squeeze flash:** command:

```
router# squeeze flash:
```

It is not necessary to use the **squeeze flash:** command on DOS-based file systems.

SDM version 2.1 or later can be installed on your PC. To remove SDM from your PC, complete the following steps:

Step 1 Click **Start** > **Program**n> **Cisco Systems** > **Cisco SDM** > **Uninstall** to launch the Uninstall program.

Step 2 When the message "Do you want to remove the selected applications and all of its features?" appears, click **Yes**.

Step 3 When the Uninstallation Complete screen is displayed, click **Finish**.

Restrictions and Limitations

This section describes restrictions and limitations that may apply to SDM.

SDM Minimum Screen Resolution

SDM requires a screen resolution of at least 1024 x 768.

Restrictions for Cisco 7204VXR, 7206VXR, and 7301 Routers

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 and Fast Ethernet interfaces.
- The SDM Reset feature is not available.
- No SDM-default configuration file is supplied.

Important Notes

This section contains important information for SDM.

Popup Blockers Disable SDM IPS and SDM Online Help

If you have enabled popup blockers in the browser you use to run SDM or SDM IPS, SDM IPS will not launch, and SDM online help will not appear when you click the help button. To prevent this from happening, you must disable the popup blocker when you run SDM or SDMIPS. Popup blockers may be enabled in search engine toolbars, or may be standalone applications integrated with the web browser.

Microsoft Windows XP with Service Pack 2 blocks popups by default. In order to turn off popup blocking in Internet Explorer, go to **Tools** > **Pop-up Blocker** > **Turn Off Pop-up Blocker**.

If you have not installed and enabled pop up blockers, go to **Tools** >**Internet Options** > **Privacy**, and uncheck the **Block popups** checkbox.

Disable Proxy Settings

SDM will not start when run under Internet Explorer using JRE plug-in versions 1.4.2_05 and proxy settings are enabled. To correct this problem, choose Internet Options from the Tools menu, click the **Connections** tab, and then click the LAN settings button. In the LAN Settings window, disable the proxy settings.

Routers Shipped with SDM Do Not Execute the Standard Cisco IOS Startup Sequence

Because a default configuration file is provided on a router shipped with SDM, the router will not execute the standard Cisco IOS startup sequence. If you are expecting to use the Cisco IOS setup utility, a TFTP/BOOTP configuration download, or other features available through the standard Cisco IOS startup, you will need to erase the configuration file.

To erase the existing configuration and take advantage of the Cisco IOS startup sequence, perform the following steps. This will leave SDM on the router if you later decide you want to use it, but you will need to configure the router manually before you can begin using SDM. Please refer to the router quick start guide and to the SDM FAQ (available at http://www.cisco.com/go/sdm) for information about the minimum configuration required for using SDM.

Step 1 Connect the light blue console cable, included with the router, from the blue console port on the router to a serial port on your PC. See the router hardware installation guide for instructions.

Step 2 Connect the power supply to the router, plug the power supply into a power outlet, and turn on the router. See the router quick start guide for instructions.

Step 3 Use a terminal emulation program on your PC, with the terminal emulation settings 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control, to connect to the router.

Step 4 At the prompt, enter the **enable** command, and enter the password **cisco**.

```
yourname> enable

Password: cisco
yourname#
```

Step 5 Enter the **erase startup-config** command.

```
yourname# erase startup-config
```

Step 6 Confirm the command by pressing **Enter**.

Step 7 Enter the **reload** command.

```
yourname# reload
```

Step 8 Confirm the command by pressing **Enter**.

After the router completes the reload operation, it enters into the standard Cisco IOS startup sequence. You can use the startup sequence to give the router a configuration manually, or to copy a configuration file from the network. If you later decide you want to use SDM to change an existing configuration, refer to the instructions on starting SDM included in the quick start guide for the router.

Unable to Perform “squeeze flash:” Operation

If the router is using a Cisco IOS image earlier than release 12.3T, or release 12.2(13)ZH, it may be necessary to use the **squeeze flash:** command to reclaim flash memory after repeated use of SDM. If this becomes necessary, SDM will inform you that the **squeeze flash:** command must be used, and will execute the command upon your confirmation.

However, the **squeeze flash:** command will not work if an **erase flash:** command has never been executed on the router. If this is the case you will receive an "Unable to perform 'squeeze flash'" warning message, and you will need to run the **erase flash:** command to enable the use of the **squeeze flash:** command.

