Data Sheet

Cisco Security Device Manager

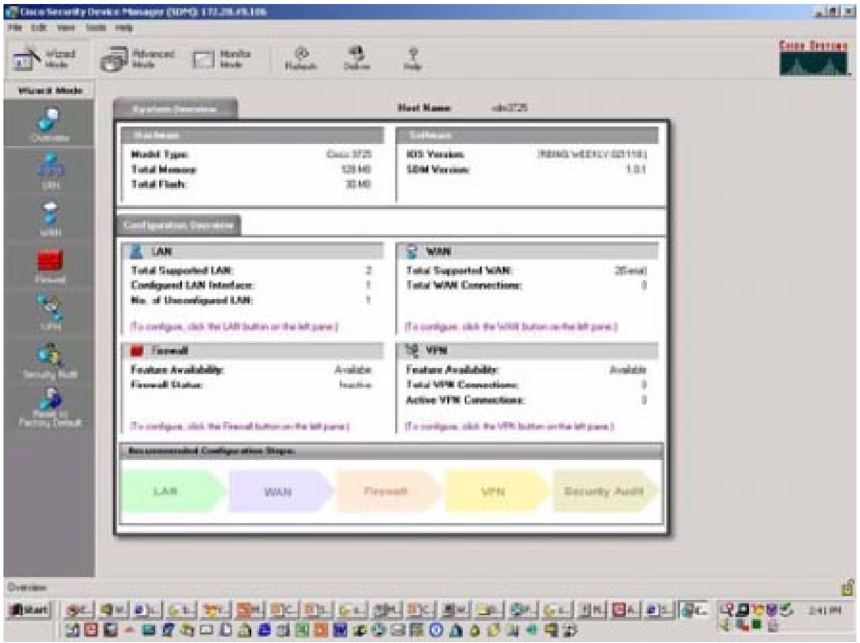
The Cisco® Security Device Manager (SDM) is an intuitive, Web-based device management tool embedded within Cisco IOS® access routers. Cisco SDM simplifies router and security configuration through intelligent wizards, enabling customers to quickly and easily deploy, configure, and monitor a Cisco access router without requiring knowledge of the Cisco IOS Software command-line interface (CLI).

Flexibility and Ease of Use

Cisco SDM allows users to easily configure Cisco IOS Software security features on Cisco access routers on a device-by-device basis, while enabling proactive management through performance monitoring. Whether deploying a new router or installing Cisco SDM on an existing router, users can now remotely configure and monitor Cisco 830, 1700, 2600xm, 3600, and 3700 series routers without using the Cisco IOS Software command-line interface (CLI).

The Cisco IOS Software CLI is an effective means of router configuration but requires a high level of proficiency and expertise. The Cisco SDM GUI aids nonexpert users of Cisco IOS Software in their day-to-day operations, providing easy-to-use intelligent wizards, automated router security management, and comprehensive online help and tutorials (Figure 1).

Figure 1 Cisco SDM Graphical User Interface



Host Name: sdm3725

Hardware

Model Type: Cisco 3725
Total Memory: 128 MB
Total Flash: 32 MB

Software

IOS Version: [illegible]
SDM Version: 1.0.1

LAN

Total Supported LAN: 2
Configured LAN Interface: 1
No. of Unconfigured LAN: 1

(To configure, click the LAN button on the left pane.)

WAN

Total Supported WAN: 2(Serial)
Total WAN Connections: 0

(To configure, click the WAN button on the left pane.)

Firewall

Feature Availability: Available
Firewall Status: Inactive

(To configure, click the Firewall button on the left pane.)

