



Release Notes For Security Device Manager Version 1.0.1

11/12/03

These release notes support Security Device Manager 1.0.1b. These release notes 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 5](#)
- [Important Notes, page 7](#)
- [Caveats, page 11](#)
- [Documentation Updates, page 17](#)
- [Related Documentation, page 18](#)
- [Obtaining Documentation, page 19](#)
- [Obtaining Technical Assistance, page 20](#)
- [Obtaining Additional Publications and Information, page 22](#)

Introduction

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, 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 Cisco Systems, Inc. All rights reserved.

System Requirements

This section contains SDM system requirements.

Memory Requirements

SDM requires 2.8 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

Network Modules and WICs Supported

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

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, 836, and 837	12.2(13)ZH or later.
1701, 1710, 1721, 1751, 1751-v, 1760, and 1760-v	<ul style="list-style-type: none"> • 12.2(13)ZH, or later • 12.2(13)T3 or later • 12.3(1)M or later • 12.2(15)ZJ2 or later • 12.2(11)T6 not supported
1711, 1712	<ul style="list-style-type: none"> • 12.2(15)ZL or later • 12.2(15)ZJ2 or later
Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and 2691	<ul style="list-style-type: none"> • 12.2(11)T6 or later • 12.3(1)M or later • 12.2(13)T3 • 12.2(15)ZJ • 12.2(15)ZJ2 or later

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

SDM-Supported Routers	SDM-Supported Cisco IOS Versions
Cisco 3620, 3640, 3640A, 3661, and 3662	<ul style="list-style-type: none"> • 12.2(11)T6 or later • 12.3(1)M or later • 12.2(13)T3 • 12.2(15)ZJ2 or later
Cisco 3725 and 3745	<ul style="list-style-type: none"> • 12.2(11)T6 or later • 12.3(1)M or later • 12.2(13)T3 or later • 12.2(15)ZJ2 or later

Determining the Cisco IOS Software Version

To determine the version of Cisco IOS software currently running on your Cisco 820 series 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

SDM can be used with the following browsers:

- Netscape version 4.79
- Internet Explorer version 5.5 and later.

PC Operating System Versions

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

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

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 Security Device Manager (SDM) Version 1.0* 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 Security Device Manager (SDM) Version 1.0* 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, 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]
router#squeeze flash:
```

Step 2 Repeat the commands to delete the following additional files from Flash memory: sdm.shtml, sdmconfig-*<model>*xxx.cfg. sdmconfig-*<model>*xxx.cfg represents the default configuration file that is supplied with SDM. For example, the default configuration file for the supported 2600 platforms is sdmconfig-26xx.cfg.

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 1.0.1

SDM Release 1.0.1 supports the following new features:

- **SDM Update**—SDM can determine whether a newer version of SDM is available for download on Cisco.com, and can perform an update from the PC or directly from Cisco.com
- **Management Access**—SDM allows you to create management policies. These policies can specify the networks or hosts from which SDM can be run, and can specify the protocols that can be used to run SDM and manage the router in other ways. NTP client for Cisco 17xx, 26xx, 36xx, and 37xx routers.
- **Router date and time.** You can use SDM to configure the router's date and time, or use SDM to synchronize the router's date and time settings with the date and time settings on the PC.
- **Support for the Cisco IDS Network Module.**

Important Notes

This section contains important information for this release.

No Enable Password in Default Configuration File

The default configuration file shipped with earlier versions of SDM configured an enable password, which controlled access to the CLI via the console port. The default configuration files provided with SDM version 1.0.1a do not configure an enable password.

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:
- Click the **Network Configuration** button on the left pane, to display the AAA Clients window in the right pane.
 - Click **Add Entry** button. The Add AAA Client window appears.
 - 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)**.
 - Check **Single Connect TACACS+ AAA Client (Record stop in accounting on failure)**.
 - 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/flash/sdm.shtml
```

Replace *router IP-address* with the IP address of the router interface the PC is connected to.

