



## Data Sheet

# Cisco Router and Security Device Manager

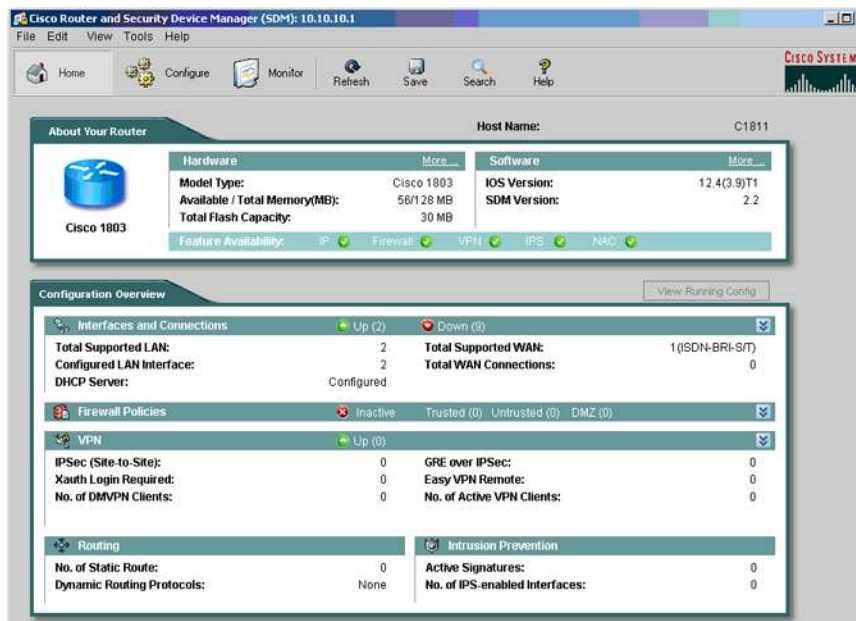
This data sheet provides an overview of features, benefits, and product availability of the Cisco® Router and Security Device Manager (SDM).

The Cisco SDM is an intuitive, Web-based device-management tool for Cisco IOS® Software-based routers. The Cisco SDM simplifies router and security configuration through smart wizards, which help customers and Cisco partners quickly and easily deploy, configure, and monitor a Cisco Systems® router without requiring knowledge of the command-line interface (CLI). The Cisco SDM is supported on a wide range of Cisco routers and Cisco IOS Software releases. Refer to Table 3 for specific model numbers supported by the Cisco SDM.

## EASE OF USE AND BUILT-IN APPLICATION INTELLIGENCE

The Cisco SDM allows users to easily configure routing, switching, security, and quality-of-service (QoS) services on Cisco routers while enabling proactive management through performance monitoring (Figure 1). Cisco SDM users can now remotely configure and monitor their Cisco routers without using the Cisco IOS Software CLI. The Cisco SDM GUI aids nonexpert users of Cisco IOS Software in their day-to-day operations, provides easy-to-use smart wizards, automates router security management, and assists users through comprehensive online help and tutorials.

Figure 1. Cisco SDM Homepage



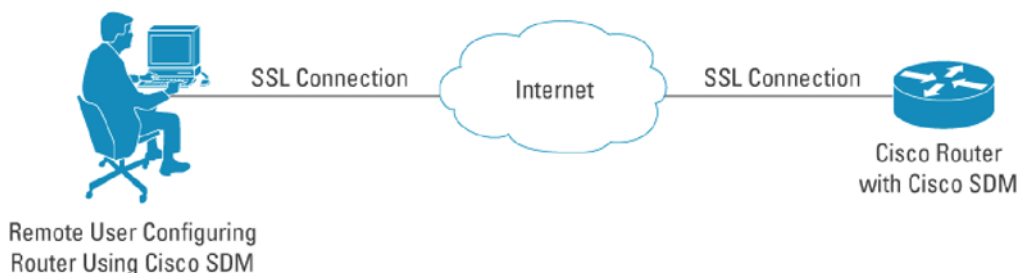
Cisco SDM smart wizards guide users step by step through router and security configuration workflow by systematically configuring LAN, WLAN, and WAN interfaces; firewalls; intrusion prevention systems (IPS); and IP Security (IPSec) VPNs. Cisco SDM smart wizards can intelligently detect incorrect configurations and propose fixes, such as allowing Dynamic Host Configuration Protocol (DHCP) traffic through a firewall if the WAN interface is DHCP-addressed. Online help embedded within the Cisco SDM contains appropriate background information, in addition to step-by-step

procedures to help users enter correct data in the Cisco SDM. 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, the Cisco SDM offers advanced configuration tools to quickly configure and fine-tune router security features, allowing network professionals to review the commands generated by the Cisco SDM before delivering the configuration changes to the router.

The Cisco SDM helps administrators configure and monitor routers from remote locations using Secure Sockets Layer (SSL) and Secure Shell (SSHv2) Protocol connections (Figure 2). This technology helps enable 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 experienced network administrators at the branch office.

