



# Release Notes for Cisco Router and Security Device Manager 2.3.3

---

**February 13, 2007**

These release notes support Cisco Router and Security Device Manager version 2.3.3. They should be used with the documents listed in the “[Related Documentation](#)” section. These release notes are updated as needed.

## Contents

This document contains the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New and Changed Information, page 11](#)
- [Limitations and Restrictions, page 15](#)
- [Important Notes, page 15](#)
- [Caveats, page 20](#)
- [Related Documentation, page 32](#)

## Introduction

Cisco Router and Security Device Manager (Cisco SDM, and hereinafter called SDM) is a web-based configuration tool that allows you to configure LAN and WAN interfaces, routing, Network Admission Control (NAC), Network Address Translation (NAT), firewalls, Intrusion Prevention System (IPS), Virtual Private Networks (VPNs), and other features on the router. SDM 2.1 and later versions can be installed on a PC, or in router flash, disk, or slot memory. Earlier versions of SDM cannot be installed on PCs, and can be installed in router flash, disk, or slot memory. If you have a router listed in the “[Hardware Supported](#)” section on page 2, SDM is either preinstalled in router memory, or is shipped on a CD with the router.



---

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

Copyright © 2003-2007 Cisco Systems, Inc. All rights reserved.

Cisco SDM Express allows you to give a router a basic LAN, WAN, firewall and NAT configuration. It is installed in router memory.

## System Requirements

This section contains SDM system requirements.

## Memory Requirements

[Table 1](#) shows how much memory is required to support Cisco SDM files.

**Table 1** Cisco SDM Memory Requirements

Cisco Router Model Series	Minimum Memory Required for Cisco SDM Files
Cisco 830, Cisco 850, Cisco 850W, Cisco 1700	5.9
Cisco 870, Cisco 870w, Cisco1800, Cisco 2600XM, Cisco 2800, Cisco 3600	6.1
Cisco 2691, Cisco 3700, Cisco 3800, Cisco 7200, Cisco 7301	6.4

2 MB of router memory is required to support Cisco SDM Express files.

The Wireless Management application requires an additional 2 MB.

Cisco SDM installed on a PC requires 5.9 MB of memory.

[Table 2 on page 7](#) lists the files that are included with Cisco SDM, Cisco SDM Express, and the Wireless Management application.

## Hardware Supported

This section lists the routers that SDM supports, by series.



### Note

SDM does not support Telco/CO router models.

Cisco SB100 series:

- Cisco SB101
- Cisco SB106
- Cisco SB107

Cisco 800 series:

- Cisco 831
- Cisco 836
- Cisco 837
- Cisco 851

- Cisco 857
- Cisco 871
- Cisco 876
- Cisco 877
- Cisco 878

SDM is supported on the following Cisco 1700 series:

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

Cisco 1800 series:

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

Cisco 2600 series:

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

2800 series:

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

Cisco 3600 series:

- Cisco 3620
- Cisco 3640

- Cisco 3640A
- Cisco 3661
- Cisco 3662

SDM is supported on the following Cisco 3700 series:

- Cisco 3725
- Cisco 3745

SDM is supported on the following Cisco 3800 series:

- Cisco 3825
- Cisco 3845

SDM is supported on the following Cisco 7000 series:

- Cisco 7204VXR
- Cisco 7206VXR
- Cisco 7301

## Supported Adapters, Cards and Network Modules

Network modules:

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

- NMD-36ESW-2GIG
- NMD-36ESW-PWR
- NMD-36ESW-PWR-2GIG

SDM supports only Ethernet configuration on the following network modules:

- NM-1E1R2W
- NM-1FE1R2W
- NM-1FE1CE1U
- NM-1FE2CE1B
- NM-1FE1CE1B
- NM-1FE2CE1U
- NM-1FE1CT1
- NM-1FE2CT1
- NM-1FE1CT1-CSU
- NM-1FE2CT1-CSU

EtherSwitch Service Network Modules:

- NME-16ES-1G-P
- NME-X-23ES-1G-P
- NME-XD-24ES-1S-P
- NME-XD-48ES-2S-P

WAN interface cards:

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

## High-speed WAN interface cards (HWICs):

- HWIC-4T
- HWIC-4A/S
- HWIC-8A/S-232
- HWIC-4ESW
- HWICD-9ESW
- HWIC-AP-G-X
- HWIC-AP-AG-X
- HWIC-ADSL-B/ST
- HWIC-ADSLI-B/ST
- HWIC-1ADSL
- HWIC-1ADSLI

## Advanced integration modules (AIMs):

- AIM-VPN/BP
- AIM-VPN/BP II
- AIM-VPN/BPII-PLUS
- AIM-VPN/HP
- AIM-VPN/HP II
- AIM-VPN/HPII-PLUS
- AIM-VPN/EP
- AIM-VPN/EP II
- AIM-VPN/EPII-PLUS
- AIM-VPN/SSL-1
- AIM-VPN/SSL-2
- AIM-VPN/SSL-3

## Port adapters on Cisco 7000 family routers:

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

## Network Processing Engines and Network Service Engines on Cisco 7000 family routers.

- NPE-225
- NPE-400
- NPE-G1
- NPE-G2
- NSE-1

## Service adapters on Cisco 7000 family routers:

- SA-VAM

- SA-VAM2
- SA-VAM2+
- C7200-VSA

SDM also supports the MOD-1700VPN.

