



Release Notes For Cisco Router and Security Device Manager Version 1.2

6/24/2004

These release notes support Cisco Router and Security Device Manager 1.2. 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](#)
- [Installation Notes, page 7](#)
- [Important Notes, page 9](#)
- [Caveats, page 13](#)
- [Documentation Updates, page 22](#)
- [Related Documentation, page 22](#)
- [Obtaining Technical Assistance, page 23](#)

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), a firewall, Intrusion Protection System (IPS), Virtual Private Networks (VPNs), and other features on your router. SDM is installed in router Flash memory, and is run in a Web browser installed on a PC. SDM may be pre installed on the routers listed in the [“Hardware Supported” section on page 2](#).



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

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

System Requirements

This section contains SDM system requirements.

Memory Requirements

SDM requires 3.4 MB of free Flash memory space on supported routers.

Hardware Supported

This section lists the hardware that SDM supports.

Cisco Routers

SDM is supported on the following Cisco 800 series routers:

- Cisco 831
- Cisco 836
- Cisco 837

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 2600 series routers:

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

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 7000 series routers:

- Cisco 7204VXR
- Cisco 7206VXR
- Cisco 7301

Supported Network Modules, WICs, Port Adapters and Service Adapters

SDM supports configuration on following Network Modules.

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

SDM supports only Ethernet configuration on 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 async)
- WIC-1DSU-T1
- WIC-1ADSL
- WIC-1ENET
- WIC-1SHDSL
- WIC-1DSU-T1-V2
- WIC-1B-S/T
- WIC-1AM
- WIC-2AM
- WIC-4ESW
- WIC-1SHDSL-V2
- WIC-1B-S/T-V2

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

PC System Requirements

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

Software Supported

This section describes SDM software requirements.

Cisco IOS Images

SDM is compatible with the Cisco IOS images listed in [Table 1](#).

Table 1 *SDM-Supported Routers and Cisco IOS Versions*

| SDM-Supported Routers | SDM-Supported Cisco IOS Versions |
|--|--|
| Cisco 831 and 837 | <ul style="list-style-type: none"> • 12.2(13)ZH or later • 12.3(2)XA or later • 12.3(2)T or later |
| Cisco 836 | <ul style="list-style-type: none"> • 12.2(13)ZH or later • 12.3(2)XA or later • 12.3(4)T or later |
| Cisco 1701 | <ul style="list-style-type: none"> • 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 and 1712 | <ul style="list-style-type: none"> • 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, 1721, 1751, 1751-v, 1760, and 1760-v | <ul style="list-style-type: none"> • 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 1710 or 1721) |
| Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and 2691 | <ul style="list-style-type: none"> • 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 3640, 3661, and 3662 | <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • 12.2(11)T6 or later • 12.3(1)M or later |

Table 1 *SDM-Supported Routers and Cisco IOS Versions*

| SDM-Supported Routers | SDM-Supported Cisco IOS Versions |
|---------------------------|---|
| Cisco 3640A | <ul style="list-style-type: none"> • 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 and 3745 | <ul style="list-style-type: none"> • 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 7204VXR and 7206VXR | <ul style="list-style-type: none"> • 12.3(2)T or later • 12.3(1)M or later <p>SDM does not support B, E, or S train releases on the Cisco 7000 routers.</p> |
| Cisco 7301 | <ul style="list-style-type: none"> • 12.3(2)T or later • 12.3(3)M or later <p>SDM does not support B, E, or S train releases on the Cisco 7000 routers.</p> |

Determining the Cisco IOS Software Version

To determine the version 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:

- Netscape version 4.79 on all supported operating systems except Windows 98.
- Internet Explorer version 5.5 and later on all operating systems.

SDM is compatible with SUN Java Runtime Environment (JRE) versions 1.3.1, 1.4.1 and 1.4.2. If the JRE is not installed on your PC, SDM functions fully using the Java Virtual Machine (JVM) in your browser.

PC Operating System Versions

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

- Windows XP

- Windows 2000
- Windows ME
- Windows 98 (second edition)
- Windows NT 4.0 Workstation with Service Pack 4.