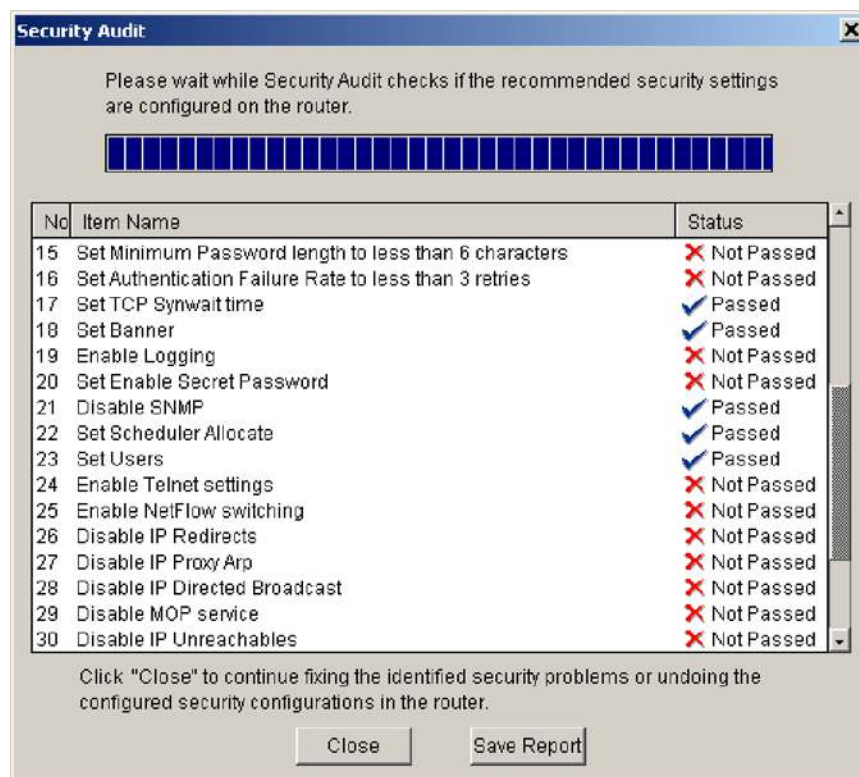
**Figure 2.** Connecting to a Cisco SDM-Enabled Router Using SSL for Secure Remote Connectivity



## INTEGRATED SECURITY CONFIGURATION

When deploying a new router, Cisco SDM can be used to configure a Cisco IOS Software firewall quickly using best practices recommended by the International Computer Security Association (ICSA) and the Cisco Technical Assistance Center (TAC). An advanced firewall wizard allows a single-step deployment of high, medium, or low application firewall policy settings. Cisco SDM users can configure the strongest VPN defaults and automatically perform 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. A recommended list of IPS signatures bundled with Cisco SDM allows quick deployment of worm, virus, and protocol exploit mitigation. The Cisco SDM Network Admission Control (NAC) wizard enables simple and fast integration of NAC and client security posture management into an existing network infrastructure.

**Figure 3.** Router Security Audit



When invoked on an already-configured 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. Administrators can fine-tune their existing router security configurations to better suit their business needs. The Cisco SDM also can be used for day-to-day operations such as monitoring, fault management, and troubleshooting.

## ROUTER CONFIGURATION

In addition to security configuration, Cisco SDM helps users quickly and easily perform router services configuration, such as LAN, WLAN, and WAN interface configuration; dynamic routing; DHCP server; QoS policy; and so on.

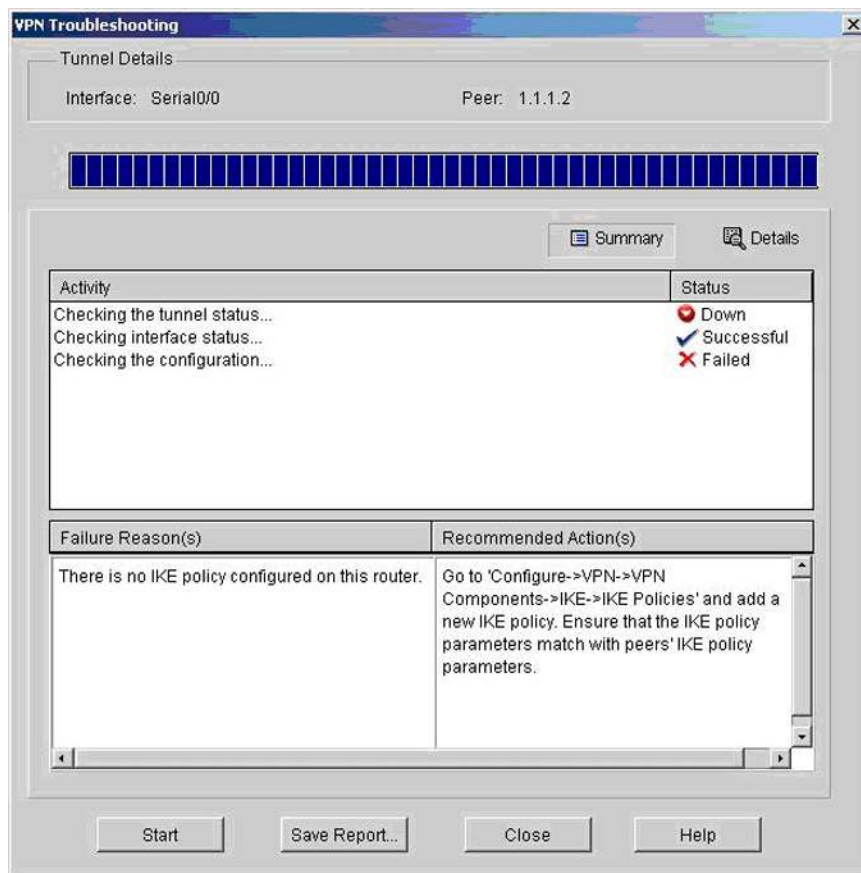
Using the LAN configuration wizard, users can assign IP addresses and subnet masks to Ethernet interfaces and can enable or disable the DHCP server. Using the WAN configuration wizard, users can configure xDSL, T1/E1, Ethernet, and ISDN interfaces for WAN and Internet access. Additionally, for serial connections, users can implement Frame Relay, Point-to-Point Protocol (PPP), and High-Level Data Link Control (HDLC) encapsulation. Cisco SDM also allows configuration of static routing and common dynamic routing protocols such as Open Shortest Path First (OSPF), Routing Information Protocol (RIP) Version 2, and Enhanced Interior Gateway Routing Protocol (EIGRP).