## PC System Requirements

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

## Software Supported

This section describes SDM software requirements.

### Cisco IOS Releases

SDM is compatible with the Cisco IOS releases listed in [Table 2](#).



Note

SDM supports the Cisco IOS Intrusion Prevention System (Cisco IOS IPS). In order to be able to use SDM to configure the Cisco IOS IPS software, the router must run Release 12.3(8)T4 or a later release. Later Cisco IOS releases support additional Cisco IOS IPS functionality. [Table 3](#) lists the Cisco IOS IPS feature history by Cisco IOS release.

**Table 2** *SDM-Supported Routers and Cisco IOS Releases*

SDM-Supported Routers	SDM-Supported Cisco IOS Releases
Cisco SB101 Cisco SB106 Cisco SB107	<ul style="list-style-type: none"> <li>• 12.3(8)YG</li> <li>• 12.4(2)T or later releases</li> </ul>
Cisco 831 Cisco 837	<ul style="list-style-type: none"> <li>• 12.2(13)ZH or later releases</li> <li>• 12.3(2)XA or later releases</li> <li>• 12.3(2)T or later releases</li> <li>• 12.4(2)T or later releases</li> </ul>
Cisco 836	<ul style="list-style-type: none"> <li>• 12.2(13)ZH or later releases</li> <li>• 12.3(2)XA or later releases</li> <li>• 12.3(4)T or later releases</li> <li>• 12.4(2)T or later releases</li> </ul>
Cisco 851 Cisco 857	<ul style="list-style-type: none"> <li>• 12.3(8)YI</li> <li>• 12.4(2)T or later releases</li> </ul>
Cisco 871 Cisco 876 Cisco 877 Cisco 878	<ul style="list-style-type: none"> <li>• 12.3(8)YI</li> <li>• 12.4(2)T or later releases</li> </ul>

**Table 2** *SDM-Supported Routers and Cisco IOS Releases (continued)*

<b>SDM-Supported Routers</b>	<b>SDM-Supported Cisco IOS Releases</b>
Cisco 1701	<ul style="list-style-type: none"> <li>• 12.2(13)ZH or later releases</li> <li>• 12.3(2)XA or later releases (SDM does not support Cisco IOS release 12.3(2)XF.)</li> <li>• 12.3(4)T or later releases</li> <li>• 12.4(2)T or later releases</li> </ul>
Cisco 1711 Cisco 1712	<ul style="list-style-type: none"> <li>• 12.2(15)ZL or later releases</li> <li>• 12.3(2)XA or later releases (SDM does not support Cisco IOS release 12.3(2)XF.)</li> <li>• 12.4(2)T or later releases</li> </ul>
Cisco 1710 Cisco 1721 Cisco 1751 Cisco 1751-v Cisco 1760 Cisco 1760-v	<ul style="list-style-type: none"> <li>• 12.2(13)ZH or later releases</li> <li>• 12.3(2)XA or later releases (SDM does not support Cisco IOS release 12.3(2)XF.)</li> <li>• 12.2(13)T3 or later releases</li> <li>• 12.3(2)T or later releases</li> <li>• 12.3(1)M or later releases</li> <li>• 12.2(15)ZJ3 (not available for the Cisco 1710 or Cisco 1721)</li> <li>• 12.4(2)T or later releases</li> </ul>
Cisco 1801 Cisco 1802 Cisco 1803 Cisco 1811	<ul style="list-style-type: none"> <li>• 12.3(8)YI</li> <li>• 12.4(2)T or later releases</li> </ul>
Cisco 1812	<ul style="list-style-type: none"> <li>• 12.3(8)YH or later releases</li> <li>• 12.4(2)T or later releases</li> </ul>
Cisco 1841	<ul style="list-style-type: none"> <li>• 12.3(8)T4 or later releases</li> <li>• 12.4(2)T or later releases</li> </ul>
Cisco 2610XM Cisco 2611XM Cisco 2620XM Cisco 2621XM Cisco 2650XM Cisco 2651XM Cisco 2691	<ul style="list-style-type: none"> <li>• 12.2(11)T6 or later releases</li> <li>• 12.3(2)T or later releases</li> <li>• 12.3(1)M or later releases</li> <li>• 12.3(4)XD</li> <li>• 12.2(15)ZJ3</li> <li>• 12.4(2)T or later releases</li> </ul>
Cisco 2801 Cisco 2811 Cisco 2821 Cisco 2851	<ul style="list-style-type: none"> <li>• 12.3(8)T4 or later releases</li> <li>• 12.4(2)T or later releases</li> </ul>