- Step 6** 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 **sdm**.
- ```
yourname> enable

Password: sdm
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.

- 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.

## 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 1.0.1

This section lists caveats that are open in release 1.0.1.

- CSCec38346

When updating SDM using Netscape 4.79, SDM occasionally is unable to contact the Cisco.com webserver when the webserver is running, and displays the message "Contacting Cisco.com for SDM updates. Please wait ..."for an indefinite time. The user has to shut down the web browser to dismiss the message. If the web server is actually down, the following message is displayed:

"SDM failed to contact Cisco.com. Please check that your internet connection is up. Then try again."

**Workaround:**

Before launching SDM or performing SDM updates, clear the browser cache.

- 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.

- CSCec39725

In SDM updates, back up will fail for the image 12.2(13)T8. This is because the time stamps that the SDM backup feature checks to compare modification dates are not present in Flash memory. If the file being checked is an SDM file, the back up of that file fails.

**Workaround:**

Configure date and time on the router—the SDM Date/Time feature can be used for this—and try SDM Updates again. This time ignore the back up option by clicking "No" when prompted. Backup will still not work, but update will work fine.

- CSCec41131

Configuration of NTP client using SDM fails if an interface configured as a firewall trusted interface is deleted.

**Workaround:**

Use the CLI to remove the description "\$FW\_INSIDE\$" from any interface that does not have an IP address configured.

The command **no description** entered in interface configuration mode removes the description.

- CSCea84865

In routers running a Cisco IOS image of version 12.2(11)T6, SDM treats PPPoE connections that do not contain the **vpdn-enable**, **vpdn-group**, **request-dialin**, and **protocol pppoe** commands as read only. The Edit button is not enabled in the Interfaces and Connections window, and the connection is treated as "Other" in the WAN window.

If SDM is subsequently used to configure another PPPoE connection on the router, those commands are added, and the original PPPoE connections are made complete. However SDM will not show these original connections as editable.

**Workaround**

Select **Refresh** from the View menu to make SDM display these PPPoE connections as editable.

- CSCea89141  
Port Address Translation (PAT) rules configured with no access list using the CLI are not removed when using SDM to delete WAN connections the rules are associated with.

**Workaround**

Remove the PAT rules using the CLI.

- CSCin40086  
SDM can take more than 30 seconds to switch from Advanced Mode to Wizard Mode.
- CSCin42927  
When performing Security Audit from a PC with more than one Network Interface Card (NIC) which is in one of the directly connected Inside Interface networks (as chosen by the user), "Access class not set on VTY lines" security problem as reported cannot be fixed.
- 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 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.

- 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.



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

- 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.

- CSCea68007

Due to an IOS caveat, if you configure an Ethernet connection with a dialer-pool command, such as a PPPoE connection, subsequently delete the connection, then configure an ATM connection with PPPoE, and then recreate the Ethernet connection with the **dialer-pool** command, that Ethernet configuration will contain multiple **dialer-pool** statements, and be read-only in SDM.

**Workaround**

Use the CLI to remove all PPPoE and dialer-pool statements from the Ethernet interface configuration. After saving the configuration, save the running configuration to the startup configuration. Then, reload the router and reconfigure the Ethernet connection.

- CSCin48956

When configuring Point-to-Point Protocol over Ethernet (PPPoE) for the Cisco 1711 or 1712 VLAN1 interfaces, SDM does not deliver the **ip tcp adjust-mss** command to the router's configuration.

**Workaround**

Use the CLI to add the **ip tcp adjust-mss** command to the VLAN1 interface configuration. Telnet to the router and enter the following command in VLAN1 interface configuration mode.

**ip tcp adjust-mss 1452**

- 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.

## Resolved Caveats - Release 1.0.1

This section lists caveats that are resolved in release 1.0.1.

- CSCeb65816

SDM does not show Open Shortest Path First (OSPF) as a supported routing protocol for 83x routers running Cisco IOS version 12.3(2) XC images. This problem has been resolved in this release.

- CSCin60785

When SDM is invoked on routers running Cisco IOS version 12.3(4)T, the controls on SDM windows are disabled. This problem has been resolved in this release.

- CSCec68028  