QoS policies can now easily be applied to any WAN or VPN tunnel interface using Cisco SDM. The QoS policy wizard automates the Cisco architecture guidelines for QoS Policies to effectively prioritize the traffic between real-time applications (voice or video), business-critical applications (Structured Query Language [SQL], Oracle, Citrix, routing protocols, etc), and the rest of network traffic (Web, e-mail, etc.). Network-based application recognition (NBAR)-based monitoring in the Cisco SDM allows users to visually inspect the application layer traffic in real time and confirms the effect of QoS policies on different classes of application traffic.

## MONITORING AND TROUBLESHOOTING

In monitor mode, Cisco SDM provides a quick, graphical status of important router resources and performance measurements such as the interface status (up or down), CPU, and memory usage (see Figure 4). For wireless models Cisco SDM provides comprehensive support for real-time 802.11 a/b/g interface statistics. Cisco SDM takes advantage of integrated routing and security features on routers to provide in-depth diagnostics and troubleshooting of WAN and VPN connections. For example, while troubleshooting a failed VPN connection, the Cisco SDM verifies the router configurations and connectivity from the WAN interface layer to the IPSec Crypto Map layer. While testing configuration and remote-peer connectivity at each layer, Cisco SDM provides pass or fail status, possible reasons of failure, and Cisco TAC–recommended actions for recovery.

**Figure 4.** VPN Troubleshooting and Recovery



Cisco SDM monitor mode also allows users to view the number of network access attempts that were denied by the Cisco IOS Software firewall, and it provides easy access to the firewall log. Users also can monitor detailed VPN status, such as the number of packets encrypted or decrypted by IPSec tunnels, and Easy VPN client session details.

**Table 1.** Cisco SDMv2.2 Features

Feature	Benefit
<b>New Hardware Support</b>	
<ul style="list-style-type: none"><li>• EtherSwitch service modules: NME-16ES-1G-P, NME-X-23ES-1G-1P, NME-XD-24ES-1S-P, NME-XD-48ES-2S-P</li><li>• USB Flash keys and USB eTokens (Aladdin's eToken)</li><li>• ADSL 2/2+ and ISDN HWICs</li><li>• NM-1FE-FX-V2 and NM-1FE2W-V2</li></ul>	<ul style="list-style-type: none"><li>• Automatically recognizes, configures, and monitors the new hardware</li><li>• USB flash filesystem management, digital certificate storage, and secure credentials with USB tokens</li><li>• VLAN trunking and Ethernet sub-interface configuration support</li></ul>
<b>Cisco Incident Control Services (ICS)</b>	
<ul style="list-style-type: none"><li>• Support Trend Micro signatures</li></ul>	<ul style="list-style-type: none"><li>• Rapid deployment and customization of signatures for day-zero protection against new attacks</li></ul>
<b>Network Admission Control (NAC)</b>	
<ul style="list-style-type: none"><li>• Configuration wizard and client security posture management on routers</li></ul>	<ul style="list-style-type: none"><li>• Simple and fast integration of NAC into existing network infrastructure</li></ul>
<b>Application Firewall</b>	
<ul style="list-style-type: none"><li>• Advanced firewall wizards, policy views, inspection rule editors, and log views</li><li>• Peer-to-peer (P2P) applications: BitTorrent, Kazaa, Gnutella, eDonkey</li><li>• Instant Messaging: Yahoo, MSN, AOL</li><li>• Protocol conformance: HTTP and e-mail (Simple Mail Transfer Protocol [SMTP], ESMTP, POP3, and Internet Message Access Protocol [IMAP])</li></ul>	<ul style="list-style-type: none"><li>• Delivers application-level control and unified threat management for accelerated security solutions deployment</li><li>• Protocol anomaly detection services</li><li>• High, medium, and low security levels for firewall policy settings to enable accelerated and easy deployment<ul style="list-style-type: none"><li>– Low—for business environments that do not need to track P2P and IM applications on the network or check for protocol conformance</li><li>– Medium—for business environments where security is important and need to track the use of IM and P2P applications and check for HTTP and Email protocol conformance</li><li>– High—for business environments where security is critical; need protocol anomaly detection services to drop non conformant HTTP and email traffic and prevent use of P2P and IM applications</li></ul></li></ul>
<b>Granular Protocol Inspection</b>	
<ul style="list-style-type: none"><li>• User-customizable application to port (or port range) mapping over TCP and UDP ports</li></ul>	<ul style="list-style-type: none"><li>• Menu of applications for easy and granular protocol selection in policies</li></ul>
<b>Threat-Based Intrusion Protection</b>	
<ul style="list-style-type: none"><li>• Threat-based signature categories to ease IPS deployments</li><li>• IPS configuration wizards, event viewer</li></ul>	<ul style="list-style-type: none"><li>• Easier and more intelligent signature selection based on available resources and attack categories (Viruses/Worms/Trojans, DoS/DDos etc.)</li><li>• Real-time reporting of signature engine status</li></ul>
<b>Easy VPN Server and Remote Enhancements</b>	
<ul style="list-style-type: none"><li>• Advanced wizards, remote configuration update, Web intercept, dial backup, and QoS support</li></ul>	<ul style="list-style-type: none"><li>• Scalable, easy-to-manage, secure remote access for teleworkers or small offices on hub routers or branch office access routers</li></ul>

