Release Notes for Cisco Router and Security Device Manager 2.5

January 21, 2008

These release notes support Cisco Router and Security Device Manager (Cisco SDM) version 2.5. 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

Cisco 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. Cisco SDM 2.1 and later versions can be installed on a PC, or in router flash, disk, or slot memory. Earlier versions of Cisco 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, Cisco SDM is either preinstalled in router memory, or is shipped on a CD with the router.

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

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 Cisco SDM system requirements.

Memory Requirements

Table 1 shows how much memory is required to support Cisco SDM and related applications.

Table 1 Cisco SDM Memory Requirements

Application	Minimum Memory Required
Cisco SDM	7.63 MB (8,008,718 bytes)
Cisco SDM Express	2.43 MB (2,550,798 bytes)
Cisco SDM installed on a PC	8.14 MB (8,545,681 bytes)
Wireless Management application	2.13 MB (2,242,560 bytes), in addition to Cisco SDM memory requirements.

Table 4 on page 12 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 Cisco SDM supports, by series.

Note Cisco SDM does not support Telco/CO router models.

Cisco SB100 series:

- Cisco SB101
- Cisco SB106
- Cisco SB107

Cisco 800 series:

- Cisco 815
- Cisco 831
- Cisco 836
- Cisco 837
- Cisco 851
- Cisco 857
- Cisco 871

- Cisco 876
- Cisco 877
- Cisco 877-M
- Cisco 877W-M
- Cisco 878

Cisco 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

Cisco SDM is supported on the following Cisco 1800 series routers:

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

Cisco SDM is supported on the following Cisco 2600 series routers:

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

Cisco SDM is supported on the following 2800 series routers:

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

Cisco SDM is supported on the following 3600 series routers:

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

Cisco SDM is supported on the following Cisco 3700 series routers:

- Cisco 3725
- Cisco 3745

Cisco SDM is supported on the following Cisco 3800 series routers:

- Cisco 3825
- Cisco 3845

Cisco SDM is supported on the following Cisco 7000 series routers:

- Cisco 7204VXR
- Cisco 7206VXR
- Cisco 7301

Supported Adapters, Cards and Network Modules

Cisco SDM supports the following 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

Cisco 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

Cisco SDM supports the following EtherSwitch Service Network Modules:

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

Cisco SDM supports the following Wide Area Application Services (WAAS) modules:

- NME-WAE-502-K9
- NME-WAE-522-K9
- NME-WAE-302-K9

Cisco SDM supports the following WAN interface cards:

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

- WIC-4ESW
- WIC-1SHDSL-V2
- WIC-1SHDSL-V3
- WIC 1ADSL-DG
- WIC 1ADSL-I-DG

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

- HWIC-4T
- HWIC-4A/S
- HWIC-8A/S-232
- HWIC-4ESW
- HWICD-9ESW
- HWIC-AP-G-X
- HWIC-AP-AG-X
- HWIC-ADSL-B/ST
- HWIC-ADSLI-B/ST
- HWIC-1ADSL
- HWIC-1ADSLI
- HWIC1-ADSL-M
- HWIC-1CABLE-D
- HWIC-1CABLE-E/J
- HWIC-1FE
- HWIC-2FE

Cisco SDM supports the following advanced integration modules (AIMs):

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

Cisco SDM supports the following port adapters on Cisco 7000 family routers:

- PA-2FE-TX
- PA-2FE-FX

- PA-8E
- PA-4E

Cisco SDM supports the following Network Processing Engines and Network Service Engines on Cisco 7000 family routers.

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

Cisco SDM supports the following service adapters on Cisco 7000 family routers:

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

Cisco SDM also supports the MOD-1700VPN.

PC System Requirements

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

Software Supported

This section describes Cisco SDM software requirements.

Cisco IOS Releases

Cisco SDM is compatible with the Cisco IOS releases listed in Table 2.

Note Cisco SDM supports the Cisco IOS Intrusion Prevention System (Cisco IOS IPS). In order to be able to use Cisco 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 Cisco SDM-Supported Routers and Cisco IOS Releases

Cisco SDM-Supported Routers	Cisco SDM-Supported Cisco IOS Releases
Cisco SB101 Cisco SB106 Cisco SB107	• 12.3(8)YG • 12.4(2)T or later releases
Cisco 815	• 12.4(6)XE1 or later releases. • 12.4(11)XJ2 or later releases. • 12.4(11)T or later releases.