Installation Notes

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

Cisco 1700 Routers Running ITS/CCME and Cisco IOS Version 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, you may exceed the number of files allowed in Flash memory by installing SDM. Cisco 1700 routers using a Cisco IOS version 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 Your 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 your router. To obtain this document, visit the following URL.

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

Upgrading to a New SDM Release

If SDM is already installed on a router, and you are upgrading to a newer SDM release, you must also upgrade the configuration file for the router in order for new SDM software to function properly. The latest SDM configuration files are contained in the SDM .zip file, available from Cisco.com 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 obtain the SDM zip file and how to install SDM and all related files on your 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 your router and completing the following steps in EXEC mode:

Step 1 Type the following commands:

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

Step 2 Repeat the commands to delete the following additional files from Flash memory: sdm.shtml, home.tar, home.html, and home.shtml (on Cisco 7xxx routers). Also delete the default configuration files if they are present in flash. These are named using the convention sdmconfig-*<model>*xxx.cfg. For example, the default configuration file for the supported 2600 platforms is sdmconfig-26xx.cfg. No default configuration file is provided for Cisco 7xxx routers.

Step 3 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.

New and Changed Information

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

New Features Supported in SDM Release 1.2

SDM version 1.2 supports the following new features:

- IOS IPS—SDM allows you to enable IOS Intrusion Protection System on router interfaces and to specify the traffic direction on which the feature is to apply.
- MD5 hash algorithm encryption of user passwords—SDM allows you to perform one-way encryption of user passwords using the Message Digest 5 encryption algorithm.

Default Configuration File Changes

The SDM default configuration file has changed with SDM version 1.2. The changes are as follows:

- A DHCP server is configured on the lowest-numbered Ethernet port on Cisco 83x and Cisco 1701, 1710, 1711, and 1712 routers. The subnet number is 10.10.10.0, and the subnet mask is 255.255.255.248. Therefore, the DHCP server will grant addresses in the range 10.10.10.2 through 10.10.10.6. You must configure the PC to obtain an IP address automatically if SDM is running on one of these routers.
- A DHCP server is *not* configured on other supported Cisco routers. You must configure the PC with a static IP address in the range 10.10.10.2 through 10.10.10.6, and you must use the subnet mask 255.255.255.248.

Important Notes

This section contains important information for SDM.

Popup Blockers Disable SDM Online Help

If you have enabled popup blockers in the browser you use to run SDM, SDM online help will not display when you click the help button. To allow SDM online help to be displayed, you must disable the popup blocker when you run SDM. Popup blockers may be enabled in search engine toolbars, or may be stand-alone applications integrated with the web browser.

Configuring Your Router as an AAA Client

This section explains how you can configure your router as an Authentication, Authorization, and Accounting (AAA) client in a way that will enable the AAA server to authenticate users logging on to SDM.

Configure the AAA Server

Configure the AAA server by performing the following tasks:

-
- Step 1** Make sure you can ping your AAA server from your local router. If you can't ping the server, you may have to change the configuration on the local router or on the AAA server in order for the ping to succeed.
 - Step 2** Make sure you have configured your AAA server and added at least one user name/password, with the correct privileges. You must enter a username and password for each user you want to allow access to SDM. Refer to your AAA server configuration manual for instructions.
 - Step 3** On the AAA Server, add the information about the local router. If you have a Cisco Access Control Server, the steps are as follows:
 - a. Click the **Network Configuration** button on the left pane, to display the AAA Clients window in the right pane.
 - b. Click **Add Entry** button. The Add AAA Client window appears.
 - c. Enter the AAA client host name, the client IP address, for example 10.1.1.1, and a key, for example "sdm." In the Authenticate Using field, select **TACACS+(Cisco IOS)**.
 - d. Check **Single Connect TACACS+ AAA Client (Record stop in accounting on failure)**.
 - e. Click **Submit+Restart**.
-

Configure the local router as an AAA client by completing the steps in the next section.

Configure the Local Router as an AAA Client

Open a Telnet or console session to the router you want to be the AAA client, and complete the following steps to configure your router and then log on to SDM.