**Table 2** *SDM-Supported Routers and Cisco IOS Releases (continued)*

SDM-Supported Routers	SDM-Supported Cisco IOS Releases
Cisco 3640 Cisco 3661 Cisco 3662	<ul style="list-style-type: none"> <li>• 12.2(11)T6 or later releases</li> <li>• 12.3(2)T or later releases</li> <li>• 12.3(1)M or later releases</li> <li>• 12.3(4)XD</li> <li>• 12.2(15)ZJ3</li> <li>• 12.4(2)T or later releases</li> </ul>
Cisco 3620	<ul style="list-style-type: none"> <li>• 12.2(11)T6 or later releases</li> <li>• 12.3(1)M or later releases</li> </ul>
Cisco 3640A	<ul style="list-style-type: none"> <li>• 12.2(13)T3 or later releases</li> <li>• 12.3(2)T or later releases</li> <li>• 12.3(1)M or later releases</li> <li>• 12.3(4)XD</li> <li>• 12.2(15)ZJ3</li> <li>• 12.4(2)T or later releases</li> </ul>
Cisco 3725 Cisco 3745	<ul style="list-style-type: none"> <li>• 12.2(11)T6 or later releases</li> <li>• 12.3(2)T or later releases</li> <li>• 12.3(1)M or later releases</li> <li>• 12.3(4)XD</li> <li>• 12.2(15)ZJ3</li> <li>• 12.4(2)T or later releases</li> </ul>
Cisco 3825 Cisco 3845	<ul style="list-style-type: none"> <li>• 12.3(11)T or later releases</li> <li>• 12.4(2)T or later releases</li> </ul>
Cisco 7204VXR Cisco 7206VXR	<ul style="list-style-type: none"> <li>• 12.3(2)T or later releases</li> <li>• 12.3(1)M or later releases</li> <li>• 12.4(2)T or later releases</li> </ul> <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"> <li>• 12.3(2)T or later releases</li> <li>• 12.3(3)M or later releases</li> <li>• 12.4(2)T or later releases</li> </ul> <p>SDM does not support B, E, or S train releases on the Cisco 7000 routers.</p>

**Table 3** shows the Cisco IOS IPS feature history, and lists the Cisco IOS releases that offered each set of features, beginning with the latest release. This information is available in the Cisco IOS IPS Deployment Guide available at the following link.

[http://www.cisco.com/en/US/products/ps6634/prod\\_white\\_papers\\_list.html](http://www.cisco.com/en/US/products/ps6634/prod_white_papers_list.html)

**Table 3** Feature History of Cisco IOS IPS

Cisco IOS Release	Cisco IOS IPS Features or Improvements
12.4(6)T	Session setup rate performance improvements
12.4(3a)/12.4(4)T	String engine memory optimization
12.4(4)T	MULTI-STRING engine support for Trend Labs and Cisco Incident Control System Performance improvements Distributed Threat Mitigation (DTM) support
12.4(2)T	Layer 2 transparent intrusion prevention system (IPS) support
12.3(14)T	Support for three string engines (STRING.TCP, STRING.UDP, and STRING.ICMP) Support for two new local shunning event actions: denyAttackerInline and denyFlowInline
12.3(8)T	Support for Security Device Event Exchange (SDEE) protocol Support for ATOMIC.IP, ATOMIC.ICMP, ATOMIC.IPOPTIONS, ATOMIC.UDP, ATOMIC.TCP, SERVICE.DNS, SERVICE.RPC, SERVICE.SMTP, SERVICE.HTTP, SERVICE.FTP, and OTHER engines

### Determining the Cisco IOS Release

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

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

### Web Browser Versions and Java Runtime Environment Versions

SDM can be used with the following browsers:

- Firefox 1.0.6 and later versions
- Internet Explorer 5.5 and later versions
- Netscape 7.1 and 7.2

SDM requires Sun Java Runtime Environment (JRE). The following versions are supported:

- JRE1.4.2\_08
- JRE 1.5.0\_06
- JRE 1.5.0\_07

Although the SDM application requires JRE to run, the Cisco SDM Express application included with SDM can run under the native Java Virtual Machine in the supported browsers, and also JRE.

## PC Operating System Versions

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

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



**Note**

Windows 2000 Advanced Server is not supported.

SDM 2.3.3 is available only in English. SDM 2.2.1 is available in six additional languages: French, German, Italian, Japanese, Simplified Chinese, and Spanish and. SDM 2.2.1 supports full SDM functionality released prior to SDM 2.3. If you want to use SDM 2.2.1 in one of these languages, your PC must run one of the following operating systems:

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

See the Release Notes for Cisco Router and Security Device Manager Version 2.2.1 for more information.

## New and Changed Information

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

### New Cisco Secure Desktop Client Software and SSL VPN Client Software

The file SDM-V233.zip contains updated Cisco Secure Desktop Client software and SSL VPN Client software. These software packages are listed below:

- securedesktop-ios-3.1.1.45-k9.pkg, 1.61 MB
- sslclient-win-1.1.2.169.pkg, 405 KB

### Resolved Caveats in SDM 2.3.3

The following caveats have been resolved SDM 2.3.3:

- CSCek35024—The SDM configuration file `sdmconfig-modelnum.cfg` enforces the one-time use of the default credentials `cisco/cisco`. After logging on to the router for the first time, users must create a new username and password to replace the credentials `cisco/cisco` whether they logged on using SDM, using Telnet, or using the Console port.
- CSCsf21354—SDM no longer requires you to enter a domain name when configuring a single context and gateway. If you create additional contexts or gateways, you will be required to enter a domain name.

- CSCsf07616—SDM no longer displays an audit-trail off or audit-trail on message when delivering Application Firewall commands to the router.
- CSCsg19590—SDM Express delivers configuration commands to Cisco 857 routers running Cisco IOS release 12.4(6)T or higher.
- CSCsg18934—The SDM Firewall log now displays the IP address for listed top attackers.
- CSCek55990—SDM warns users who opt to modify an existing ACL to work with Network Address Translation (NAT) that the modification may introduce a security problem.
- CSCsg29317—SDM deletes WAN configurations when NAT has been configured on the WAN interface.
- CSCsg45552—The SDM Wireless application no longer generates a Java error message when you create a new IP Address filter in the Services: Filters -- IP filters screen.
- CSCsf19995—SDM no longer spuriously reports errors on port mapping statements entered using the Cisco IOS command line interface (CLI).
- CSCsg33987—When using the Basic Firewall wizard, the **Allow secure SDM from WAN** checkbox is disabled if HTTPS or SSH are not enabled, or if at least one outside interface is not configured with a static IP address. The SDM user interface now provides a help topic that explains this behavior and provides a help topic that explains how to enable HTTPS and SSH.

## SDM User Interface Incorporates New Cisco Systems Logo

The SDM user interface now displays the new Cisco Systems Logo in application screens and in the online help system.

## SDM Files

This section describes the files used in SDM version 2.3.3.

[Table 4 on page 12](#) describes the files that SDM and SDM applications use.

**Table 4** *SDM File List*

Filename	Size	Description
attack-drop.sdf	236 KB	Signature Definition File (SDF) used by Cisco IOS IPS
common.tar	1.0 MB	SDM and SDM Express support file
es.tar	825 KB	SDM Express application file
home.shtml	1.01 KB	SDM and SDM Express support file
home.tar	99 KB	SDM and SDM Express support file
sdmconfig-modelnum.cfg	2.0 KB	Default configuration file
For example: sdmconfig-180x.cfg		
sdm.tar	4.52 MB	SDM application file
sdmips.sdf	Variable	File created when SDM is used to modify Cisco IOS IPS signatures

Table 4 SDM File List (continued)

Filename	Size	Description
securedesktop-ios-3.1.1.45-k9.pkg	1.61 MB	Cisco Secure Desktop client software for WebVPN clients
sslclient-win-1.1.2.169.pkg	405 KB	Full tunnel client software for WebVPN clients
wlanui.tar	1.86 MB	Wireless Application
128MB.sdf	479 KB	Signature Definition File (SDF) used by Cisco IOS IPS
256MB.sdf	698 KB	Signature Definition File (SDF) used by Cisco IOS IPS

## Installation Notes

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

### Cisco 1700 Routers Running Cisco ITS/Cisco CallManager Express and Cisco IOS Release 12.2(13)T

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

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

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

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

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

### Upgrading to a New SDM Version

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

If you are currently using SDM 1.0, you must download the file SDM-Vnn.zip at the following URL:

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

See *Downloading and Installing Cisco Router and Security Device Manager (SDM)* to learn how to install SDM and all related files on the router at the following URL:

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

Click **Install and Upgrade** in the Technical Documentation and Tools box, and then click **Install and Upgrade Guides**.

## Uninstalling SDM Files

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

---

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

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

```
router# cd flash:
```

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

```
router# cd diskN
```

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

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

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

Press **Return** to confirm the deletion.

**Step 3** Use the **delete** command to remove the remaining SDM files. The “[SDM Files](#)” section on page 12 lists the files used by SDM.

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

```
router# squeeze flash:
```

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

---

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

---

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

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

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

---

# Limitations and Restrictions

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

## SDM Minimum Screen Resolution

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

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

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

- The SDM Express application is not supported. You must use the Cisco IOS CLI to give the router an initial configuration that will enable you to connect to the router using a browser.
- WAN configuration is not supported. SDM supports configuration of Ethernet and Fast Ethernet interfaces.
- The SDM Reset feature is not available.
- No SDM-default configuration file is supplied. To run SDM, you must provide a configuration that includes the commands necessary to support operation of SDM.

The document [Cisco Router and Security Device Manager \(SDM\), Version 2.3.1 User Guide for the Cisco 7000 Family](#) describes how to give the router a configuration that supports SDM and how to start SDM on Cisco 7000 Family routers.

## Important Notes

This section contains important information for SDM. It contains the following sections:

- [Cisco SDM Security Dashboard May Display Threats Unrelated to Your Cisco IOS IPS Installation, page 16](#)
- [SDM May not Launch Using IP Address of WebVPN Gateway, page 16](#)
- [SDM IPS User Guide Discontinued for SDM 2.2, page 16](#)
- [SDM May Lose Connection to Network Access Device, page 17](#)
- [SDM on PC May Not Launch under Windows XP with Service Pack 2, page 17](#)
- [Popup Blockers Disable SDM Online Help, page 17](#)
- [Disable Proxy Settings, page 17](#)
- [Routers Shipped with SDM Do Not Execute the Standard Cisco IOS Startup Sequence, page 18](#)
- [Unable to Perform “squeeze flash:” Operation, page 18](#)
- [Security Alert Dialog May Remain After SDM Launches, page 20](#)

## Cisco SDM Security Dashboard May Display Threats Unrelated to Your Cisco IOS IPS Installation

Some (or all) of the top threats you obtain using the Cisco SDM Security Dashboard may not pertain to your Cisco IOS IPS installation. After you deploy the signatures applicable to the top threats displayed by the Cisco SDM Security Dashboard, the Cisco SDM Security Dashboard may still display some (or all) top threats with a red icon because applicable signatures could not be found. Those remaining top threats are unrelated to your Cisco IOS IPS installation and not a danger to your router running Cisco IOS software.