Executing the **erase flash:** command removes SDM and the Cisco IOS image from the router flash memory, and you will lose your connection to the router. Complete the following steps to save files in flash memory, execute **erase flash:**, and copy the files back so you can reconnect to SDM.

Step 1 Ensure that the router will not lose power. If the router loses power after an **erase flash:** operation, there will be no Cisco IOS image in memory.

Step 2 Prepare a TFTP server to which you can save files and copy them over to the router. You must have write access to the TFTP server. Your PC can be used for this purpose if it has a TFTP server program.

Step 3 Open up a Telnet session on the router so that you can use the CLI.

Step 4 Save the router's running configuration to the startup configuration by entering the command **copy running-config startup-config**.

Step 5 Use the **copy tftp** command to copy the Cisco IOS image, and the SDM files from flash memory to a TFTP server:

copy flash: *filename* **tftp:**//*tftp-server-address*/*filename*

For example:

```
Router# copy flash: sdm.tar tftp://10.10.10.3/sdm.tar
```

Table 2 on page 9 lists the files SDM uses.

Tip If you prefer to download a Cisco IOS image, and the SDM-V*nn*.zip file, follow these instructions to use an Internet connection to download an SDM-supported Cisco IOS image, and the SDM-V*nn*.zip file.

a. Click the following link to obtain a Cisco IOS image from the Cisco Software Center:

   http://www.cisco.com/kobayashi/sw-center

b. Obtain an image that supports the features you want on the Cisco 12.2(11)T release or later. Save the file to the TFTP server that is accessible from the router.

c. Use the following link to obtain the latest SDM-V*nn*.zip file.

   http://www.cisco.com/cgi-bin/tablebuild.pl/sdm

d. Extract the SDM files from SDM-V*nn*.zip.

e. Click the **setup.exe** file to start the SDM installation wizard.

Step 6 From the PC, log in to the router using Telnet, and enter Enable mode.

```
Router> enable
Password:
Router#
```

Step 7 Enter the command **erase flash:**, and confirm. The router's IOS image, configuration file, and the SDM files are removed from flash memory.

Step 8 Use the **copy tftp** command to copy the IOS image and the SDM files from the TFTP server to the router:

copy tftp://*tftp-server-address*/*filename* **flash:**

Example:

```
Router# copy tftp://10.10.10.3/SDM.tar flash:
```

Note Copy the Cisco IOS image first, followed by the SDM files.

Step 9 Start your web browser, and reconnect to SDM, using the same IP address you used when you started the SDM session.

Now that an **erase flash:** operation has been performed on the router, you will be able to execute the **squeeze flash:** command when necessary.

Security Alert Dialog May Remain After SDM Launches

When SDM is launched using HTTPS, a security alert dialog box that informs you of possible security problems and asks you if you want to proceed with program launch may appear. This can happen if the router does not have the following global configuration command in the running configuration:

```
ip http timeout-policy idle 600 life 86400 requests 10000
```

Caveats

Caveats describe unexpected behavior in SDM. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels.

Open Caveats—Release 2.1.1

This section lists caveats that are open in release 2.1.1.

- CSCsa40535

  VPN status in the Monitor windows do not show IPSec security association (SA) parameters for DMVPN whenCLI status commands report that the crypto tunnels are up and traffic is passing through. The DMVPN tunnel is shown as established in the IKE SA tab.

  Workaround: Use the CLI to view DMVPN status.

- CSCef50601

  This problem is encountered on routers running Cisco IOS image c3825-advsecurityk9-mz.123-10.2. If an ATM interface is configured on routers running this image, WAN troubleshooting may display inconsistent results. PVC connections may be shown as UP when they are DOWN.

  Workaround: None.

- CSCef29588

  When both SDM and IPS are open, an open dialog box requiring an OK or Cancel in one application will prevent the user from working in the other application.

Workaround: Complete the work in the dialog box and click OK, or click Cancel to close the dialog box before switching to the other application.

- CSCef34056

  If multiple instances of SDM are run under Netscape version 7.1 using the Java Virtual Machine (JVM) or the Java plug-in, and the user shuts down one instance of SDM, then all other open instances of SDM on that PC are shut down.