-
- Step 1** Enter configuration mode on the router.
- Step 2** Make sure you have defined at least one local user. The following sample line is entered in global configuration mode:
- ```
username lab privilege 15 password 7 121504151E0A0E
```
- Step 3** Enter the following AAA commands in global configuration mode:
- ```
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication ppp default group tacacs+ local
aaa authorization exec default group tacacs+ local
aaa authorization network default group tacacs+ local
!
tacacs-server host 10.1.1.1
tacacs-server directed-request
tacacs-server key sdm
!
ip http authentication aaa
!
```
- Step 4** Exit configuration mode.
- Step 5** Open a web browser window and enter the URL to start SDM on the router you just configured.
- ```
http://router IP-address
```
- Replace *router IP-address* with the IP address of the router interface the PC is connected to.
- Step 6** Click **Cisco Router and Security Device Manager** on the left panel of the router home page.
- Step 7** The AAA server will authenticate you. Enter the user ID and password you defined on the AAA server in the login and password dialog box.
- 

All users accessing SDM on this router will be authenticated by the AAA server.

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

Because a default configuration file is provided on a router shipped with SDM, it 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 your router's 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 your router, from the blue console port on your router to a serial port on your PC. Refer to your router's Hardware Installation Guide for instructions.
- Step 2** Connect the power supply to your router, plug the power supply into a power outlet, and turn on your router. Refer to your router's 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 your 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 IOS startup sequence. You can use the startup sequence to give your 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 your router.

## Unable to perform 'squeeze flash'

If your router is using a Cisco IOS image with a version earlier than 12.3 in the T release, or 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** will remove SDM and the Cisco IOS image from the router's Flash memory, and you will lose your connection to the router. Complete the following steps to save files in Flash, 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, the file SDM.tar, and the file SDM.shtml from Flash to a TFTP server:

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

Example:

```
copy flash: sdm.tar tftp://10.10.10.3/SDM.tar
```

**Note**

If you prefer to download a Cisco IOS image, the file SDM.tar, and the file SDM.shtml, follow these instructions to use an Internet connection to download an SDM-supported Cisco IOS image, the files SDM.tar, and the file SDM.shtml, then place those files on a TFTP server.

- 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 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 files SDM.tar and SDM.shtml, then save SDM.tar and SDM.shtml to the TFTP server.

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

- 
- Step 6** From the PC, log onto the router using telnet, and enter Enable mode.
- Step 7** Enter the command **erase flash:**, and confirm. The router's IOS image, configuration file, the file SDM.tar, and the file SDM.shtml are removed from Flash memory.
- Step 8** Use the **copy tftp** command to copy the IOS image and SDM.tar from the TFTP server to the router:

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

Example:

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

**Note**

Copy the Cisco IOS image first, followed by the files sdm.tar and sdm.shtml. Then copy the files home.html (home.shtml on Cisco 7xxx routers), and home.tar.

- 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:** has been performed on the router, you will be able to execute the squeeze flash command when necessary.

## Restrictions and Limitations

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

### Restrictions for SDM Running on Cisco 7204VXR, 7206VXR, and 7301 Routers

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

- The SDM Startup wizard does not operate.
- WAN configuration is not supported. SDM supports configuration of Ethernet and Fast Ethernet interfaces.
- The SDM Reset feature does not operate.
- No default configuration file is supplied.

## 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 1.2

This section lists caveats that are open in release 1.2.

- CSCin54600

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

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

**Workaround:**

On running Firewall wizard in an interface configured with Management Access policy select **Merge** option instead of **Replace** and proceed.

- CSCin57472

If SDM is launched in Netscape, using the Secure Shell (SSH) protocol, an SDM wizard launched for the first time will not deliver the configuration to the router when you click **Finish**. This problem occurs on PCs with processors slower than Pentium III processors, or on PCs with low memory.

**Workaround:**

While in SDM, select **Advanced Mode** and click **Deliver**. The configuration generated in Wizard mode will be delivered to the router. Once this configuration has been delivered to the router using the **Deliver** button, the LAN, WAN, Firewall, and other wizards will deliver the configuration when you click **Finish**.