## SDM May not Launch Using IP Address of WebVPN Gateway

This information provides more information about the caveat CSCek33306. When SDM attempts to connect to a router with a WebVPN gateway configured using the Cisco IOS CLI, it might not launch from the IP address used by that gateway if the CLI statements necessary for SDM access are not included.

For example, if you have configured a WebVPN connection on the interface Fe 0/0 with the gateway IP address 10.10.10.1, and the gateway name MyWebVPN, you may not be able to launch SDM using that IP address.

To be able to launch SDM using that IP address, add the following Cisco IOS CLI commands:

```
Router#config t
Router(config)# interface loopback next-available-loopback-number
Router(config-if)# description Do not delete - SDM WebVPN generated interface
Router(config-if)# ip address 192.168.1.1 255.255.255.252
Router(config-if)# no shutdown
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# ip nat inside source static tcp 192.168.1.1 443 10.10.10.1 4443
Router(config)# router(config)# webvpn gateway MyWebVPN
Router(config-webvpn-gateway)# http-redirect port 80
Router(config) # interface FastEthernet 0/0
Router(config-if)# ip nat outside
Router(config-if)# exit
```

After adding these commands, you can launch SDM by entering the following IP address and port in the browser:

```
https://10.10.10.1:4443
```

If you remove the WebVPN gateway that was modified for SDM access, you must remove the loopback interface and NAT rule that you created to allow access in the first place. Enter the commands shown in the description of caveat CSCek38259.

## SDM IPS User Guide Discontinued for SDM 2.2

The SDM IPS application has been merged with SDM version 2.2. Instructions for using IPS are included in the [Cisco Router and Security Device Manager Version 2.2 User's Guide](#) and later versions of the user's guide. No SDM IPS User's Guide has been published for this release.

## SDM May Lose Connection to Network Access Device

This note concerns the NAC feature.

If the PC used to invoke SDM returns a posture state (Healthy, Infected, Checkup, Quarantine, or Unknown) and if the group policy on the ACS server attached to the posture token assigned to the PC has a redirect URL configured, the connection between SDM and the router acting as the Network Access Device (NAD) may be lost. The same problem can occur if an exception list entry attached to a policy with a redirect URL is configured with the IP address or MAC address of the PC.

If you try to reinvoke SDM from this PC, you will not be able to do so because the browser will be redirected to the location specified in the redirect URL.

There are two workarounds for this problem:

- Ensure that the PC that you use to invoke SDM attains a posture token which has an associated group policy on the ACS server that is not configured with a redirect URL.
- Alternatively, use SDM to create a NAC exception list entry with the IP address or MAC address of the PC you use to invoke SDM. Note that the exception list entry created for the PC should be associated to an exception policy which does not have a redirect URL configured in it.

For more information, see the links in the SDM NAC online help pages.

## SDM on PC May Not Launch under Windows XP with Service Pack 2

When SDM is installed on a PC running Windows XP with Service Pack 2, Internet Explorer may display HTML source code when you attempt to launch SDM. To fix this problem, go to **Tools > Internet Options > Advanced**. Then scroll to the Security section, check **Allow active content to run in files on my computer**, and click **Apply**. Then relaunch SDM.

## 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 appear when you click the help button. To prevent this from happening, you must disable the popup blocker when you run SDM. Popup blockers may be enabled in search engine toolbars, or may be standalone applications integrated with the web browser.

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

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

## Disable Proxy Settings

SDM will not start when run under Internet Explorer with proxy settings enabled. To correct this problem, choose **Internet Options** from the Tools menu, click the **Connections** tab, and then click the **LAN settings** button. In the LAN Settings window, disable the proxy settings.

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

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

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

- 
- Step 1** Connect the light blue console cable, included with the router, from the blue console port on the router to a serial port on your PC. See the router hardware installation guide for instructions.
- Step 2** Connect the power supply to the router, plug the power supply into a power outlet, and turn on the router. See the router quick start guide for instructions.
- Step 3** Use a terminal emulation program on your PC, with the terminal emulation settings 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control, to connect to the router.
- Step 4** At the prompt, enter the **enable** command, and enter the password **cisco**.
- ```
yourname> enable

Password: cisco
yourname#
```
- Step 5** Enter the **erase startup-config** command.
- ```
yourname# erase startup-config
```
- Step 6** Confirm the command by pressing **Enter**.
- Step 7** Enter the **reload** command.
- ```
yourname# reload
```
- Step 8** Confirm the command by pressing **Enter**.
- 

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

## Unable to Perform “squeeze flash:” Operation

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

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

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

- 
- Step 1** Ensure that the router will not lose power. If the router loses power after an **erase flash:** operation, there will be no Cisco IOS image in memory.
- Step 2** Prepare a TFTP server to which you can save files and copy them over to the router. You must have write access to the TFTP server. Your PC can be used for this purpose if it has a TFTP server program.
- Step 3** Open up a Telnet session on the router so that you can use the CLI.
- Step 4** Save the router’s running configuration to the startup configuration by entering the command **copy running-config startup-config**.
- Step 5** Use the **copy tftp** command to copy the Cisco IOS image, and the SDM files from flash memory to a TFTP server:

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

For example:

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

Table 4 on page 12 lists the files SDM uses.