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

Cisco SDM-Supported Routers	Cisco SDM-Supported Cisco IOS Releases
Cisco 831 Cisco 837	• 12.2(13)ZH or later releases • 12.3(2)XA or later releases • 12.3(2)T or later releases • 12.4(2)T or later releases
Cisco 836	• 12.2(13)ZH or later releases • 12.3(2)XA or later releases • 12.3(4)T or later releases • 12.4(2)T or later releases
Cisco 851 Cisco 857	• 12.3(8)YI • 12.4(2)T or later releases
Cisco 871 Cisco 876 Cisco 877 Cisco 878	• 12.3(8)YI • 12.4(2)T or later releases
Cisco 1701	• 12.2(13)ZH or later releases • 12.3(2)XA or later releases (Cisco SDM does not support Cisco IOS release 12.3(2)XF.) • 12.3(4)T or later releases • 12.4(2)T or later releases
Cisco 1711 Cisco 1712	• 12.2(15)ZL or later releases • 12.3(2)XA or later releases (Cisco SDM does not support Cisco IOS release 12.3(2)XF.) • 12.4(2)T or later releases
Cisco 1710 Cisco 1721 Cisco 1751 Cisco 1751-v Cisco 1760 Cisco 1760-v	• 12.2(13)ZH or later releases • 12.3(2)XA or later releases (Cisco SDM does not support Cisco IOS release 12.3(2)XF.) • 12.2(13)T3 or later releases • 12.3(2)T or later releases • 12.3(1)M or later releases • 12.2(15)ZJ3 (not available for the Cisco 1710 or Cisco 1721) • 12.4(2)T or later releases
Cisco 1801 Cisco 1802 Cisco 1803 Cisco 1811	• 12.3(8)YI • 12.4(2)T or later releases
Cisco 1812	• 12.3(8)YH or later releases • 12.4(2)T or later releases

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

Cisco SDM-Supported Routers	Cisco SDM-Supported Cisco IOS Releases
Cisco 1841	• 12.3(8)T4 or later releases • 12.4(2)T or later releases
Cisco 2610XM Cisco 2611XM Cisco 2620XM Cisco 2621XM Cisco 2650XM Cisco 2651XM Cisco 2691	• 12.2(11)T6 or later releases • 12.3(2)T or later releases • 12.3(1)M or later releases • 12.3(4)XD • 12.2(15)ZJ3 • 12.4(2)T or later releases
Cisco 2801 Cisco 2811 Cisco 2821 Cisco 2851	• 12.3(8)T4 or later releases • 12.4(2)T or later releases
Cisco 3640 Cisco 3661 Cisco 3662	• 12.2(11)T6 or later releases • 12.3(2)T or later releases • 12.3(1)M or later releases • 12.3(4)XD • 12.2(15)ZJ3 • 12.4(2)T or later releases
Cisco 3620	• 12.2(11)T6 or later releases • 12.3(1)M or later releases
Cisco 3640A	• 12.2(13)T3 or later releases • 12.3(2)T or later releases • 12.3(1)M or later releases • 12.3(4)XD • 12.2(15)ZJ3 • 12.4(2)T or later releases
Cisco 3725 Cisco 3745	• 12.2(11)T6 or later releases • 12.3(2)T or later releases • 12.3(1)M or later releases • 12.3(4)XD • 12.2(15)ZJ3 • 12.4(2)T or later releases
Cisco 3825 Cisco 3845	• 12.3(11)T or later releases • 12.4(2)T or later releases

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

Cisco SDM-Supported Routers	Cisco SDM-Supported Cisco IOS Releases
Cisco 7204VXR Cisco 7206VXR	• 12.3(2)T or later releases • 12.3(1)M or later releases • 12.4(2)T or later releases Cisco SDM does not support B, E, or S train releases on the Cisco 7000 routers.
Cisco 7301	• 12.3(2)T or later releases • 12.3(3)M or later releases • 12.4(2)T or later releases Cisco SDM does not support B, E, or S train releases on the Cisco 7000 routers.

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

Table 3 Feature History of Cisco IOS IPS

Cisco IOS Release	Cisco IOS IPS Features or Improvements
12.4(11)T2	Support for a versioned-based signature definition format used by Cisco appliance-based IPS products, and the predefined Basic and Advanced signature categories.
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

Table 3 Feature History of Cisco IOS IPS

Cisco IOS Release	Cisco IOS IPS Features or Improvements
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

Cisco 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, 7.2, and 9.0

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

- JRE 1.5_09
- JRE1.4.2_08
- JRE 1.5.0_06
- JRE 1.5.0_07
- JRE 1.6.0_02
- JRE 1.6.0_03

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

PC Operating System Versions

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

- Microsoft Windows Vista (Business Edition)
- 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.

Cisco SDM 2.5 is available only in English. Cisco SDM 2.4.1 is available in six additional languages: French, German, Italian, Japanese, Simplified Chinese, and Spanish. Cisco SDM 2.4.1 supports full Cisco SDM functionality released prior to Cisco SDM 2.5. If you want to use Cisco SDM 2.4.1 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 2.3.4 for more information.

New and Changed Information

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

New Features Supported in Cisco SDM 2.5

Cisco SDM 2.5 supports the following new features:

- The following hardware is now supported:
  - The Cisco 815 router.
  - The following 1 and 2 port high speed Ethernet WICs:
    - HWIC-1FE
    - HWIC-2FE

    Refer to the following link for more information about these cards:

    http://www.cisco.com/en/US/products/ps5853/products_data_sheet0900aecd80581fe6.html
  - The following cable modem network adapters:
    - HWIC-1CABLE-D
    - HWIC-1CABLE-E/J
  - The following Wide Area Application Services (WAAS) modules.
    - NME-WAE-502-K9
    - NME-WAE-522-K9
    - NME-WAE-302-K9
- Quality of Service (QoS) over Dynamic Virtual Tunnel Interfaces (DVTI) Support—Cisco SDM enables you to associate QoS policies with DVTIs.
- QoS Policing, Queuing , and Shaping Support—Cisco SDM allows you to configure policing, queuing, and shaping in QoS policies.

  - For more information on QoS policing, refer to http://www.cisco.com/en/US/tech/tk543/tk545/tsd_technology_support_protocol_home.html
  - For more information on QoS queuing, refer to http://www.cisco.com/en/US/tech/tk543/tk544/tsd_technology_support_protocol_home.html
  - For more information on QoS shaping, refer to http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a008022136e.html

- Easy VPN Enhancements— Cisco SDM supports the following Easy VPN enhancements:

  Per-user Authentication, Authorization and Accounting (AAA) policy download with Public Key Infrastructure (PKI). For more information on per-user AAA policy download with PKI, refer to the following link: http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455b6a.html

  - Password aging—The Easy VPN server configured on the router can notify a user that their passwords is expiring and prompt them to change it.
  - Split DNS—Split DNS enables Cisco routers to answer DNS queries using the internal hostname cache specified by a selected virtual DNS name server.
  - Cisco Tunneling Control Protocol (cTCP)—cTCP is a protocol that encapsulates Encapsulating Security Payload (ESP) and Internet Key Exchange (IKE) traffic in the TCP header, so that firewalls in between the client and the server or headend device permit this traffic, considering it as TCP traffic.

    For more information on password aging, split DNS, and cTCP, refer to the following link: http://www.cisco.com/en/US/products/ps6441/prod_bulletin09186a00804a84ad.html
  - Identical Addressing Support—Identical Addressing provides the ability to reach devices having identical IP addresses over an EasyVPN connection through the use of Network Address Translation.

    For more information about Identical Addressing Support, refer to http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801541d5.html#wp1335885
  - Syslog Message Enhancements—Easy VPN syslog messages can be globally enabled on the Easy VPN server. Syslog messages can be enabled for all Easy VPN client connections or for client connections belonging to specific groups.

- Zone-Based Policy Firewall (ZPF) Voice Protocol Support—Cisco SDM supports theSession Initiation Protocol (SIP), H.323 protocol, and Skinny Client Control Protocol (SCCP) protocol.
- ZPF user interface enhancements.
- Wireless Application Enhancements—Cisco SDM supports the following enhancements:
  - Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP)
  - IEEE 802.1x Local Authentication Service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST).
  - Service Set Identifier (SSID) Globalization
  - Multiple Basic Service Set IDs (BSSID).
  - Wireless Root, Non-Root Bridge & Universal Client Mode
  - Multiple Encrypted VLANs

  - VLAN assignment by name
  - Wi-Fi Multimedia (WMM) elements.
- Cisco IOS Intrusion Prevention System (IPS) user interface enhancements—The following enhancements are now supported:
  - Total compiled signatures are now displayed in the Signatures screen.
  - The SDM and CLI signature packages can now be downloaded in one operation.
  - Downloaded signature packages are automatically pushed to the router.
- Secure Socket Layer VPN (SSL VPN) enhancements—Cisco SDM now supports:
  - URL Obfuscation
  - Automatic download of the Thin Client applet
  - Radius Accounting
  - Application ACL

Cisco SDM Files

This section describes the files used in Cisco SDM 2.5. Table 4 lists the name, size, and description of each file.

Table 4 Cisco SDM File List

Filename	Size	Description
common.tar	1.43 MB (1,505,280 bytes)	Cisco SDM and Cisco SDM Express support file
es.tar	910 KB (931,840 bytes)	Cisco SDM Express application file
home.shtml	1.01 KB (1,038 bytes)	Cisco SDM and Cisco SDM Express support file
home.tar	110 KB	Cisco SDM and Cisco SDM Express support file
sdmconfig-modelnum.cfg For example: sdmconfig-180x.cfg	2.68 to 3.20 KB (2,746 to 3,278 bytes)	*Default configuration file*
sdm.tar	6.09 MB (6,389,760 bytes)	Cisco SDM application file
sdmips.sdf	Variable	File created when Cisco SDM is used to modify Cisco IOS IPS signatures.
securedesktop-ios-3.1.1.45-k9.pkg	1.61 MB (1,697, 952 bytes)	Cisco Secure Desktop client software for SSL VPN clients.
sslclient-win-1.1.4.176.pkg	406 KB (415,956 bytes)	Full tunnel client software for SSL VPN clients
wlanui.tar	2.13 MB (2, 242, 560 bytes)	Wireless Application

Table 4 Cisco SDM File List (continued)

Filename	Size	Description
128MB.sdf	515 KB (527, 849 bytes)	Signature Definition File (SDF) used by Cisco IOS IPS
256MB.sdf	775 KB (793, 739 bytes	Signature Definition File (SDF) used by Cisco IOS IPS

Installation Notes

This section contains important information regarding installation and upgrades to Cisco SDM 2.5.

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

If you are installing Cisco SDM 2.5 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 Cisco SDM 2.5. Cisco 1700 routers using Cisco IOS Release 12.2(13)T cannot have more than 32 files in flash memory.

Before installing Cisco SDM 2.5, you must delete any unneeded files from flash memory. If no files can be deleted, do not install it on the router.

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

If Cisco SDM 2.5 is not currently installed on the router, see *Downloading and Installing Cisco Router and Security Device Manager* to learn how to download Cisco 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

In the Support box, click **Install and Upgrade**. Then click **Install and Upgrade Guides > Downloading and Installing Cisco Router and Security Device Manager**.

Upgrading to a New Cisco SDM Version

If a version of Cisco SDM later than version 1.0 is already installed on the router, use the Cisco SDM automatic update feature to install the latest files on the router. Cisco SDM automatically checks Cisco.com for more recent versions of Cisco SDM, downloads them to your PC, removes the old Cisco 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 Cisco SDM 1.0, you must download the file SDM-V*nn*.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

In the Support box, click **Install and Upgrade**. Then click **Install and Upgrade Guides > Downloading and Installing Cisco Router and Security Device Manager**.

Uninstalling Cisco SDM Files

If you want to remove Cisco 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 Cisco 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 Cisco 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 Cisco SDM files. The "Cisco SDM Files" section on page 12 lists the files used.

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.

Cisco SDM version 2.1 or later can be installed on your PC. To remove Cisco 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 Cisco SDM.

Cisco SDM Minimum Screen Resolution

Cisco 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 Cisco SDM running on Cisco 7204VXR, Cisco 7206VXR, and Cisco 7301 Routers:

- The Cisco 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. Cisco SDM supports configuration of Ethernet and Fast Ethernet interfaces.
- The Cisco SDM Reset feature is not available.
- No SDM-default configuration file is supplied. To run Cisco SDM, you must provide a configuration that includes the commands necessary to support operation of Cisco SDM.

The document Cisco Router and Security Device Manager (SDM) User Guide for the Cisco 7200 VXR and Cisco 7301 Routers describes how to give the router a configuration that supports Cisco SDM and how to start Cisco SDM on Cisco 7000 Family routers.

ROUTER-SDM-NOCF and ROUTER-SDM-CD-NOCF SKUS

If you purchased a router with Cisco SDM using the SKU ROUTER-SDM-NOCF or the SKU ROUTER-SDM-CD-NOCF, the router is shipped without a default configuration in non-volatile RAM (NVRAM), and the *Cisco Router and Security Device Manager Quick Start Guide* cannot be used to configure the router.

Important Notes

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

Cisco IOS Enforces One-Time Use of Default Credentials

To address CSCsm25466, Cisco IOS images included with recent shipments of Cisco 800, Cisco 1800, Cisco 2800, and Cisco 3800 routers, enforce the one-time use of the default username and password provided in the Cisco SDM configuration file. If you bypass Cisco SDM or Cisco SDM Express and use a console or Telnet connection to log into the router, the login and exec banners warn you that you must change the username "cisco" and password "cisco" before you log off of the router. If you do not change the credentials as directed, you will not be able to log on to the router the next time that you attempt to do so.

The following Cisco IOS releases enforce the one-time use of the default credentials:

- 12.4(11)T or later
- 12.4(11)SW, 12.4(11)SW1, 12.4(11)XV, 12.4(11)XJ
- 12.4(9)T5, 12.4(9)T6
- 12.3(21), 12.3(22)

Follow the procedure in this section to secure the router by creating a new username and password, to remove the login banner and exec banner warnings, and to save the configuration changes to the router startup configuration.

Note If you login to the router using a Telnet or a console connection but do not complete the steps in this procedure, be aware of the following:

- If you do not change the default username and password, and then log off the router, you will not be able to log into the router again without entering the **reload** command. No additional warning is given before you log off.
- If you do not change the default username and password, but do enter the **write memory** command before ending the session, future logins will be disabled. In this case, you will need to follow the password recovery procedure at the following link:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml

To secure the router, remove the banner warnings and save the changes to the router startup config, complete the following steps:

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

Step 4 When prompted, enter the username **cisco**, and password **cisco**.

Step 5 Enter configuration mode by entering the following command:

```
yourname# configure terminal
```

Step 6 Create a new username and password by entering the following command:

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

Replace *username* and *password* with the username and password that you want to use.

Step 7 Remove the default username and password by entering the following command:

```
yourname(config)# no username cisco
```

Step 8 To remove the login banner, enter the following command:

```
yourname(config)# no banner login
```

The login banner warning will no longer appear.

Step 9 To remove the exec banner, enter the following command:

```
yourname(config)# no banner exec
```

The exec banner warning will no longer appear.

Step 10 Leave configuration mode, by entering the following command:

```
yourname(config)# end
```

Step 11 Copy the configuration changes to the startup configuration by entering the following command:

```
yourname# copy running-config startup-config
```

When logging into the router in the future, use the username and password that you created in Step 6.

Cisco SDM May Not Operate with Custom Configuration File

If you load a custom configuration file on the router using Cisco Configuration Express or any other process, you may remove Command Line Interface (CLI) commands that Cisco SDM operation requires amd prevent it from operating. Cisco SDM requires the following basic configuration in order to connect to the router and manage it.

- An http or https server must be enabled with local authentication.
- A local user account with privilege level 15 and accompanying password must be configured.
- Vty line with protocol ssh/telnet must be enabled with local authentication. This is needed for interactive commands.
- An http timeout policy must be configured with the parameters shown in the following example to avoid a known launch issue with SDM.
- The PC on which SDM is to run and the interface through which SDM will be launched must be configured with IP addresses from the same subnet.

The following example shows a configuration that contains the CLI commands Cisco SDM requires in order to operate.

```
hostname yourname
!
logging buffered 51200 warnings
!
username cisco privilege 15 secret 0 cisco
```

```
!
ip domain-name yourdomain.com
!
interface FastEthernet0
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-10/100 Ethernet$
ip address 10.10.10.1 255.255.255.248
description PC must be on the same subnet as this interface
no shutdown
!
ip http server
ip http secure-server
ip http authentication local
ip http timeout-policy idle 60 life 86400 requests 10000
!
line vty 0 4
privilege level 15
login local
transport input telnet
transport input telnet ssh
line vty 5 15
privilege level 15
login local
transport input telnet
transport input telnet ssh
```

Cisco SDM Merge and Replace Configuration Functions Fail Under Some Conditions

The problem described here is caveat CSCsj21989. If you attempt to merge configuration changes made using the Cisco SDM Config Editor feature, or replace the running configuration with a configuration from the Config Editor, the router configuration will not be changed if there is a network device with a Network Address Translation (NAT) IP address, or a cache engine in the connection between the PC and the router. If you need to make changes to the router configuration that you would normally make using the Cisco SDM Config Editor, use the Cisco IOS CLI instead.

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 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.

Cisco SDM May not Launch Using IP Address of SSL VPN Gateway

This information provides more information about the caveat CSCek33306. When Cisco SDM attempts to connect to a router with a SSL VPN 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 Cisco SDM access are not included.

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

To be able to launch Cisco 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 SSLVPN 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 MySSLVPN
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 Cisco SDM by entering the following IP address and port in the browser:

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

If you remove the SSL VPN gateway that was modified for Cisco 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.

Cisco SDM IPS User Guide Discontinued for Cisco SDM 2.2

The Cisco SDM IPS application has been merged with Cisco SDM 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 Cisco SDM IPS User's Guide has been published for this release.

Cisco SDM May Lose Connection to Network Access Device

This note concerns the NAC feature.

If the PC used to invoke Cisco 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 Cisco 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 Cisco 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 Cisco 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 Cisco SDM to create a NAC exception list entry with the IP address or MAC address of the PC you use to invoke Cisco 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 Cisco SDM NAC online help pages.

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

When Cisco 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 Cisco 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 Cisco SDM.

Popup Blockers Disable Cisco SDM Online Help

If you have enabled popup blockers in the browser you use to run Cisco 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 Cisco 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 third-party pop up blockers, go to **Tools >Internet Options > Privacy**, and uncheck the **Block popups** checkbox.

In Firefox 1.5 and later versions, click **Tools > Options > Content**. Uncheck **Block pop-up windows**.

Disable Proxy Settings

Cisco 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 Cisco SDM Do Not Execute the Standard Cisco IOS Startup Sequence

Because a default configuration file is provided on a router shipped with Cisco 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 Cisco 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 Cisco SDM. Please see the router quick start guide and to the SDM FAQ for information about the minimum configuration required for using Cisco SDM. This document is available at:

http://www.cisco.com/go/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 Cisco SDM to change an existing configuration, see the instructions on starting Cisco 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 Cisco SDM. If this becomes necessary, Cisco SDM informs 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 Cisco 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 Cisco 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 Cisco 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 Cisco SDM uses.

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

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

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

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

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

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

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

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

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

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

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

Step 8 Use the **copy tftp** command to copy the IOS image and the Cisco 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 Cisco SDM files.

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

When Cisco 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 Cisco 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—Cisco SDM 2.5

This section lists caveats that are open in Cisco SDM 2.5.

- CSCsk51555

  This caveat is caused by Cisco IOS caveat CSCsl42697. When configuring a radio interface using the Cisco SDM Wireless application, QoS access commands such as max-contention and min-contention window settings are not delivered to the router.

- CSCsk88931

  This caveat is caused by Cisco IOS caveat CSCsl39285. Registration with the WAAS Central Manager from the WAAS NM tab fails when the username, password, and primary interface are entered and the user clicks OK.

- CSCsk78581

  When Cisco SDM is invoked using HTTPS on a router running Cisco IOS version 12.4(17), the router crashes.

  Workaround:

  Invoke Cisco SDM using HTTP, as in the following example:

  ```
  http://10.10.10.1
  ```

- CSCsl47234

  When a AAA network authorization policy is being added, the delivery of IOS CLI commands to the router fails if the if-authenticated method is selected along with other methods,

- CSCsl00095

  Due to a Cisco IOS 12.4(15)T1 issue, when an Easy VPN Server is configured with the split DNS option, and an Easy VPN remote client is configured on another router, the details screen on the remote client does not display split DNS details for the Easy VPN server.

- CSCsl13151

  When Cisco SDM is run under Microsoft Vista, and the -Xmx256m heap size statement is present in the Java runtime settings, Cisco SDM closes when you enter Cisco IOS IPS credentials. This problem has been found in the following operating environment: Microsoft Vista, Netscape 7.1 and Internet Explorer 7.0, and the Java Runtime Environments 1.5.0_06, 1.5.0_07, and 1.5.0_13.

  Workaround:

  Use the following procedure to remove the -Xmx256m heap size statement:

  1. Exit Cisco SDM.
  2. Click **Start > Control Panel > Java**.
  3. Open the Java Runtime Settings dialog. The location of this dialog varies by release.
  4. Click the **Advanced** tab. Locate the Java Runtime Settings dialog and proceed to 6.. If the dialog is not available from the Advanced tab, proceed to 5.

5. Click the **Java** tab. Locate the Java Runtime Settings dialog. Click the **View** button if necessary to display the dialog, and proceed to 6.
6. In the Java Runtime Parameters column, remove the value `-Xmx256m` from the Java runtime parameters column. If this statement is found in other rows, remove the statement from those rows as well.
7. Click **OK** in the Java Runtime Settings dialog.
8. Click **Apply** in the Java Control Panel, and then click **OK**.
9. Restart Cisco SDM.

- CSCsl32119

  When Cisco SDM is used to configure Cisco IOS IPS on a Cisco 7301 router, Cisco SDM may take as much as 10 minutes to launch and correctly display Cisco IOS IPS signatures. If Cisco SDM launches without delay, Cisco IOS IPS signatures are not displayed correctly, and errors can be seen when the Edit Signatures window is displayed. When the Cisco SDM display is refreshed in these circumstances it may take up to 10 minutes for the signatures to be displayed correctly,

  This problem has been found on 7301 routers running Cisco IOS 12.4(11)T3, when Cisco SDM is run under Internet Explorer 6.0 using Java Runtime Environment 1.6.0_03.

- CSCsk98378

  Due to a Cisco IOS problem described in CSCsk67302, the output of the show running-config command will not show SSL VPN gateways associated with SSL VPN contexts. This problem has been found in Cisco IOS 12.4(15)T and 12.4(15)T1 images

- CSCsj21989

  For a description of this caveat, see Cisco SDM Merge and Replace Configuration Functions Fail Under Some Conditions.

- CSCsi34046

  The java console displays an exception when a rule is created by going to **Edit Firewall Policy** > **Add a Rule**, and creating a rule that specifies application inspection for any Instant Messaging (IM) or Peer-to-Peer (P2P) protocol. This occurs when traffic is first specified, followed by the IM or P2P service and then the application inspection parameters.

  Workaround: Go to **Edit Firewall Policy** > **Add a Rule**, and create the IM or P2P rule but do not specify traffic information. In the Edit Firewall Policy window, choose the rule you created, click **Edit**, add the traffic information, and click **OK**.

- CSCsg61829

  When Cisco SDM is invoked using Firefox 2.0 is closed and then Firefox is relaunched, a pop-up saying that the browser was not closed properly appears and asks if the user wants to restore the previous session or start a new session. Clicking **Restore Session** opens the previously established SDM session without asking for any credentials.

  Workaround: Instead of choosing to restore the old session, click **Start new session** to start a fresh browser session.

- CSCsh11991

  Because of a Cisco IOS IPS problem, when migrating a Cisco IOS IPS configuration created using a Cisco IOS image older than version 12.4(11)T to a 12.4(11)T or later environment, user-modified signatures are not migrated.

  Workaround: After migrating, use the Add or Edit controls in the Edit IPS window to create the signature in the new format.

- CSCsh31616

  Because of Cisco IOS caveat CSCsh32935, when reordering class maps in the Edit Inspection Policy Map dialog, the Cisco SDM-defined class map sdm-protocol-p2p may be removed if it was included in the policy map being edited.

- CSCsh39685

  Because of Cisco IOS caveat CSCek68311, a Certificate Authority (CA) server created using the Cisco SDM CA Server wizard will be shown as stopped. This problem occurs when the router is running a Cisco IOS 12.4(11)T image.

  Workaround: Upgrade the Cisco IOS image on the router to version 12.4(11)T2.

- CSCsh41150

  When the router is running a Cisco IOS image older than 12.4(11)T the Easy VPN Server Status screen in Monitoring mode displays the IP address of a client configured with a Dynamic Virtual Template Interface (DVTI) as 0.0.0.0.

- CSCsh46525

  You may be unable to delete a DVTI-based Easy VPN Remote configuration using Cisco SDM.

  Workaround: Click **Refresh** in the Cisco SDM toolbar and then delete the configuration.

- CSCsh57750

  When starting Cisco SDM under Firefox 2.0, online help, IDS, and the Wireless Application open as a tab in the Cisco SDM splash screen. This problem occurs because the default setting for Firefox is to open a new page as a tab.

  Workaround: Do the following.

  - Launch Firefox 2.0.
  - From the Tools menu, choose **Options**.
  - Click **Tabs**.
  - In the Open links from other applications box, choose **a new window** option and click OK.

- CSCsh62598

  When the QoS wizard is used to give a WAN interface QoS configuration with the NBAR option, the configuration is not completely delivered to the router because some of the match protocols are not present in Cisco IOS.

- CSCsh96364

  Multiple instances of Cisco SDM in the Firefox 2.0 browser can cause exceptions to be displayed in the Java console.

  Workaround: Start only a single instance of SDM in the Firefox browser.

- CSCsi03518

  When a firewall is configured using Cisco SDM, and then Cisco SDM is used to create an SSL VPN configuration on the router, a NAT passthrough configuration is added by the SSL VPN wizard. No NAT passthrough configuration is added when creating an SSL VPN configuration using the SSL VPN edit windows.

- CSCsi23696

  Because of Cisco IOS caveat CSCsi23729, when Cisco SDM is used to restore the defaults to a signature on a router running Cisco IOS 12.4(11)T2, signatures that were previously displayed no longer appear in the signature list.

Workaround: This may be addressed in a future release of Cisco IOS.

- CSCsh44720

  When Cisco SDM installed on a PC is invoked in Internet Explorer 7.0 using either HTTP or HTTPS, the popup window asking for the IP address of the router appears again after the IP address has been entered in the first popup window.

  When Cisco SDM installed on router flash memory nvoked in Internet Explorer 7.0 using HTTPS, a certification error is displayed. Cisco SDM starts if you choose **Continue to this website (not recommended)**.

- CSCsg53496

  Because of Cisco IOS caveat CSCsg63809, SSID configuration values entered in the Wireless Security > Bridging/Routing window are not delivered to the router.

  Workaround: This may be addressed in a future release of Cisco IOS.

- CSCsg36618

  The Cisco SDM Wireless Application does not work on modular routers using wireless network adaptors running Cisco IOS release 12.4(9)T1.

- CSCsg90956

  If you use the Cisco SDM install wizard to install Cisco 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.

- CSCek38259

  If the router is configured to allow Cisco SDM access through a SSL VPN 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 Cisco SDM access are not automatically removed, and must be removed using the Cisco IOS CLI. The SSL VPN gateway may have been configured using the SSL VPN wizard, or it may have been configured manually and then modified to allow Cisco SDM access by adding the commands described in Cisco SDM May not Launch Using IP Address of SSL VPN Gateway.

  Workaround:

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

  - Go to **Configure > VPN > SSLVPN > Edit SSL VPN**, select the gateway and click **Edit**.
  - Uncheck the **Enable secure SDM access through** *IP address* checkbox is 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 SSL VPN gateway to use.
  - Remove the loopback interface that was created for Cisco 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.

    Cisco 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 Cisco 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.