Alternatively, you can close SDM, and relaunch it using Internet Explorer 5.5 or later. If you want to use Netscape, invoke SDM using the Telnet protocol. Do this by starting SDM as usual, and clicking **Cancel** in the Enter SSH Credentials window. SDM will display another username and password dialog. Enter the username and password in that window and click **OK**.

- CSCin57344

If the Intrusion Detection Device Manager (IDM) is launched using SDM set to automatic discovery of IP address, IP address discovery may fail. This is a rare problem that occurs when the SSH protocol is used to launch SDM in Netscape 4.79.

**Workaround:**

Close SDM. Clear the browser cache and try to relaunch the IDM after a short time. You can also try using Internet Explorer 5.5 or later to launch SDM.

- CSCec31789

When updating 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. This problem rarely occurs.

**Workaround:**

Restart the router to be able to perform operations on flash. 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 user executes Reset To Factory Defaults in SDM.

If router is running a Cisco IOS image of version 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 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 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).

- CSCin33529

SDM may require up to 10 seconds to launch when being run using Internet Explorer version 6.0 with service pack 1 and JRE version 1.4.1\_01 to configure a new serial WAN connection in Wizard mode.

**Workaround**

Upgrade the Java Plug-in to the latest version available from the Sun website at the following URL:<http://java.sun.com/>.

Alternatively, disable the Java plug-in. In Internet Explorer, click **Tools**, select **Internet Options**, click **Advanced**, and uncheck the Use Java 2 v1.4.1\_01 option. In Netscape, click **Edit**, select **Preferences**, click **Advanced**, and uncheck **Enable Java Plug-in**.

- CSCin40379

Text display is cut and scrolling causes loss of text in Security Audit when browser uses the Java Runtime Environment (JRE) 1.3.1\_07 plug-in.

Various text messages are cut and not displayed properly in the Security Audit feature if JRE 1.3.1\_07 is installed on the system. For example, the report card contains incomplete sentences, and scrolling up and down in the "Fix It" window causes many of the lines to disappear or to appear incomplete.

The problem is seen only when the plug-in is installed.

**Workaround**

Upgrade Java Plug-ins to the latest version available from the Sun website at the following URL:

<http://java.sun.com/>

Alternatively, disable the Java plug-in. In Internet Explorer, click **Tools**, select **Internet Options**, click **Advanced**, and uncheck the **Use Java 2 v1.3.1\_07** option. In Netscape, click **Edit**, select **Preferences**, click **Advanced**, and uncheck **Enable Java Plug-in**.

- CSCea89054

If you delete a WAN connection that you created in Wizard mode, 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 to Interfaces and Connections in Advanced Mode, select 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 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 router to use 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](http://www.cisco.com/en/US/products/hw/routers/ps259/products_data_sheet09186a0080088750.html)

- CSCeb01244

In Advanced Mode 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 your router.

- CSCea80627

After the SDM Startup Wizard has been completed by the user, SDM terminates and all browser windows close except the browser window hosting the Applet area, when run in Netscape Communicator version 4.79.

**Workaround**

Manually close the browser window(s) that remain open.

- CSCdy80223

When SDM runs with a Cisco IOS image of a version earlier than 12.3 in the T release, or earlier than version 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:

- Select the Easy VPN tunnel in the VPN Connections window and click **Disconnect**. If the Connect/Disconnect button is disabled, select 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 Associations tab, and reselect the Easy VPN connection name

- CSCeb05125

When SDM is run in Internet Explorer using Java Plug-in 1.3.1\_07, some text in the Wizard Mode Reset to Factory Defaults screen gets cut off.

**Workaround**

Resize the SDM window to display all text. Upgrade Java Plugins to the latest version available from the Sun website at the following URL:

<http://java.sun.com/>

- CSCea69632

When run using Netscape version 4.79, all SDM windows display a blank signature in the lower left corner. The text "Signed by:" appears, but no signature text follows.

**Workaround**

None needed. This does not affect the operation of the router.

- 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 onto 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 IOS version 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, select 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 runs with a Cisco IOS image of version 12.2(15)T, SDM fails to download the configuration file from the CNS server through startup wizard. Please refer Bug CSCin65539 for more details. This issue occurs only with Cisco IOS image version 12.2(15)T.

**Workaround:**

Upgrade to Cisco IOS image version 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's Flash Disk or compact Flash 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 compact Flash 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 IOS image, and then invoke SDM. See [Table 1 on page 5](#) for the Cisco IOS versions 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 type 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 4t+ PA.

- 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. An IOS bug (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:**

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 in Wizard Mode, SDM may report that the interface contains unsupported configuration parameters.

**Workaround:**

Click **Refresh** on the SDM toolbar, and delete the connection.

- CSCin64412

When shutting down SDM by clicking the X button in the top-right corner of the browser window, occasionally the parent Internet Explorer windows do not close, and it is necessary to restart the PC in order to close the window and restart SDM. Another instance of SDM cannot be opened if the parent windows of a previous instance of SDM are still open. This problem occurs on PCs running Windows 98 SE.

- CSCed18560

The Interfaces and Connections window may display the Backup option in disabled state for Async 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 Async 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 select Yes, SDM removes the backup configuration, but the Interfaces and Connections window still shows the backup option as disabled, preventing you from selecting the Async interface as a backup interface. The same problem occurs in Wizard Mode if you change the IP Address type of the Primary interface using the Edit button in the Wizard Mode window.

**Workaround:**

Delete the Async interface configuration using the Interfaces and Connections window.

- CSCin35643

When all WAN connections have been configured, the SDM WAN wizard may not display the Edit Connection and the Delete Connection buttons when the WAN wizard window is resized. This problem does not always occur.

**Workaround:**

If you need to use the Edit Connection or Delete Connection button, try the following to redisplay the buttons:

- Navigate to another Wizard mode window and then return to the WAN Wizard window.
- Resize the SDM window manually until the buttons reappear.
- Use the Maximize and Minimize icons on the top right of the SDM window to resize the window.
- If the Edit Connection and Delete Connection buttons still do not display, restart SDM.

- CSCin64039

The Show Running Configuration window is blank when the size of the running configuration approaches 200 KB. This problem occurs when SDM is run under Windows 98, using Internet Explorer 6.0 running JRE.1.3.1.08.

**Workaround:**

Either disable the plugin, or upgrade the JRE plugin to version 1.4.1 or later.

- CSCin48956

When the router is configured to use PPPoE, a user may not be able to download a file using FTP or display web pages from Internet hosts that he is able to ping or telnet to. 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. Telnet to the router and enter the following command in VLAN or Token Ring interface configuration mode.

**ip tcp adjust-mss 1452**

- CSCed00381

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

**Workaround:**

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

- CSCed25696

SDM may take up to 12 seconds to display the DMVPN Hub and Spoke wizard after it is selected and the **Launch the selected task** button is clicked. This latency may occur if a JRE plugin 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 plugin is running in the browser.

- CSCed34587

Using an interface configured with IP unnumbered as a DMVPN tunnel source may cause the Cisco IOS to crash. An interface configured as IP unnumbered uses the IP address of another interface on the router. This 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.

- CSCin65767

SDM cannot be launched successfully using Internet Explorer if the browser is using java plugin 1.3.1 or 1.4.1 and java plugin 1.4.2 is installed but not integrated in Internet Explorer.

**Workaround:**

Use custom installation mode to install java plugin 1.4.2, and select the option to integrate the plugin with Internet Explorer.

- CSCed91235

The router reloads when an NHRP tunnel interface is removed. This is an IOS caveat which you may encounter when deleting a Dynamic Multipoint VPN tunnel. This caveat duplicates CSCed41641. 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 an IOS caveat, CSCin69090. This occurs on routers using Cisco IOS images of version 12.3(4)XG or later, or Cisco IOS version 12.3(7)T. There is no workaround for this problem.

- CSCed92739

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

**Workaround:**

Start SDM by entering `http://<ip-address>`. Do not use `https://<ip-address>`.

- CSCee67639

The SDM Startup Wizard may fail if the router is running Cisco IOS version 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.