Feature	Benefit
<b>Dynamic DNS</b>	
<ul style="list-style-type: none"> <li>• HTTP-based and IETF-based updates</li> <li>• Integration with existing WAN interface configuration wizard</li> </ul>	<ul style="list-style-type: none"> <li>• Scalable, remote management of dynamically addressed routers</li> <li>• Run business services without dedicated and expensive static IP addresses</li> </ul>
<b>Usability Improvements</b>	<ul style="list-style-type: none"> <li>• Real time viewer for Security Device Event Exchange (SDEE) alarms from IPS signature engines</li> <li>• Layer 3 and above firewall policy templates</li> <li>• Application firewall alarm log</li> <li>• Network Address Translation (NAT) wizards to simplify IP address management</li> <li>• Search toolbar for Cisco SDM UI pages, features, and wizards</li> </ul>

## COST SAVINGS

Cisco SDM is ideal for enterprise branch offices and small and medium-sized businesses that are sensitive to device deployment and network management costs and have limited access to skilled technicians. Cisco SDM allows businesses and Cisco channel partners to implement router security and network configurations easily and confidently. Cisco IOS Software configurations generated by Cisco SDM are approved by the Cisco TAC. Cisco SDM enhances the productivity of network and security administrators through built-in configuration checks, configuration editor for experts, and meaningful defaults. Cisco SDM features provide an additional advantage of improved network availability through reduced instances of configuration errors.

For businesses with larger networks, Cisco SDM helps enable easy and highly scalable deployment of routers through integration with the Cisco CNS Configuration Engine. Cisco IOS Software configuration generated by Cisco SDM can be imported into the Cisco CNS Configuration Engine to be deployed across thousands of Cisco routers in a cookie-cutter fashion.

## MANAGED CPE SERVICES

Cisco SDM provides a highly cost-effective solution for service providers to offer a read-only, graphical view of Cisco router services (firewall, IPSec VPNs, intrusion prevention, WAN access, QoS, etc.). This allows for faster provisioning of value-added customer-premises-equipment (CPE) services without requiring investment in complex operations-support-system (OSS) software to provide end-customer views.

Additionally, this solution provides the service provider end customers a local tool they can use to quickly troubleshoot any CPE-related issues, thus reducing the support burden on the network help desk.

Cisco resellers can take advantage of Cisco SDM to offer value-added security, traffic shaping, or managed CPE services to the installed base of Cisco access routers or to new Cisco router customers.

## CISCO SDM AND OTHER CISCO MANAGEMENT APPLICATIONS

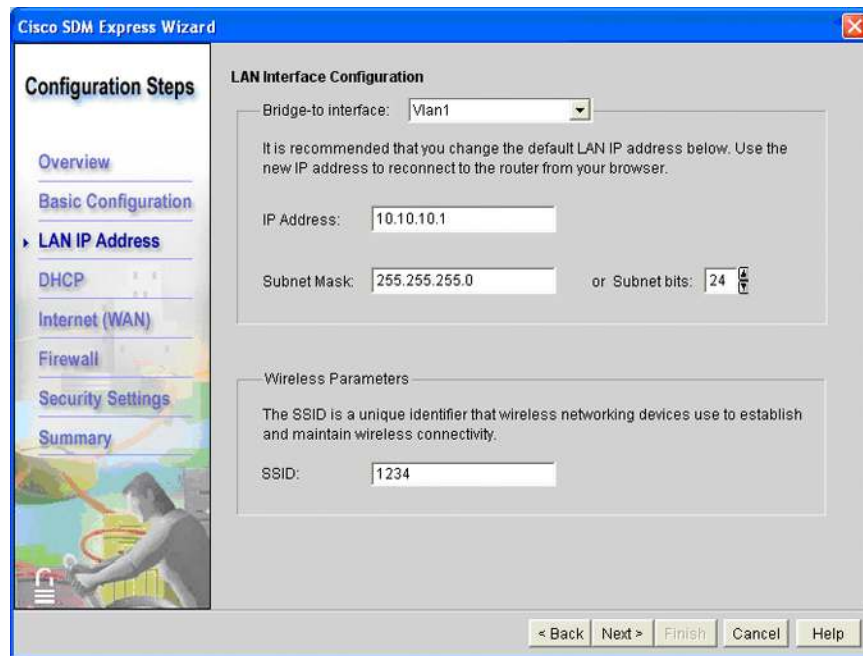
Cisco offers additional device and network management applications that can be used in conjunction with Cisco SDM. CiscoView, a Web-based management application, can be installed on a dedicated CiscoWorks server to display and monitor the physical view of Cisco devices. Cisco SDM and CiscoView client interfaces can coexist on the same workstation: Cisco SDM can be used primarily for router and security feature configuration, and CiscoView can be used for real-time display of the physical router status and for Simple Network Management Protocol (SNMP)-based device monitoring.

## APPLICATIONS

### Cisco Router Initial Deployment

Cisco SDM helps Cisco partners and customers deploy Cisco routers quickly and securely using the Cisco SDM Express (Figure 5) and several other task-based smart wizards. The one-step router lockdown feature helps ensure that all nonessential services in Cisco IOS Software are shut off before the Cisco router is connected to the public Internet or a WAN.