  This problem occurs because Netscape version 7.1 uses only one instance of the JVM or the Java plug-in, even when multiple instances of Netscape are launched. As a result, when one instance of SDM is shut down, Netscape shuts down the JVM or the Java plug-in, and all other instances of SDM are also shut down.

  Workaround: If SDM is run under Netscape version 7.1, open only one instance of SDM . Using Internet Explorer is advised when multiple instances of SDM must be opened, such as when the user must configure multiple routers at the same time.

- CSCef43267

  When the **crypto identity ca** command is used, the Loopback0 interface is shown as having no configured IP address in the Edit Interfaces and Connections window when an IP address has been configured.

  Workaround: Disregard the IP address information in the Interfaces and Connections window. If you need to view the IP address, choose the interface and click the Edit button.

- CSCef43429

  This problem is caused by the Cisco IOS caveat CSCef46305. After an Easy VPN Remote connection has been brought up after a successful user authentication (Xauth), the remote peer may not be listed in the Easy VPN Remote Edit screen if SDM is refreshed or reinvoked. If this problem occurs, Easy VPN Remote troubleshooting might not behave as expected for this connection.

  This problem will occur only when the Easy VPN server sends Xauth challenges to the Easy VPN remote at the same time that the Easy VPN remote is trying to establish a tunnel with the VPN server.

  Workaround: None.

- CSCef50389

  When an Easy VPN Server is configured using Digital Certificates for authentication, and an Easy VPN Remote connection is configured on another router, the client statistics for the Easy VPN server are all shown as 0 in the VPN Status window.

  Workaround: To view client statistics, choose **Tools** > **Telnet**. Log in to the router, and issue the **show crypto session** command.

- CSCef57546

  When adding a new signature to the ATOMIC.ICMP engine, you may see the error message "[Enum(xxx)-StorageKey-ATOMIC.ICMP] the value AaBb is not a valid value."

  Workaround: In the Add Signature window, go to the parameter StorageKey, and click the green square to enable editing for this parameter. the green square icon will change to a red diamond icon. Choosing any value from the drop down box will fix this problem.

- CSCef63016

  This problem is caused by the Cisco IOS caveat CSCef64124. When the user unchecks the Save Xauth username and password on the router check box in the Edit Easy VPN Remote dialog box and clicks OK, the command is delivered to the router, but SDM shows the check box as checked, and the corresponding command is still shown in the running configuration if SDM is refreshed.

This occurs when the user wants to remove the saved Xauth username and password in Easy VPN Remote.

- CSCef63313

  If an Easy VPN Remote configuration has connections to more than one Easy VPN server configured, VPN troubleshooting decaveatging may report troubleshooting results for only one VPN server or give incorrect recommendations. This issue is seen only in some Cisco IOS images.

  Workaround: None.

- CSCef72022

  Invoking SDM with a user associated with SDM_Monitor view adds a PKI trust point and an Easy VPN profile. This behavior does not affect the running configuration.

  Workaround: Invoke SDM with a user associated with a different CLI view, or with a user of privilege level 15.

- CSCef53222

  SDM filenames are case sensitive. If the SDM files are copied from the PC hard disk to a flash card, File Explorer changes the names to uppercase. When this happens, SDM cannot be invoked from this flash card.

  Workaround: Before removing the flash card from the PC, restore the filenames to lowercase.

- CSCef77689

  When the router is running a Cisco IOS image that does not support the **show pppoe session** command, WAN troubleshooting may not report any reasons for failure or recommended actions for PPPoE connections that are found to be down.

  Workaround: None.

- CSCin54600

  If a firewall is configured for an interface which already has a Management Access policy associated with it, choosing **Replace** in the Merge/Replace dialog box might prevent access to certain networks.

  This occurs because choosing **Replace** causes the policy access control entries (ACEs) to be disassociated from the interface but not from the vty or HTTP line.

  Workaround: When running Firewall wizard on an interface configured with Management Access policy, choose **Merge** option instead of **Replace** and proceed.

- CSCef73879

  VPN troubleshooting may report a possible Maximum Transmission Unit (MTU) problem in the passthrough network when the tunnel is up. If the VPN interface is a dialer interface configured on an asynchronous interface, this problem may not always exist, and the displayed recommended action will have no effect.

  Workaround: Ignore this message and the corresponding recommendation.