VPN

Feature Availability: Available
Total VPN Connections: 0
Active VPN Connections: 0

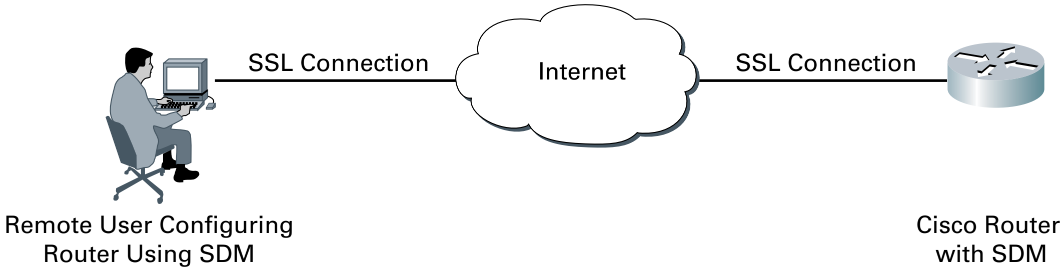
(To configure, click the VPN button on the left pane.)

Cisco SDM wizards guide users step-by-step through router configuration and security configuration workflow by systematically configuring LAN and WAN interfaces, firewalls, and VPNs. Cisco SDM wizards can intelligently detect incorrect configurations and propose fixes, such as allowing Dynamic Host Control Protocol (DHCP) traffic through a firewall if the WAN interface is DHCP addressed. Online help embedded within Cisco SDM contains appropriate background information, in addition to step-by-step procedures to help users enter correct data in Cisco SDM application windows. Networking and security terms and definitions that users might encounter are included in an online glossary.

For network professionals familiar with Cisco IOS Software and its security features, Cisco SDM offers an advanced mode to quickly configure and fine-tune router security features, allowing network professionals to review the commands generated by Cisco SDM before delivering the configuration changes to the router. Advanced users can also quickly fine-tune configurations using features such as the access control list (ACL) editor.

Cisco SDM enables all types of users to configure and monitor routers from remote locations using Secure Sockets Layer (SSL) connections (Figure 2). This technology enables a secure connection, over the Internet, between the user's browser and the router. When deployed at a branch office, a Cisco SDM-enabled router can be configured and monitored from corporate headquarters, reducing the need for IT support at the branch.

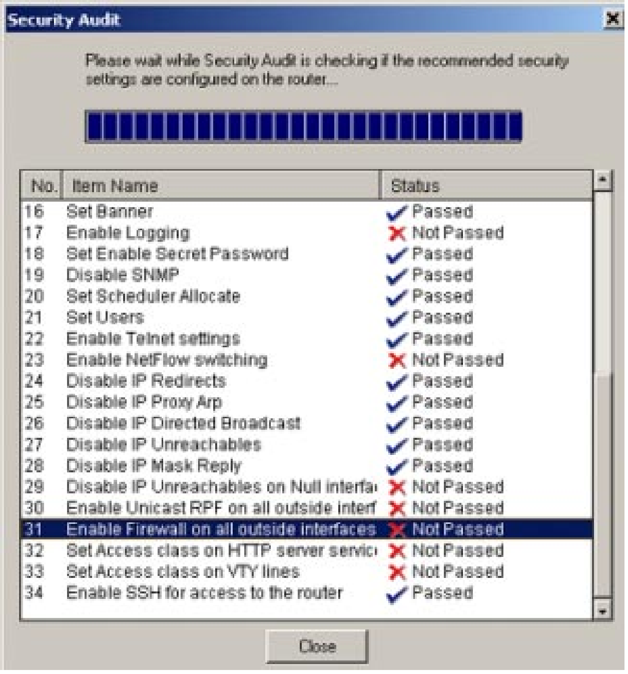
Figure 2 Connecting to a Cisco SDM-Enabled Router Using SSL for Secure Remote Connectivity



Security Configuration

When deploying a new router, Cisco SDM can be used to quickly configure Cisco IOS Firewall using best practices recommended by the International Computer Security Association (ICSA) and the Cisco Technical Assistance Center (TAC). Cisco SDM users can configure the strongest VPN defaults, and automatically performs security audits (Figure 3). In addition, Cisco SDM users can perform one-step router lockdown for firewalls and one-step VPN for quick deployment of secure site-to-site connections.

Figure 3 Router Security Audit



Please wait while Security Audit is checking if the recommended security settings are configured on the router...