**Figure 5.** Cisco SDM Express



### Cisco Router Mass Deployments

Cisco SDM is integrated with the Cisco CNS 2100 Series Intelligence Engine to help enable fast and cost-effective mass deployments of Cisco routers with factory default configurations. Service providers and large enterprises have the flexibility to use the Cisco SDM and Cisco CNS 2100 Series combination during staging or allow an untrained, onsite administrator to download the final Cisco IOS Software configuration without using the Cisco IOS Software CLI.

### Cisco Router Security Management

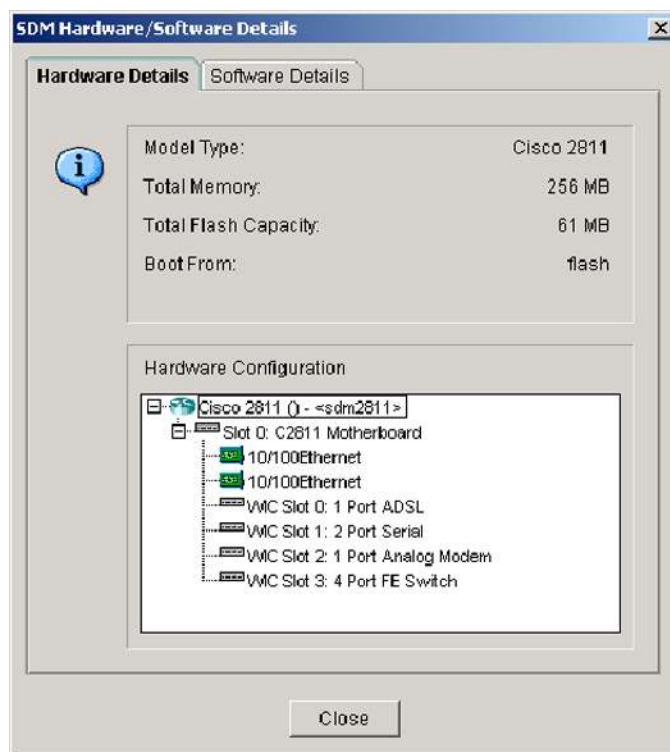
Cisco SDM helps Cisco partners and customers easily deploy Cisco IOS Software security features—NAT, access control lists (ACLs), firewalls, IPS, and IPSec VPNs—and integrate these security features into existing router configuration and network architectures. Smart wizards in the Cisco SDM understand the interaction of routing and security features and guide the user to a final configuration that is approved and tested by the Cisco TAC from end to end. The CLI preview mode in the Cisco SDM allows expert users to manually validate the final configuration before it is delivered to the router.

### Cisco Router Operational Management

Cisco SDM helps Cisco partners and customers securely (using SSL and SSH) and remotely manage all critical aspects of router operations: hardware and software inventory status, interface status, firewall and ACL logs, VPN tunnel status, and most recent syslog messages.



**Figure 6.** Cisco Router Hardware and Software Inventory



## CONCLUSION

The Cisco SDM is a valuable productivity-enhancing tool for network and security administrators. Cisco partners can use the Cisco SDM for faster and easier deployment of Cisco routers for both WAN access and network security features.

Cisco customers can use the Cisco SDM for reducing the total cost of ownership of their Cisco routers by relying on Cisco SDM-generated configurations that are tested end to end by Cisco engineers and approved by the Cisco TAC. Configuration checks built into Cisco SDM reduce the instances of configuration errors.

## PRODUCT SPECIFICATIONS

Table 2 shows primary features and benefits of the Cisco SDM. Table 3 shows product specifications for the Cisco SDM.

**Table 2.** Cisco SDM Primary Features and Benefits

Feature	Benefit
<b>Embedded Web-based Management Tool</b>	<ul style="list-style-type: none"> <li>• Turns the router into a complete security and remote-access solution with its own management tool</li> <li>• Does not require a dedicated management station</li> <li>• Allows remote management from any supported desktop or laptop</li> </ul>
<b>SSL- and SSHv2-Based Secure Remote Access</b>	<ul style="list-style-type: none"> <li>• Provides for secure management across the WAN</li> </ul>
<b>At-a-Glance Router Status Views</b>	<ul style="list-style-type: none"> <li>• Offers quick graphical summary of router hardware, software, and primary router services such as VPN, firewall, QoS, etc.</li> </ul>