**Tip**

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

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

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

- b. Obtain an image that supports the features you want on the Cisco 12.2(11)T release or later. Save the file to the TFTP server that is accessible from the router.
- c. Use the following link to obtain the latest SDM-Vnn.zip file.

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

- d. Extract the SDM files from SDM-Vnn.zip.
- e. Click the **setup.exe** file to start the SDM installation wizard.

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

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

- Step 7** Enter the command **erase flash:**, and confirm. The router’s IOS image, configuration file, and the SDM files are removed from flash memory.
- Step 8** Use the **copy tftp** command to copy the IOS image and the SDM files from the TFTP server to the router:
- copy tftp://tftp-server-address/filename flash:**

Example:

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




---

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

---

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

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

## Security Alert Dialog May Remain After SDM Launches

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

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

## Caveats

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

### Open Caveats—SDM 2.3.3

This section lists caveats that are open in SDM 2.3.3.

- CSCsg90956

If you use the SDM install wizard to install SDM on a router that is running Cisco IOS 12.4(12), or if the file management feature is used to place a .tar file on the router running Cisco IOS 12.4(12), the operation may fail.

Workaround:

The workaround for both problems is to manually copy the files from the PC to the router using TFTP or FTP.

- CSCek47737

If you attempt to associate an inspection rule with an interface that is part of a firewall zone, Cisco IOS returns the following error: “Cannot configure inspect rule on an interface which is member of a zone. Remove the interface from the zone and retry.”

Workaround:

If you want to associate the inspection rule with the interface, you must first remove the interface from the zone using the Cisco IOS CLI.

- CSCek38259

If the router is configured to allow SDM access through a WebVPN gateway that listens on the standard port 443, and that gateway is modified to listen on another custom port, the commands that were added for SDM access are not automatically removed, and must be removed using the Cisco IOS CLI. The WebVPN gateway may have been configured using the SDM WebVPN wizard, or it may have been configured manually and then modified to allow SDM access by adding the commands described in [SDM May not Launch Using IP Address of WebVPN Gateway](#).

Workaround:

To safely edit the the WebVPN gateway to listen to a port other than 443, do the following:

- Go to **Configure > VPN > WebVPN > Edit WebVPN**, select the gateway and click **Edit**.
- Uncheck the **Enable secure SDM access through IP address** checkbox if checked, uncheck it, and click **OK** to deliver the configuration change to the router.
- Click **Edit** again and enter the port number that you want the WebVPN gateway to use.
- Remove the loopback interface that was created for SDM access by clicking **Configure > Interfaces and Connections > Edit Interfaces/Connections** and removing the loopback interface.
- To remove the NAT rule, click **Configure > NAT > Edit NAT Configuration**, and remove the NAT rule that was added. Do not remove the NAT rule if it is being used by other parts of the configuration.

SDM can now be invoked using the standard HTTPS port 443.

If you prefer to use the Cisco IOS CLI, enter the following commands to remove the loopback interface and NAT rule that were added to allow SDM access. In these steps, Loopback 0 with an IP address of 192.168.1.1, and FastEthernet 0/0 with an IP address of 10.20.30.40 are used as examples.

```
Router# config t
Router(config)# no interface Loopback0
Router(config)# interface FastEthernet0/0
Router(config-if)# no ip nat outside
Router(config-if)# exit
Router(config)# no ip nat inside source static tcp 192.168.1.1 443 10.20.30.40 4443
Router(config)# exit
```



**Note**

Do not enter the `no ip nat inside` command if other NAT translation rules are using it. If no other rules use this command, remove it.

- CSCsd31498

Due to a Cisco IOS problem, no more than 5 actions can be assigned to a signature. This problem has no workaround.

- CSCsd28755

When you import signatures from a large Signature Definition File (SDF) more than 4 or 5 times during the same session, SDM may close. This problem has not been observed consistently. This problem has no workaround.

- CSCek33306

SDM may not launch from an interface with a CLI-configured WebVPN if the CLI commands necessary for SDM access have not been added. This includes WebVPNs configured with the command **webvpn enable WebVPNname IP-address SSLVPN**.

For more information about this caveat, see the [“SDM May not Launch Using IP Address of WebVPN Gateway” section on page 16](#).

- CSCsd33430

SDM Express browser windows do not close if the Secure Device Provisioning application is launched from SDM Express. If you choose Secure Device Provision in the SDM Express Router Provisioning screen, the SDP application is launched after you complete the SDM Express wizard and deliver the commands to the router. After the commands are delivered, SDM Express closes, but the two browser windows associated with SDM Express do not close automatically. This behavior has been observed in all browsers.