- CSCef73395

  Due to a problem with Cisco IOS, if a custom protocol is mapped to a port and the same custom protocol is specified for matching under a classmap, and then the mapping of the custom protocol is deleted from the configuration , Cisco IOS does not give any warning message that the user should first delete the **match protocol custom-01** commands that make use of the custom protocol mapping.

Workaround: Do the following:

- Configure the custom protocol again.
- Remove all the match protocol statements that reference the custom protocol that you configured.
- Remove the custom protocol from the configuration.

- CSCef52940

  This problem is caused by Cisco IOS caveat CSCef52919. A user with privilege level 1 who is associated with a view may be able to log in to SDM with a privilege level of 15. This occurs when authentication authorization and accounting (AAA) is enabled, and a vty line is configured with privilege level 2 through 15.

  Workaround: Do not configure privilege 1-level users. The problem does not occur when users of higher privilege levels are configured.

- CSCec31789

  When you update SDM, if any of the uploaded SDM files shows a size of zero bytes when **show flash** is invoked, no operations such as copy or delete can be performed on flash memory. This problem rarely occurs.

  Workaround: Restart the router to be able to perform operations on flash memory. If files of zero bytes are shown in a **show flash** display, restart the router before starting SDM.

- CSCea90231

  Router does not reload with default configuration when a' user executes a Reset To Factory Defaults operation in SDM.

  If the router is running Cisco IOS Release 12.2(11)T6, and the last 4 bits of the config-register value are set to 0, for example 0x2100 or 0x1100, the router does not reload when the user performs a Reset To Factory Defaults. SDM indicates that it has sent a **reload** command to the router and shuts down, and the default configuration is copied to the startup-config, but the **reload** command has not executed, and the router is still using the running configuration that was present before the Reset To Factory Defaults operation.

  Workaround: Use the CLI config-register command to ensure that the last 4 bits of the config register are not set to 0 (zero).

- CSCea89054

  If you delete a WAN connection that you created, an **ip nat inside** command may still remain in a LAN interface configuration.

  Workaround: To delete the ip nat inside command from the LAN interface configuration, go t o Edit Interfaces and Connections, choose the LAN interface, click Edit, and delete the association in the Association tab.

- CSCin44264

  Enabling AES encryption or IP compression in the Add/Edit IKE Policy or Add/Edit Transform Set windows might not work even though the Cisco IOS image running on the router supports AES encryption or IP Compression. This may happen in the following circumstances:

  - Hardware encryption is enabled.
  - The router has a VPN module that does not support AES encryption or IP compression.

Workaround: Do one of the following:

- Disable hardware encryption by adding the **no crypto engine accelerator** command to the configuration file using the CLI interface. This command tells the router to use Cisco IOS software for encryption instead of using the encryption provided by the VPN module.
- Upgrade your hardware VPN module to one that supports AES or IP compression.

  For more info on VPN Modules, refer to the document at the following URL:

http://www.cisco.com/en/US/products/hw/routers/ps259/products_data_sheet09186a0080088750.html

- CSCeb01244

  When configuring static routing, if a virtual-template interface is configured as the next hop interface in a static route, SDM generates corresponding CLI commands. Delivering such commands to the router may fail on some platforms.

  Workaround: Do not configure a virtual-template interface as a next hop interface if it is not supported on the router.

- CSCdy80223

  When SDM runs with a Cisco IOS image of a release earlier than 12.3T, or earlier than Release 12.2(13)ZH, the HTTP server appends unnecessary characters to names of files it displays. As a result, when SDM is started, the web browser displays the warning "Content does not match the signature."

  Workaround: Disregard the warning and click **Yes** to continue.

- CSCin44119

  When an Easy VPN tunnel is active, using SDM to apply a NAT configuration to the Easy VPN inside and outside interfaces will deliver **ip nat inside** and **ip nat outside** commands to the router, but the running configuration will not be changed. SDM displays no error message when this is attempted.

  Workaround: To apply a NAT configuration to interfaces that have been designated as Easy VPN inside or outside interfaces, complete the following steps in SDM:

  - Choose the Easy VPN tunnel in the VPN Connections window and click Disconnect. If the Connect/Disconnect button is disabled, choose the interface in the Interfaces and Connections window, open the Association tab for that connection and change the Easy VPN association to **None**.
  - Open the NAT window, click Designate **NAT Interfaces**, and designate NAT inside and NAT outside interfaces.
  - Select the Easy VPN tunnel, and click **Connect**. If you had to disassociate the Easy VPN tunnel from the connection, return to the Association tab, and choose the Easy VPN connection name again.