Feature	Benefit
<b>Router Security Audit</b>	<ul style="list-style-type: none"> <li>Assesses vulnerability of existing router</li> <li>Provides quick compliance to best-practices (Cisco TAC, ICSA recommendations) security policies for routers</li> </ul>
<b>One-Step Router Lockdown</b>	<ul style="list-style-type: none"> <li>Simplifies firewall and Cisco IOS Software configuration without requiring expertise about security or Cisco IOS Software</li> </ul>
<b>Smart Wizards for Most Frequent Router and Security Configuration Tasks</b>	<ul style="list-style-type: none"> <li>Generates Cisco TAC–approved configurations</li> <li>Averts misconfigurations with integrated routing and security knowledge</li> <li>Reduces network administrators' training needs for new Cisco IOS Software security features</li> <li>Secures the existing network infrastructure easily and cost-effectively</li> </ul>
<b>Policy-Based Firewall and ACL Management (Firewall Policy)</b>	<ul style="list-style-type: none"> <li>Allows security administrators to easily and quickly manage ACLs and packet-inspection rules through a graphical and intuitive policy table</li> </ul>
<b>IPS</b>	<ul style="list-style-type: none"> <li>Allows easy and quick provisioning of Cisco tuned and recommended high-fidelity attack signatures on any router interface for inbound and outbound traffic</li> <li>Allows dynamic update of new IPS signatures without impacting basic router operations</li> <li>Allows graphical customization of IPS signatures for immediate response to new worm or virus variants</li> <li>Allows filtering of signatures and mass configuration changes (action or severity) for the selected signatures</li> <li>Shows real-time status and error messages from IPS engine</li> </ul>
<b>Cisco Easy VPN Server</b>	<ul style="list-style-type: none"> <li>Offers wizard-based configuration and real-time monitoring of remote-access VPN users</li> <li>Provides integration with on-router or remote authentication, authorization, and accounting (AAA) server</li> </ul>
<b>Role-Based Access</b>	<ul style="list-style-type: none"> <li>Offers logical separation of router between different router administrators and users</li> <li>Provides for secure access to Cisco SDM user interface and Telnet interface specific to each administrator's profile</li> <li>Helps enable Cisco value-added resellers and service providers to offer a graphical, read-only view of the CPE services to end customers</li> <li>Offers factory-default profiles: <ul style="list-style-type: none"> <li>Administrator</li> <li>Firewall administrator</li> <li>Easy VPN client user</li> <li>Read-only user</li> </ul> </li> </ul>
<b>WAN and VPN Troubleshooting</b>	<ul style="list-style-type: none"> <li>Reduces mean time to repair (MTTR) by taking advantage of the integration of routing, LAN, WAN, and security features on the router for detailed troubleshooting</li> <li>Takes advantage of integration of routing, LAN, WAN, and security features on the router for detailed troubleshooting of IPSec VPNs or WAN links</li> <li>Integrates Layer 2 and above troubleshooting with Cisco TAC knowledge base of recovery actions</li> </ul>
<b>QoS Policy</b>	<ul style="list-style-type: none"> <li>Easily and effectively optimizes WAN and VPN bandwidth and application performance for different business needs (voice and video, enterprise applications, Web, etc.)</li> <li>Three predefined categories: real time, business critical, and best effort</li> </ul>
<b>NBAR</b>	<ul style="list-style-type: none"> <li>Provides real-time validation of application usage of WAN and VPN bandwidth against predefined service policies</li> <li>Provides for traffic performance monitoring</li> </ul>
<b>SSHv2</b>	<ul style="list-style-type: none"> <li>Provides for secure management between PC and Cisco router</li> <li>Automatically uses SSHv2 for all encrypted communication between Cisco SDM and router</li> </ul>

Feature	Benefit
<b>Real-Time Monitoring and Logging</b>	<ul style="list-style-type: none"> <li>Allows administrators to proactively manage router resources and security before they affect mission-critical applications on the network</li> </ul>
<b>Digital Certificates</b>	<ul style="list-style-type: none"> <li>Offers highly scalable and more secure solution than preshared keys</li> <li>Now easy to use and deploy with the combination of Cisco SDM, Cisco IOS Certificate Authority Server, and Easy Secure Device Deployment (EzSDD)</li> </ul>
<b>Real-Time Network and Router Resource Monitoring</b>	<ul style="list-style-type: none"> <li>Offers faster and easier analysis of router resource and network resource usage</li> <li>Offers graphical charts for LAN and WAN traffic and bandwidth usage</li> </ul>
<b>Task-Based Cisco SDM User Interface</b>	<ul style="list-style-type: none"> <li>Provides for faster and easier configuration of security configurations—IPSec VPNs, firewall, ACLs, IPS, etc.</li> <li>Offers quick snapshot of router services configuration through dashboard view on the homepage</li> </ul>
<b>Cisco SDM Express Wizard-Based Deployment of Router</b>	<ul style="list-style-type: none"> <li>Offers quick and easy router deployment for basic WAN access configurations</li> <li>Ideal router deployment tool for non-expert users</li> </ul>
<b>PC-Based SDM Cisco SDM Installed on Windows-based PC Instead of Router Flash Memory</b>	<ul style="list-style-type: none"> <li>No extra Flash memory space required on router for Cisco SDM</li> <li>Great tool to manage the installed base of Cisco routers</li> </ul>
<b>Localized in Six Languages</b>	<ul style="list-style-type: none"> <li>Simplifies router management for national language users</li> <li>Cisco SDM user interface and online help translated in Japanese, Simplified Chinese, French, German, Spanish, and Italian (available from Sep 2005)</li> <li>MS Windows OS support for these languages (available now)</li> </ul>
<b>Integrated Wireless Management</b>	<ul style="list-style-type: none"> <li>Express Setup wizard simplifies the first-time setup of wireless interface</li> <li>Advanced Web-based configuration and monitoring available</li> <li>Reduces time and skill set required to bring-up wireless interfaces</li> <li>Flexibility to customize wireless configuration and security based on site-specific needs</li> </ul>
<b>IPS Provisioning Improvement</b>	<ul style="list-style-type: none"> <li>Allows rapid deployment of IPS signatures specific to router model</li> </ul>