No.	Item Name	Status
16	Set Banner	✓ Passed
17	Enable Logging	✗ Not Passed
18	Set Enable Secret Password	✓ Passed
19	Disable SNMP	✓ Passed
20	Set Scheduler Allocate	✓ Passed
21	Set Users	✓ Passed
22	Enable Telnet settings	✓ Passed
23	Enable NetFlow switching	✗ Not Passed
24	Disable IP Redirects	✓ Passed
25	Disable IP Proxy Arp	✓ Passed
26	Disable IP Directed Broadcast	✓ Passed
27	Disable IP Unreachables	✓ Passed
28	Disable IP Mask Reply	✓ Passed
29	Disable IP Unreachables on Null interfa	✗ Not Passed
30	Enable Unicast RPF on all outside interf	✗ Not Passed
31	Enable Firewall on all outside interfaces	✗ Not Passed
32	Set Access class on HTTP server servic	✗ Not Passed
33	Set Access class on VTY lines	✗ Not Passed
34	Enable SSH for access to the router	✓ Passed

When installed on an existing router, Cisco SDM allows users to perform one-step security audits to evaluate the strengths and weaknesses of their router configurations against common security vulnerabilities. Using the advanced mode, administrators can fine-tune their existing security configurations to better suit their business needs. Cisco SDM can also be used for ongoing monitoring, fault management, and troubleshooting.

Router Configuration

In addition to security configuration, Cisco SDM enables users to quickly and easily perform basic router configuration, such as LAN and WAN interface configuration. Using the LAN configuration wizard, users can assign IP addresses and subnet masks to Ethernet interfaces, and can enable or disable DHCP server.

Using the WAN configuration wizard, T1/E1, Ethernet, and xDSL interfaces can be assigned static or dynamic IP address as well as subnet masks. Additionally, for serial connections, Frame Relay, Point-to-Point Protocol (PPP), and High-Level Data Link Control (HDLC) encapsulation can be implemented. Using Cisco SDM, authentication can be configured for PPP connections, and for Frame Relay connections, Local Management Interface (LMI) and data-link connection identifier (DLCI) parameters can be entered. Cisco SDM also allows configuration of common routing protocols like OSPF, RIP, and EIGRP.

Monitoring

In “monitor” mode, Cisco SDM provides an overview of router status and performance metrics such as the Cisco IOS Software release, interface status (up or down), and CPU and memory usage. Monitor mode also allows users to view the number of network access attempts that were denied by Cisco IOS Firewall, and provides easy access to the firewall log. Additionally, VPN status, such as the number of active IP Security (IPSec) tunnels, can be monitored. Interfaces, firewall, VPN, and logging status and performance may also be monitored independently, and with greater detail.

Cost Savings

Cisco SDM is ideal for enterprise branch offices and small and medium-sized businesses that are sensitive to network management costs. Cisco SDM allows businesses to implement router security configurations on a device-by-device basis and in a timely manner—without purchasing new network management software. For businesses with larger networks, Cisco SDM enables easy deployment of individual routers—by nonexpert administrators—at branch offices. These devices can then be managed from corporate headquarters through central management tools, providing cost savings in terms of time and IT support expenses at the branch office.

Cisco SDM and Other Cisco Management Applications

Cisco offers additional device management and network management applications that can be used in conjunction with Cisco SDM. CiscoView, a Web-based management application, can be installed on a dedicated CiscoWorks server to display and monitor the physical view of Cisco devices. Cisco SDM and CiscoView client interfaces can coexist on the same workstation—Cisco SDM can be used primarily for router and security feature configuration, while CiscoView can be used for real-time display of the physical router status and for Simple Network Management Protocol (SNMP) based device monitoring. Cisco QoS Device Manager (QDM), a Web-based quality of service (QoS) management application, and Cisco SDM can also coexist on the router, where Cisco QDM is used primarily to configure QoS-related Cisco IOS Software configurations on the router.

Cisco IP Solution Center (ISC) and CiscoWorks VPN/Security Management Solution (VMS) both offer highly scalable security management solutions for Cisco IOS routers. Cisco ISC can cost-effectively scale to 10,000 or more devices. Cisco SDM complements these centralized management solutions by aiding in the deployment of LAN, WAN, and security features on a router through intelligent wizards that can detect and correct any security configuration mismatches at the device level.