- CSCec83817

  SDM will not start on a Cisco 831 router with 32 MB of memory if run from Netscape. An exception will be displayed in the Java console window, and in the router console window indicating a memory allocation failure.

  Workaround: Run SDM using Internet Explorer version 5.5 or later. Or, if you want to continue to use Netscape, log in to the router CLI and enter the following memory-size command in global configuration mode:

  ```
  Router# memory-size iomem 10
  ```

- CSCin61634

  XAuth authentication intermittently fails, and Easy VPN tunnels cannot be established using SDM on routers running Cisco IOS Release 12.3(4)T. When the user attempts to do an Xauth authentication in SDM, the following error message is displayed:

  ```
  Unable to establish a session with the router to process XAUTH request from the Easy VPN server. Easy VPN tunnel cannot be successfully brought up.
  ```

  This message is followed by another indicating that the **connect** command was delivered to the router, but that the tunnel was not established.

  Workaround: In the VPN Connections window, choose the Easy VPN tunnel configuration and click the **Reset Tunnel** button to clear the tunnel and reconnect it. If this does not bring up the tunnel, use the **Login** button, more than once if necessary, to bring up the tunnel.

- CSCed06737

  When SDM Express runs with Cisco IOS image of Release 12.2(15)T, it fails to download the configuration file from the CNS server through the SDM Express wizard. See CSCin65539 for more details. This issue occurs only with Cisco IOS Release 12.2(15)T.

  Workaround: Upgrade to Cisco IOS Release 12.3(4)T or later.

- CSCec87975

  On Cisco 7x00 routers, the SDM Update feature is supported if the current SDM files were loaded onto the router flash disk or CompactFlash disk. However, the SDM Updates feature fails to upload new SDM files to the router if the current SDM files were installed in flash memory. The SDM Updates feature uses RCP protocol to upload the new SDM files to the router, but the RCP Server misinterprets the “flag” sent by the RCP Client for the above mentioned file systems.

  Workaround: If the current SDM files were loaded into flash memory, update to the new SDM version by manually copying the new SDM files to the file system of the router using a TFTP server. To make use of the automatic SDM Update feature, always install SDM files on the flash disk or CompactFlash disks (disk0, disk1, disk2).

- CSCed31085

  SDM should not get invoked from boot images such as kboot images on 72xx routers. Such boot images are a subset of the Cisco IOS software and do not support all router functions.

  Workaround: Boot the router with an SDM-supported Cisco IOS image, and then invoke SDM. See Table 1 on page 6 for the Cisco IOS releases that SDM supports.

- CSCed26049

  On 72xx platforms, encryption is not supported on PA-4T port adapters. Because the CLI does not support crypto maps for these types of interfaces, SDM will fail to assign crypto maps to these interfaces. The PA-4T port adapter will not support future compression and encryption features.

  Workaround: Upgrade your 72xx router hardware to the 4t+ PA port adapter.

- CSCed30721

  Whenever any unconfigured interface contains the description FW_INSIDE, on a router configured with a firewall, adding a new NTP server will not modify the firewall ACLs to allow NTP passthrough traffic. Instead, when the user edits the firewall’s outside interface in the Interfaces and Connections window, SDM prompts the user to add the NTP passthrough traffic.

  Workaround: Use the CLI to manually remove the description FW_INSIDE from the unconfigured interface.

- CSCin63613

  If the interface used for the primary backup connection is configured for PPPoE encapsulation, the backup connection will not function properly if the next hop address is specified during configuration. A Cisco IOS caveat (CSCin64336) has been filed for this problem. If the interface used for the primary backup connection is an Ethernet interface configured without encapsulation, the backup connection will not function properly if the next hop address is not specified during configuration.

  Workaround: Do one of the following:

  – For PPPoE connections: *Do not* provide the next hop IP address when you configure the primary backup connection.

  – For Ethernet connections without encapsulation: *Do* provide the next hop IP address when you configure the primary backup connection.

- CSCin63415

  If the WAN wizard is used to configure an analog modem connection as a primary backup connection, and the analog modem connection is deleted, SDM may report that the interface contains unsupported configuration parameters.

  Workaround: Click Refresh on the SDM toolbar, and delete the connection.