**Table 3.** Product Specifications for Cisco SDM (Minimum Cisco IOS Software Release Supported)

<b>Supported Platforms</b>	<ul style="list-style-type: none"> <li>• Cisco Small Business 101, Cisco Small Business 106, Cisco Small Business 107: <ul style="list-style-type: none"> <li>– Cisco IOS Software Release 12.3(8)YG</li> </ul> </li> <li>• Cisco 831 Ethernet Broadband Router, Cisco 836 ADSL over ISDN Broadband Router, and Cisco 837 ADSL Broadband Router: <ul style="list-style-type: none"> <li>– Cisco IOS Software Release 12.2(13)ZH or 12.3(2)T</li> </ul> </li> <li>• Cisco 851, 856, 871, 876, 877, and 878 integrated services routers: <ul style="list-style-type: none"> <li>– Cisco IOS Software Release 12.3(8)YI</li> </ul> </li> <li>• Cisco 1701 ADSL Security Access Router; Cisco 1710, 1711, and 1712 security access routers; and Cisco 1721, 1751, 1751-V, 1760, and 1760-V modular access routers: <ul style="list-style-type: none"> <li>– Cisco IOS Software Release 12.2(13)ZH, 12.2(13)T3, or 12.3(1)M</li> </ul> </li> <li>• Cisco 1801, 1802, 1803, 1811, and 1812 integrated services routers: <ul style="list-style-type: none"> <li>– Cisco IOS Software Release 12.3(8)YI</li> </ul> </li> <li>• Cisco 1841 Integrated Services Router: <ul style="list-style-type: none"> <li>– Cisco IOS Software Release 12.3(8)T4</li> </ul> </li> <li>• Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, and 2651XM and Cisco 2691 multiservice platforms: <ul style="list-style-type: none"> <li>– Cisco IOS Software Release 12.2(15)ZJ3, 12.2(11)T6, or 12.3(1)M</li> </ul> </li> <li>• Cisco 2801, 2811, 2821, and 2851 integrated services routers: <ul style="list-style-type: none"> <li>– Cisco IOS Software Release 12.3(8)T4</li> </ul> </li> <li>• Cisco 3725 and 3745 multiservice access routers: <ul style="list-style-type: none"> <li>– Cisco IOS Software Release 12.2(15)ZJ3, 12.2(11)T6, or 12.3(1)M</li> </ul> </li> <li>• Cisco 3825 and 3845 integrated services routers: <ul style="list-style-type: none"> <li>– Cisco IOS Software Release 12.3(11)T</li> </ul> </li> <li>• Cisco 7204VXR, 7206VXR, and 7301 routers: <ul style="list-style-type: none"> <li>– Cisco IOS Software Release 12.3(2)T or 12.3(3)M; no support for B, E, and S trains</li> </ul> </li> </ul>
<b>Software Compatibility</b>	<ul style="list-style-type: none"> <li>• Compatible with all Cisco IOS Software feature sets for the previously mentioned Cisco SDM-supported releases of Cisco IOS Software</li> </ul>
<b>Connectivity</b>	<ul style="list-style-type: none"> <li>• HTTP and HTTPS; Telnet, SSH, and SSHv2</li> </ul>
<b>Basic Router Configuration Parameters</b>	<ul style="list-style-type: none"> <li>• Users with different access profiles</li> <li>• Domain Name System (DNS)</li> <li>• DHCP server and client</li> <li>• SNMP</li> <li>• Telnet, SSH, SSHv2, and vty</li> <li>• Date and time, Network Time Protocol (NTP)</li> <li>• Syslog</li> <li>• Reset to factory defaults</li> <li>• Host name, domain name, and banner</li> </ul>

<b>Advanced Router Configuration Parameters</b>	<ul style="list-style-type: none"> <li>• Routing protocols: static, RIP Versions 1 and 2, OSPF, and EIGRP</li> <li>• NAT (static and dynamic)</li> <li>• ACLs</li> <li>• QoS policies, NBAR</li> <li>• VLANs on Cisco EtherSwitch® ports</li> <li>• IP proxy Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP) redirects, ICMP unreachable, ICMP mask reply, and directed broadcasts</li> <li>• AAA local or remote configuration</li> </ul>
<b>Configurable Router Interfaces</b>	<ul style="list-style-type: none"> <li>• Ethernet (10, 10/100, and 10/100/1000 Mbps)</li> <li>• 802.11 a, 802.11 b/g</li> <li>• xDSL (asymmetric DSL [ADSL] and G.SHDSL)</li> <li>• T1/E1 (serial)</li> <li>• ISDN Basic Rate Interface (BRI; with multilevel precedence and preemption)</li> <li>• Analog modem</li> </ul>
<b>Supported WAN Encapsulations</b>	<ul style="list-style-type: none"> <li>• Frame Relay</li> <li>• PPP</li> <li>• PPP over Ethernet (PPPoE)</li> <li>• PPP over ATM (PPPoA)</li> <li>• RFC 1483 routing</li> <li>• HDLC</li> <li>• ADSL autodetect</li> </ul>
<b>Configurable VPN Parameters</b>	<ul style="list-style-type: none"> <li>• Internet Key Exchange (IKE), digital certificates, Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES), and compression</li> <li>• IPSec site to site</li> <li>• Cisco Easy VPN Server</li> <li>• Cisco Easy VPN Remote</li> <li>• Generic-routing-encapsulation (GRE) tunnel</li> <li>• Dynamic Multipoint VPN (DMVPN; both hub and spoke), including dynamic spoke to spoke with redundant hubs</li> </ul>
<b>Supported Firewall Parameters</b>	<ul style="list-style-type: none"> <li>• Context-based access control (CBAC), DMZ, firewall log, firewall and ACL policy view, secure management access</li> </ul>
<b>Supported IPS Features</b>	<ul style="list-style-type: none"> <li>• IPS rules for inbound or outbound traffic inspection, signature fine-tuning, signature customization, and SDEE error message display</li> </ul>
<b>CiscoView Compatibility</b>	<ul style="list-style-type: none"> <li>• Usable with Cisco SDM</li> </ul>
<b>Cisco CallManager Express Compatibility</b>	<ul style="list-style-type: none"> <li>• Usable with Cisco SDM</li> </ul>
<b>Performance</b>	<ul style="list-style-type: none"> <li>• Cisco SDM has negligible impact on router DRAM or CPU</li> </ul>

## SYSTEM REQUIREMENTS

Table 4 lists the system requirements for the Cisco SDM.