- CSCee37365

If SDM is run under Netscape 4.79, a null pointer exception may appear in the Java console after completion of the Startup wizard. Although this exception may appear, the configuration commands are delivered to the router, and no further action is required on the part of the user. This problem is seen with any communication protocol in use between the PC and the router, e.g. Telnet, SSH (Secure Shell) and PAI, and when Netscape 4.79 is run on any supported version of Microsoft Windows.

**Workaround:**

Avoid using Netscape 4.79. Instead, use Internet Explorer version 6.0 or later.

- CSCee22688

When SDM is run using JRE 1.4.1, adjacent WAN wizard dialogs overlap when an Ethernet or a Serial interface is being configured for the first time. Overlapping ceases when the mouse is moved, or when another key is pressed.

**Workaround:**

Go to the following URL and obtain JRE 1.4.2:

<http://java.sun.com>

Alternatively, disable the Java plug-in. In Internet Explorer, click Tools, select Internet Options, click Advanced, and uncheck the Use Java 2 v1.4.1 option.

- CSCin74090

SDM may not deliver configurations to the router when it is run using Netscape 4.79. This may happen when SDM wizards, including the Startup wizard, are used to deliver configuration changes, and primarily when the communications protocol with the router is SSH. This issue has been found when the router is running Cisco IOS 12-11T, 12-13T, and 12-15T images, and when Netscape 4.79 is run under any supported version of Microsoft Windows.

**Workaround:**

Avoid using Netscape 4.79, especially if SSH or Telnet is used to communicate with the router. Instead, use Internet Explorer version 6.0 or later.

- CSCed13205

, SDM does not issue the **ntp update-calendar** 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 and only one NTP server IP address was provided and no ntp update-calendar IOS command was present in the running configuration.

**Workaround:**

Use SDM to delete the NTP server configuration entry, click Refresh, and then recreate the entry, or make changes to the existing NTP server entry.

- CSCee71373

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

**Workaround:**

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

## Resolved Caveats—Release 1.2

The following caveats have been resolved in SDM version 1.2:

- CSCin70278

An ISDN connection configured using SDM may not come up if the router is running Cisco IOS versions 12.3(7)T or 12.3(6) and if the ISDN connection was created after deleting an existing ISDN connection. This problem has been resolved in this release.

# Documentation Updates

The following sections explain how documentation may be inaccurate or incomplete.

## Omissions

The following sections explain information that was not included in documentation.

### Cisco Router and Security Device Manager (SDM) Quick Start Guide: Disable Proxy Settings

SDM will not launch when run under Internet Explorer using JRE plugin versions 1.3.1, 1.4.0, 1.4.1, or 1.4.2 and proxy settings are enabled. To correct this problem, select **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.

## SDM Default Configuration File

SDM includes a default configuration file. The configuration does the following:

- Provides an IP address for your Fast Ethernet interface, enabling an interface to your LAN
- Enables your router's HTTP server, allowing http access from your LAN
- Creates a default username (**cisco**) and password (**cisco**) with privilege level 15
- Enables Telnet access to the router from your LAN



#### Note

---

The default configuration included does not configure any WAN interfaces. To connect to the Internet, you must use SDM to configure a WAN interface.

---



#### Caution

---

It is highly recommended that you change the username and password values because they are well known. If you do not change the username and password values from the default, you will have a security risk because your router will be vulnerable to attacks.

---

## Related Documentation

This section lists other documents with information on SDM.

## Platform-Specific Documents

Refer to the Quick Start Guide for your router, available on [www.cisco.com](http://www.cisco.com), to learn how to start SDM for the first time.

## Software Documents

These documents are available on [www.cisco.com/go/sdm](http://www.cisco.com/go/sdm)

- Cisco Security Device Manager (SDM) Frequently Asked Questions.
- Downloading and Installing Cisco Security Device Manager (SDM)
- Switching Between Cisco Security Device Manager (SDM) and Cisco Router Web Setup Tool (CRWS) on Cisco 83X Series Routers

## Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to [bug-doc@cisco.com](mailto: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.

## Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

## Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—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.

### Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

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

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

### Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

---

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section.

a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, 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, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0711R)

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