**Workaround:**

Close these windows manually. However, note that closing these windows manually also closes the SDP application. Therefore, do not close these windows until you have completed configuring the router using the SDP application.

- CSCsd63661

If you edit the IPS rule for incoming traffic or outgoing traffic or edit both rules on the interface that SDM is using to communicate with the router, the **no** form of the existing rule is delivered first. For all other interfaces the **no** form of the rule is delivered last.

**Workaround:**

No workaround is available. However, this behavior does not cause a loss of functionality.

- CSCsb33111

When signatures are reloaded using the option available in **IPS > Edit IPS > Global Settings > Reload Signatures**, and an IPS rule is applied on the interface on which SDM communicates with the router, the reload does not succeed because the commands from this interface are generated last.

This problem will occur only when IPS rule is applied on the interface on which SDM communicates to the router.

**Workaround:**

Do the following:

- Disable IPS on the connected interface
- Reload the signatures by clicking **IPS > Edit IPS > Global Settings > Reload Signatures**
- Enable IPS on the connected interface

- CSCei33081

When SDM is run on the PC, the Load File from PC function available from the File Management window may not work properly.

**Workaround:** With a TFTP server application on the PC, copy files to the router using the **copy tftp flash** command.

- CSCej01054

The SDM\_HIGH security policy may not block Instant Messaging (IM) applications. The application security feature blocks IM applications using the **server deny name** command. New servers may become available, and if they do, IM applications may connect to them.

**Workaround:** Complete the following steps:

- Turn on firewall logging for IM applications. The names of the servers that the IM applications connect to will be revealed in the log.
- Use the CLI to block the new servers. The following example uses the server *newserver.yahoo.com*:

```

router# config t
router(config)# appfw policy-name SDM_HIGH
router(cfg-appfw-policy)# application im yahoo
router(cfg-appfw-policy-ymsgr)# server deny name newserver.yahoo.com
router(cfg-appfw-policy-ymsgr)# end
router#

```

**Note**

- IM applications are able to communicate over nonnative protocol ports, such as HTTP, and through their native TCP and UDP ports. SDM configures block and permit actions based on the native port for the application, and always blocks communication conducted over HTTP ports.
- Some IM applications, such as MSN Messenger 7.0, use HTTP ports by default. To permit these applications, configure the IM application to use its native port.

- CSCei84100

When the applications security policy blocks some Point-to-Point (P2P) applications, but permits others, blocked applications may be able to download files.

**Workaround:** Instead of permitting some P2P applications and blocking others, exclude the applications that you want to permit from the application security policy by unchecking the box next to the application name.

- CSCej07924

Because of a problem with the Cisco IOS NBAR feature, some Point-to-Point applications are able to download files even when application security is configured to block them. When the Cisco IOS NBAR feature is used to block Point-to-Point applications, only those applications and protocols supported by the NBAR feature will be successfully blocked.

**Workaround:** None

- CSCsb26386

Because of a problem with Cisco IOS (CSCin92327), a connection between an Easy VPN Remote client and an Easy VPN Server may timeout before the user has time to enter the credentials.

**Workaround:** None

- CSCsb59200

Due to a JVM bug ([http://bugs.sun.com/bugdatabase/view\\_bug.do?bug\\_id=4110094](http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=4110094)) SDM IPS may crash when large Signature Definition Files (SDF) are imported. When SDM is used to import large SDFs such as virtalsensor.xml or IOS-S178.zip, SDM crashes when dismissing the Import Signature dialog. This problem does not always occur.

**Workaround:** Set the java heap size to -Xmx256m and try to import the file again. If you need to use SDM to perform a critical operation, complete that operation before reattempting to import the file.

- CSCsa40535

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

**Workaround:** Use the CLI to view DMVPN status.

- CSCef34056

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

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

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

- CSCef43267

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

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

- CSCef50389

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

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

- CSCef57546

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

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

- CSCef63313

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

**Workaround:** None.

- CSCef72022

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

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

- CSCef53222

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

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

- CSCef77689

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

**Workaround:** None.
- CSCin54600

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

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

**Workaround:** When running Firewall wizard on an interface configured with Management Access policy, choose **Merge** option instead of **Replace** and proceed.
- CSCef73879

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

**Workaround:** Ignore this message and the corresponding recommendation.
- CSCef73395

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

**Workaround:** Do the following:

  - Configure the custom protocol again.
  - Remove all the match protocol statements that reference the custom protocol that you configured.
  - Remove the custom protocol from the configuration.
- CSCef52940

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

**Workaround:** Do not configure privilege 1-level users. The problem does not occur when users of higher privilege levels are configured.
- CSCec31789

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

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

- CSCea90231

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

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

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

- CSCea89054

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

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

- CSCin44264

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

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

**Workaround:** Do one of the following:

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

For more info on VPN Modules, see the data sheet at the following link: [VPN data sheet](#).