**Table 4.** System Requirements

<b>Router Flash Memory</b>	<ul style="list-style-type: none"><li>• Minimum of 6 MB of free Flash memory on the router for Cisco SDM files, or</li><li>• Minimum of 2 MB of free Flash memory on the router for Cisco SDM Express. Wireless Management file requires additional 1.7 MB. Rest of the SDM files can be installed on PC hard disk.</li></ul>
<b>PC Hardware</b>	<ul style="list-style-type: none"><li>• Pentium III or later series processor</li></ul>
<b>PC Operating System</b>	<ul style="list-style-type: none"><li>• Windows XP Professional</li><li>• Windows 2003 Server (Standard Edition)</li><li>• Windows 2000 Professional</li><li>• Windows NT 4.0 Workstation (Service Pack 4)</li><li>• Windows ME</li><li>• Japanese, Simplified Chinese, French, German, Spanish, and Italian language OS support<ul style="list-style-type: none"><li>– Windows XP Professional</li><li>– Windows 2000 Professional</li></ul></li></ul>
<b>Browser Software</b>	<ul style="list-style-type: none"><li>• Microsoft Internet Explorer 5.5 or later</li><li>• Netscape Navigator 7.1 and 7.2</li><li>• Firefox 1.0.5</li></ul>
<b>Java Software</b>	<ul style="list-style-type: none"><li>• Java Virtual Machine (JVM) built-in browsers required</li><li>• Java plug-in (Java Runtime Environment Version 1.4.2_05 or later)</li></ul>

## ORDERING INFORMATION

Table 5 lists ordering and factory shipping options for the Cisco SDM.

**Table 5.** Ordering and Factory Shipping Options for Cisco SDM

<b>Cisco 831 Ethernet Broadband Router, Cisco 836 ADSL over ISDN Broadband Router, Cisco 837 ADSL Broadband Router, Cisco Small Business 100 Series, Cisco 850 Series, and Cisco 870 Series</b>	<ul style="list-style-type: none"><li>• Cisco SDM software ships by default from factory.<ul style="list-style-type: none"><li>– SDM Express is factory installed on router Flash memory, and a Cisco SDM CD is bundled with the router.</li></ul></li></ul>
<b>Cisco 1700 Series Modular Access Routers and Cisco 2600XM Series</b>	<ul style="list-style-type: none"><li>• Cisco SDM software ships by default on security bundles (k9).</li><li>• Cisco SDM software \$0 configuration option (ROUTER-SDM or ROUTER-SDM-NOCF) is available on all SKUs.<ul style="list-style-type: none"><li>– Cisco SDM Express is factory installed on router Flash memory, and a Cisco SDM CD is bundled with the router.</li></ul></li></ul>
<b>Cisco 1800, 2800, and 3800 Series Integrated Services Routers</b>	<ul style="list-style-type: none"><li>• Cisco SDM software ships by default from factory.<ul style="list-style-type: none"><li>– Cisco SDM is factory installed on router Flash memory.</li></ul></li></ul>
<b>Cisco 2691 Multiservice Platform and Cisco 3700 Series Multiservice Access Routers</b>	<ul style="list-style-type: none"><li>• Cisco SDM software ships by default on security bundles (k9).</li><li>• Cisco SDM software \$0 configuration option (part number ROUTER-SDM or ROUTER-SDM-NOCF) is available on all SKUs.<ul style="list-style-type: none"><li>– Cisco SDM is factory installed on router Flash memory.</li></ul></li></ul>

#### **Cisco 7204VXR, 7206VXR, and 7301 Routers**

- Cisco SDM software ships by default on security bundles (k9).
- Cisco SDM software \$0 configuration option (part number ROUTER-SDM or ROUTER-SDM-NOCF) is available on all SKUs.
  - Cisco SDM is factory installed on router Flash memory.

For customers who want to use the Auto-Install feature in Cisco IOS Software, two US\$0 SKUs are offered: ROUTER-SDM-NOCF and ROUTER-SDM-CD-NOCF. If either of these SKUs is ordered with a Cisco router, then manufacturing only loads Cisco SDM files on the router Flash memory, and the default startup configuration is not loaded in the router's NVRAM.

To place an order, visit the [Cisco Direct Order page](#).

### **TO DOWNLOAD THE SOFTWARE**

Visit the [Cisco Software Center](#) to download the latest Cisco SDM software that can be installed on a router Flash memory or on a PC.

### **SERVICE AND SUPPORT**

Cisco offers a wide range of services to accelerate customer success. These innovative services are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, refer to [Cisco Technical Support Services](#).

### **FOR MORE INFORMATION**

For more information about the Cisco SDM, visit <http://www.cisco.com/go/sdm> or contact your Cisco account representative.

**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.  
168 Robinson Road  
#28-01 Capital Tower  
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 Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus  
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

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

205233.BN\_ETMG\_KS\_10.05