- CSCed18560

  The Interfaces and Connections window may display the Backup option in disabled state for asynchronous interfaces on Cisco 831 and Cisco 837 routers. This will occur when the following operations have been performed:

  – The interface used for the primary backup connection is configured with an SDM-supported IP address type.

  – The asynchronous interface is configured as the backup for a primary interface.

  – The IP address of the primary interface is changed.

  When the IP address of the primary interface is changed, SDM displays a Yes or No warning popup asking if you want to remove the backup configuration. If you choose **Yes**, SDM removes the backup configuration, but the Interfaces and Connections window still shows the backup option as disabled, preventing you from choosing the asynchronous interface as a backup interface.

  Workaround: Delete the asynchronous interface configuration using the Interfaces and Connections window.

- CSCin48956

  When the router is configured to use PPPoE, users may not be able to download a file using FTP or display web pages from Internet hosts that they are able to ping or access using telnet. This can happen if SDM is being used on a router with interfaces that SDM does not support, such as Token Ring or VLAN interfaces. SDM does not deliver the command **ip tcp adjust-mss 1452** to unsupported interfaces.

  Workaround: Use the CLI to add the **ip tcp adjust-mss 1452** command to the VLAN or Token Ring interface configuration. Use Telnet to access the router and enter the following command in VLAN or Token Ring interface configuration mode:

  ```
  Router# ip tcp adjust-mss 1452
  ```

- CSCed00381

  The SDM Express wizard may not deliver the configuration to a Cisco 2691 router running Cisco IOS images of Release 12.2(15)T or 12.2(15)ZJ when SSH is used to communicate between SDM Express and the router. When SDM Express is invoked using the string https://*router-IP-address*, it uses SSH.

  Workaround: When launching SDM Express, click Cancel in the SSH credentials window. SDM Express will use the Telnet protocol to communicate with the router. Enter the login ID and password in the Telnet credentials window.

- CSCed25696

  When launching the Dynamic Multipoint Virtual Private Network (DMVPN) Hub and Spoke wizard, SDM may take up to 12 seconds to display the first wizard window. This latency may occur if a JRE plug-in of any version is running in the browser, or if SDM is using the SSH or Telnet communications module.

- CSCed08825

  SDM may take several seconds to display screens in the DMVPN wizard. This latency may occur if a Java plug-in is running in the browser.

- CSCed34587

  Using anIP unnumbered interface as a DMVPN tunnel source may cause Cisco IOS to crash. An interface configured as IP unnumbered uses the IP address of another interface on the router. This Cisco IOS problem does not always occur.

  Workaround: Instead of using an IP unnumbered interface as the DMVPN tunnel source, use the interface that is referenced in the **ip unnumbered** command. If you are configuring a hub, the interface must have a static IP address.

- CSCed91235

  The router reloads when an NHRP tunnel interface is removed. This is a Cisco IOS caveat which you may encounter when deleting a DMVPN tunnel. This caveat duplicates CSCed41641.

  Workaround: There is no workaround for this problem.

- CSCin68829

  If an Analog Modem or ISDN connection is deleted using SDM, the dialer interface may not be deleted from the configuration and the router may reload. This is due to a Cisco IOS caveat, CSCin69090. This occurs on routers using Cisco IOS images of Release 12.3(4)XG or later, or Cisco IOS Release 12.3(7)T.

  Workaround: There is no workaround for this problem.

- CSCed92739

  On routers running Cisco IOS Release 12.3(6), Cisco IOS may reload if SDM is started using HTTPS.

  Workaround: Start SDM by entering http://*ip-address.* Do not use http**s:**//*ip-address.*

- CSCee67639

  The SDM Express wizard may fail if the router is running Cisco IOS Release 12.3(9) and there is not sufficient space in NVRAM to save the startup configuration. This problem should not occur with new routers.

  Workaround: If this problem occurs, use the CLI to remove unneeded files from NVRAM.

- CSCed13205

  SDM does not issue the **ntp update-calendar** Cisco IOS command on Cisco 7200 routers if there are no new settings to enter and if the Network Time Protocol (NTP) server was configured using the CLI, only one NTP server IP address was provided and no ntp update-calendar Cisco IOS command was present in the running configuration.

  Workaround: Use SDM to delete the NTP server configuration entry, click Refresh, and then re-create the entry, or make changes to the existing NTP server entry.

- CSCee71373

  Because of a Cisco IOS issue (CSCee63313), if SDM is used to enable IPS on an interface, and then used to disable IPS on that interface, the router crashes.

- CSCee65422

  Due to a Cisco IOS issue (refer to CSCee58000), SDM is unable to configure a virtual auxiliary port on Cisco 831, 836, or 837 routers running Cisco IOS Release 12.3(7)XR1.

  Workaround: Load the rebuilt Cisco Release 12.3(7)XR2 image on the router when it becomes available and then use SDM to configure a virtual auxiliary port.

- CSCeg57729

  When SDM is installed on a PC, it cannot be launched if run from Netscape 7.1 or 7.2 and popup blockers have been enabled.

  Workaround: In Netscape, go to **Edit** > **Preferences** > **Privacy and Security** > **Popup Windows**. In the Popup Windows section, uncheck Block unrequested popup windows, and then click Apply. Relaunch SDM.

- CSCef89472

  A download exception message may appear in the Java console when SDM is launched on a PC running Japanese Windows 2000, or Japanese Windows XP. This problem does not prevent SDM from starting or from being used.

- CSCeg40910

  The SDM installation program does not use HTTPS to back up files from the router.

  Workaround: No workaround exists.

- CSCeg67630

  When SDM is invoked from SDM Express, and SDM Express has been started under a nondefault browser, you must reenter router username and password before SDM will start.

  Workaround: Use the default browser when launching SDM Express.

- CSCeg67964

  When SDM is installed on a PC running Windows XP with Service Pack 2, Internet Explorer will display a message bar at the top of the browser window stating: “To help protect your security, Internet Explorer has restricted this file from showing active content that access your computer. Click here for options...” Clicking **Allow blocked content** does not enable SDM to launch.

  Workaround: In Internet Explorer, go to **Tools > Internet Options > Advanced**. Then scroll to the Security section, check Allow active content to run in files on my computer**,** and click Apply. Then relaunch SDM.

- CSCeg74805

  When SDM is run with certain Cisco IOS images, the number of Open Shortest Path First (OSPF) processes created can be greater than the number of interfaces in the administratively UP state. However, the running configuration does not display the value of the area configured for these additional networks. Thus, SDM is unable to display the networks for these additional OSPF processes. This problem has been reported with the following Cisco IOS images:

  – c1700-k9o3sy7-mz.123-12.8.PI6

  – c836-k9o3sy6-mz.123-11.T2.bin

  – c181x-adventerprisek9-mz

  Workaround: No workaround exists.

- CSCeh05530

  If signatures are imported using SDM IPS on a router running Cisco IOS Release 12.3(11)T3, systemvariables parameters are ignored by Cisco IOS.

  Workaround: Upgrade to a Cisco IOS image that supports SystemVariables.

- CSCeh06870

  The SDM Update from PC feature will not operate when the SDM-V*nn*.zip file is placed in a shared folder with read-only access.

  Workaround: Do not place the SDM-V*nn*.zip file in a folder with read-only access.

- CSCeg63100

  Because of a problem with Cisco IOS (CSCeg63077), VPN troubleshooting will not detect the IKE mismatch in site-to-site VPN configuration. Instead it will give a generic recommendation to apply the mirror configuration generated by SDM which would solve this problem.

  Workaround: Follow the recommendation displayed in the VPN troubleshooting windowo to apply mirror configuration on both the devices.

Related Documentation

This section lists other documents with information on SDM.

Platform-Specific Documents

Refer to the quick start guide for the router, available on www.cisco.com, to learn how to set up the router hardware connections.

Software Documents

These documents are available on www.cisco.com/go/sdm.

- *Cisco Security Device Manager Q&A*. Click **Product Literature**, and then click **Q&A**.
- *Downloading and Installing Cisco Security Device Manager (SDM)*. Click **Install and Upgrade** in the Technical Documentation and Tools box, and then click **Install and Upgrade Guides**.

- *Switching from Cisco Router Web Setup Tool (CRWS) to Cisco SDM on Cisco 83X Series Routers*. Click **Install and Upgrade** in the Technical Documentation and Tools box, and then click **Install and Upgrade Guides**.
- A number of application notes are available by clicking **Reference Guides** in the Technical Documentation and Tools box, and then clicking Technical References

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_inpck/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 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
- 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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0601R)

Copyright © 2003-2005 Cisco Systems, Inc. All rights reserved.