- CSCeb01244

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

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

- CSCdy80223

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

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

- CSCin44119

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

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

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

- CSCec83817

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

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

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

- CSCin61634

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

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

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

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

- CSCed06737

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

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

- CSCec87975
 

On Cisco 7x00 routers, the SDM Update feature is supported if the current SDM files were loaded onto the router flash disk or 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 Cisco IOS image, and then invoke SDM. See [Table 2 on page 7](#) for the Cisco IOS releases that SDM supports.
- CSCed26049
 

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

**Workaround:** Upgrade your 72xx router hardware to the 4t+ PA port adapter.
- CSCed30721
 

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

**Workaround:** Use the CLI to manually remove the description \$FW\_INSIDE\$ from the unconfigured interface.
- CSCin63613
 

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

**Workaround:** Do one of the following:

  - For PPPoE connections: *Do not* provide the next hop IP address when you configure the primary backup connection.
  - For Ethernet connections without encapsulation: *Do* provide the next hop IP address when you configure the primary backup connection.
- CSCin63415
 

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

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

- CSCed18560

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

- The interface used for the primary backup connection is configured with an SDM-supported IP address type.
- The asynchronous interface is configured as the backup for a primary interface.
- The IP address of the primary interface is changed.

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

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

- CSCin48956

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

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

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

- CSCed00381

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

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

- CSCed25696

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

- CSCed08825

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

- CSCed34587

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

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

- CSCed91235

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

**Workaround:** There is no workaround for this problem.

- CSCin68829

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

**Workaround:** There is no workaround for this problem.

- CSCed92739

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

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

- CSCee67639

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

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

- CSCed13205

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

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

- CSCee71373

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

- CSCee65422

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

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

- CSCeg57729

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

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

- CSCef89472  
A download exception message may appear in the Java console when SDM is launched on a PC running Japanese Windows 2000, or Japanese Windows XP. This problem does not prevent SDM from starting or from being used.
- CSCeg40910  
The SDM installation program does not use HTTPS to back up files from the router.  
**Workaround:** No workaround exists.
- CSCeg67630  
When SDM is invoked from SDM Express, and SDM Express has been started under a nondefault browser, you must reenter router username and password before SDM will start.  
**Workaround:** Use the default browser when launching SDM Express.
- CSCeg67964  
When SDM is installed on a PC running Windows XP with Service Pack 2, Internet Explorer will display a message bar at the top of the browser window stating: "To help protect your security, Internet Explorer has restricted this file from showing active content that access your computer. Click here for options..." Clicking **Allow blocked content** does not enable SDM to launch.  
**Workaround:** In Internet Explorer, go to **Tools > Internet Options > Advanced**. Then scroll to the Security section, check **Allow active content to run in files on my computer**, and click **Apply**. Then relaunch SDM.
- CSCeg74805  
When SDM is run with certain Cisco IOS images, the number of Open Shortest Path First (OSPF) processes created can be greater than the number of interfaces in the administratively UP state. However, the running configuration does not display the value of the area configured for these additional networks. Thus, SDM is unable to display the networks for these additional OSPF processes. This problem has been reported with the following Cisco IOS images:
  - c1700-k9o3sy7-mz.123-12.8.PI6
  - c836-k9o3sy6-mz.123-11.T2.bin
  - c181x-adventerprisek9-mz**Workaround:** No workaround exists.
- CSCeh05530  
If signatures are imported using SDM IPS on a router running Cisco IOS Release 12.3(11)T3, system variables parameters are ignored by Cisco IOS.  
**Workaround:** Upgrade to a Cisco IOS image that supports SystemVariables.
- CSCeh06870  
The SDM Update from PC feature will not operate when the SDM-Vnn.zip file is placed in a shared folder with read-only access.  
**Workaround:** Do not place the SDM-Vnn.zip file in a folder with read-only access.
- CSCeg63100  
Because of a problem with Cisco IOS (CSCeg63077), VPN troubleshooting will not detect the IKE mismatch in site-to-site VPN configuration. Instead it will give a generic recommendation to apply the mirror configuration generated by SDM which would solve this problem.  
**Workaround:** Follow the recommendation displayed in the VPN troubleshooting window to apply mirror configuration on both the devices.

## Related Documentation

This section lists other documents with information on SDM.

## Platform-Specific Documents

See the quick start guide for the router, available on <http://www.cisco.com>, to learn how to set up the router hardware connections.

## Software Documents

These documents are available on <http://www.cisco.com/go/sdm>.

- *Cisco Router and Security Device Manager Q&A*. Click **Product Literature**, and then click **Q&A**.
- *Downloading and Installing Cisco Router and Security Device Manager (SDM)*. Click **Install and Upgrade** in the Technical Documentation and Tools box, and then click **Install and Upgrade Guides**.
- *Switching from Cisco Router Web Setup Tool (CRWS) to Cisco SDM on Cisco 83X Series Routers*. Click **Install and Upgrade** in the Technical Documentation and Tools box, and then click **Install and Upgrade Guides**.
- *Running Non English Editions of SDM on English-Language Operating Systems*. Click **Maintain and Operate** in the Technical Documentation and Tools box, and then click **End User Guides**.
- A number of application notes are available by clicking **Reference Guides** in the Technical Documentation and Tools box, and then clicking Technical References



### Note

For information on obtaining documentation and technical assistance, product security, and additional information, see [What's New](#), which also lists new and revised documents each month.

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 © 2003-2007 Cisco Systems, Inc. All rights reserved.