- CSCsd28755

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

- CSCek33306

  Cisco SDM may not launch from an interface with a CLI-configured SSL VPN if the CLI commands necessary for Cisco SDM access have not been added. This includes SSL VPNs configured with the command **webvpn enable** *SSLVPNname IP-address* **SSLVPN**.

  For more information about this caveat, see the "Cisco SDM May not Launch Using IP Address of SSL VPN Gateway" section on page 17.

- CSCsd33430

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

- CSCei33081

  When Cisco 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. Cisco 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 Peer-to-Peer (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 Peer-to-Peer 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 Peer-to-Peer 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) Cisco SDM IPS may crash when large Signature Definition Files (SDF) are imported. When Cisco SDM is used to import large SDFs such as virtualsensor.xml or IOS-S178.zip, Cisco 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 Cisco 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 Cisco 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 Cisco SDM, then all other open instances of Cisco 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 Cisco SDM is shut down, Netscape shuts down the JVM or the Java plug-in, and all other instances of Cisco SDM are also shut down.

  Workaround: If Cisco SDM is run under Netscape version 7.1, open only one instance of Cisco SDM. Using Internet Explorer is advised when multiple instances of Cisco 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 Cisco 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 Cisco SDM with a user associated with a different CLI view, or with a user of privilege level 15.

- CSCef53222

  Cisco SDM filenames are case sensitive. If the Cisco SDM files are copied from the PC hard disk to a flash card, File Explorer changes the names to uppercase. When this happens, Cisco 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 Cisco 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 Cisco SDM, if any of the uploaded 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 Cisco SDM.

- CSCea90231

  Router does not reload with default configuration when a' user executes a Reset To Factory Defaults operation in Cisco 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. Cisco SDM indicates that it has sent a **reload** command to the router and shuts down, and the default configuration is copied to the startup-config, but the **reload** command has not executed, and the router is still using the running configuration that was present before the Reset To Factory Defaults operation.

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

- CSCea89054

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

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

- CSCin44264

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

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

  Workaround: Do one of the following:

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

    For more info on VPN Modules, see the data sheet at the following link: VPN data sheet.

- CSCdy80223

  When Cisco 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 Cisco 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 Cisco 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. Cisco 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 Cisco 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

  Cisco 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 Cisco 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 Cisco SDM on routers running Cisco IOS Release 12.3(4)T. When the user attempts to do an Xauth authentication in Cisco 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 Cisco 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 Cisco 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 Cisco SDM Update feature is supported if the current Cisco SDM files were loaded onto the router flash disk or Compact Flash disk. However, the Cisco SDM Update feature fails to upload new files to the router if the current Cisco SDM files were installed in flash

memory. The Cisco SDM Update feature uses RCP protocol to upload the new Cisco 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 Cisco SDM files were loaded into flash memory, update to the new Cisco SDM version by manually copying the new Cisco SDM files to the file system of the router using a TFTP server. To make use of the automatic Cisco SDM Update feature, always install Cisco SDM files on the flash disk or Compact Flash disks (disk0, disk1, disk2).

- CSCed31085

  Cisco 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 Cisco SDM-supported Cisco IOS image, and then invoke Cisco SDM. See Table 2 on page 7 for the Cisco IOS releases that Cisco 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, Cisco 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, Cisco 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, Cisco SDM may report that the interface contains unsupported configuration parameters.

  Workaround: Click Refresh on the Cisco 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 Cisco 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, Cisco SDM displays a Yes or No warning popup asking if you want to remove the backup configuration. If you choose **Yes**, Cisco 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 Cisco SDM is being used on a router with interfaces that Cisco SDM does not support, such as Token Ring or VLAN interfaces. Cisco 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 Cisco 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 Cisco SDM Express and the router. When Cisco SDM Express is invoked using the string https://*router-IP-address*, it uses SSH.

  Workaround: When launching Cisco SDM Express, click Cancel in the SSH credentials window. Cisco 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, Cisco 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 Cisco SDM is using the SSH or Telnet communications module.

- CSCed08825

  Cisco 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 Cisco 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 Cisco SDM is started using HTTPS.

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

- CSCee67639

  The Cisco 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

  Cisco 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 Cisco 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 Cisco 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), Cisco 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 Cisco SDM to configure a virtual auxiliary port.

- CSCeg57729

  When Cisco 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 Cisco SDM.

- CSCef89472

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

- CSCeg40910

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

- CSCeg67630

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

  Workaround: Use the default browser when launching Cisco SDM Express.

- CSCeg67964

  When Cisco 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 Cisco 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 Cisco SDM.

- CSCeg74805

  When Cisco 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, Cisco 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

- CSCeh05530

  If signatures are imported using Cisco 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 Cisco SDM Update from PC feature will not operate when the SDM-V*nn*.zip file is placed in a shared folder with read-only access.

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

- CSCeg63100

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