Routers with a large Cisco Express Forwarding (CEF) table may find that SDM 1.0.1 takes an extremely long time to load. This problem has been resolved in this release.
- CSCec74657  
The default configuration file shipped with SDM had no banner, and contained an enable password. A banner has been added to the default configuration file, and the enable password has been removed from the configuration file in this release.
- CSCin61509  
SDM's IDS Network Module Management feature is does not work on routers running Cisco IOS images of version 12.3(4T) because the Secure Shell (SSH) version used by SDM and the version used by IOS are not compatible. This problem has been resolved in this release. If SDM detects differing SSH versions, it will use Telnet.
- CSCin61499  
Static Network Address Translation (NAT) rules are shown as read-only by SDM on routers running Cisco IOS images of version 12.3(4T). When a user creates a static NAT rule and delivers it to the router, SDM displays the rule as read-only. This problem has been fixed 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.

### 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 (**sdm**) and password (**sdm**) 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.

It is highly recommended that you change the username and password values because they are well known. SDM will help you change those values. Please refer your router's Quick Start Guide for information on how to launch SDM.



#### Caution

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.

## SDM Is Not Supported on SOHO 91, SOHO 96, and SOHO 97 Routers.

The Cisco 831, 836, and 837 Cabling and Setup Quick Start Guides do not state that SDM is not supported on the SOHO 91, SOHO 96, and SOHO 97 routers. The SOHO series of routers do not support SDM.

## Modifying the Default Configuration File in Cisco 3620 and 3640 Routers

The instructions provided in the Cisco 3620 and 3640 Modular Access Routers Quick Start Guide for Starting SDM might not work.

The initial communication between a browser running on a PC and SDM is controlled by the default configuration file for the router. On most supported routers, SDM uses a fixed Fast Ethernet port at address `0`, Fast Ethernet 0/0 or Fast Ethernet 0. The PC is connected to this interface, and the interface is given an IP address in the default configuration file that SDM recognizes.

For the 3620 and 3640 routers there are no fixed Ethernet ports.

By convention many of these routers ship with a Fast Ethernet capable network module in Slot 0. SDM assumes this to be the case in its default configuration file. If this is not true for your router, you need to modify the default configuration file to enable and provide an IP address for an Ethernet interface before SDM can communicate with the router.

Perform the following steps to enable SDM to communicate with the browser:

- 
- Step 1** Log on to the router using the Console port, using the user name `sdm`, and password `sdm`.
  - Step 2** Enter Enable mode using the password `sdm`.
  - Step 3** Provide the IP address `10.10.10.1` and the subnet mask `255.255.255.0` for the interface you will connect the PC to, and enter the `no shutdown` command to enable the interface.
  - Step 4** Save the configuration.
  - Step 5** Connect a PC running a supported browser to the interface you configured.
  - Step 6** Enter the IP address `10.10.10.1` in the browser to start SDM.
- 

## 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) 1.0 Frequently Asked Questions.
- Downloading and Installing Cisco Security Device Manager (SDM) Version 1.0
- Switching Between Cisco Security Device Manager (SDM) and Cisco Router Web Setup Tool (CRWS) on Cisco 83X Series Routers

## Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

[http://www.cisco.com/en/US/partner/ordering/ordering\\_place\\_order\\_ordering\\_tool\\_launch.html](http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html)

All users can order monthly or quarterly subscriptions through the online Subscription Store:

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

### Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpck/pdi.htm](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 Networking Products MarketPlace:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## 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.

## Obtaining Additional Publications and Information

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:  
[http://www.cisco.com/en/US/products/products\\_catalog\\_links\\_launch.html](http://www.cisco.com/en/US/products/products_catalog_links_launch.html)
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:  
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:  
<http://www.cisco.com/go/packet>
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. 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/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:  
[http://www.cisco.com/en/US/learning/le31/learning\\_recommended\\_training\\_list.html](http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html)

---

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 Cisco Systems, Inc. All rights reserved.