For Cisco 830 series routers, either the Cisco Router Web Setup (CRWS) tool or Cisco SDM can be used for configuration. CRWS is ideally suited for deploying multiple Cisco 830 series routers with the same configuration. Cisco SDM should be used when various site-specific configurations are required.

Table 1 lists the features and benefits of Cisco SDM.

Table 1 Features and Benefits of Cisco SDM

Feature	Benefit
Embedded Web-based management tool	• Turns the router into a complete solution with its own management tool • Does not require a separate management station • Allows remote management from any supported desktop or laptop
SSL-based secure remote access	• Secure management across the WAN
At-a-glance router status views	• Provides a quick inventory of router hardware, software, and security configurations

Table 1 Features and Benefits of Cisco SDM (Continued)

Feature	Benefit
Router security audit	• Assesses existing network infrastructure against common security vulnerabilities • Provides quick compliance to expert (TAC, ICSA) recommended security policies for routers
One-step router lockdown	• Simplifies firewall configuration without requiring expertise on security or Cisco IOS Software
Wizards to assist users in quick configuration of Cisco IOS Software security features like firewall, VPN, and Network Address Translation (NAT)	• Reduces training needs for network administrators on new Cisco IOS Software security features • Easily and cost-effectively secures the existing network infrastructure
Startup wizard	• Reduces Cisco router deployment time and complexity
Advanced configuration mode	• Allows security experts to fine-tune security policies based on site-specific requirements
Preview Cisco IOS Software CLI commands	• Helps build Cisco IOS Software expertise
ACL management (editor)	• Advanced users can easily and quickly manage ACLs
Monitoring and logging	• Helps troubleshoot security-related issues and manage router performance before it affects mission-critical applications in the network
Integrated online help and tutorials	• Reduces the need for IT staff to keep up with security technology updates and complex security configurations

Table 2 lists specifications of Cisco SDM.

Table 2 Cisco SDM Specifications

Specifications	Cisco SDM
Supported platforms	• Cisco 831, 836, and 837 • Cisco 1710, 1721, 1751, and 1760 • Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and 2691 • Cisco 3620, 3640, 3661, and 3662 • Cisco 3725 and 3745
Required Cisco IOS Software	• Cisco IOS Software Release 12.2(11)T6 or later (Refer to the SDM FAQ for additional details)
Memory requirements	• Cisco SDM requires at least 2.3 MB of free Flash memory on the router
Operating system requirements	• Windows 2000 • Windows NT 4.0 (Service Pack 4) • Windows 98 • Windows ME • Windows XP

Table 2 Cisco SDM Specifications (Continued)

Specifications	Cisco SDM
Browser requirements	• Microsoft Internet Explorer 5.5 or later • Netscape Navigator 4.79
Java requirements	• The client device must have a browser that supports JDK 1.1.4 as supported in the Internet Explorer and Netscape browsers • Java plug-in, JRE2 version 1.3.1 or later
Recommended connection speed	• 56 Kbps or greater
Basic router configuration parameters	• IP • Passwords • Users • Domain Name System (DNS) • DHCP • SNMP • Telnet
Advanced router configuration parameters	• Routing protocols: Static, Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Enhanced Interior Gateway Routing Protocol (EIGRP) • NAT • ACLs
Configurable WAN interfaces	• Ethernet • xDSL • T1/E1
Supported WAN encapsulations	• Frame Relay • PPP • PPP over Ethernet (PPPoE) • RFC 1483 routing • HDLC
Configurable VPN parameters	• Internet Key Exchange (IKE) • IPSec • Easy VPN Remote • Generic routing encapsulation (GRE) tunnel
Supported firewall parameters	• Context-Based Access Control (CBAC)
CiscoView compatibility	• Can be used with Cisco SDM
Cisco QDM compatibility	• Can be used with Cisco SDM
License	• No license fee required
Availability	• Factory installed on all Cisco 1700 2600xm, 3600, and 3700 VPN bundles • Optional factory installation available on all supported Cisco router models • Posted on www.Cisco.com Software Center for free download

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe