



Data Sheet

Cisco Security Manager 3.01

Cisco® Security Manager is a leading enterprise-class application for managing security. Cisco Security Manager delivers provisioning of firewall, VPN, and intrusion prevention system (IPS) services across Cisco routers, security appliances, and switch services modules.

Cisco Security Manager is part of the Cisco Security Management Suite, which delivers comprehensive policy administration and enforcement for the Cisco Self-Defending Network. Unlike point security products from multiple vendors, which often do not work together and can leave vulnerable gaps, the suite provides a comprehensive solution for provisioning, monitoring, mitigation, and identity to keep networks safer, more resilient, and easier to operate. The suite also includes Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) for monitoring and mitigation.

Using powerful policy-based management techniques, Cisco Security Manager excels at efficiently managing networks of all sizes. Its rich-client graphical user interface provides superior ease of use. Cisco Security Manager provides multiple views into the application to accommodate different tasks and user experience levels, such as the device centric view shown in Figure 1 and the map-centric view shown in Figure 2.

Figure 1. The Device-Centric View Delivers a Simplified Interface to Add Devices and Edit and Deploy Security Policies

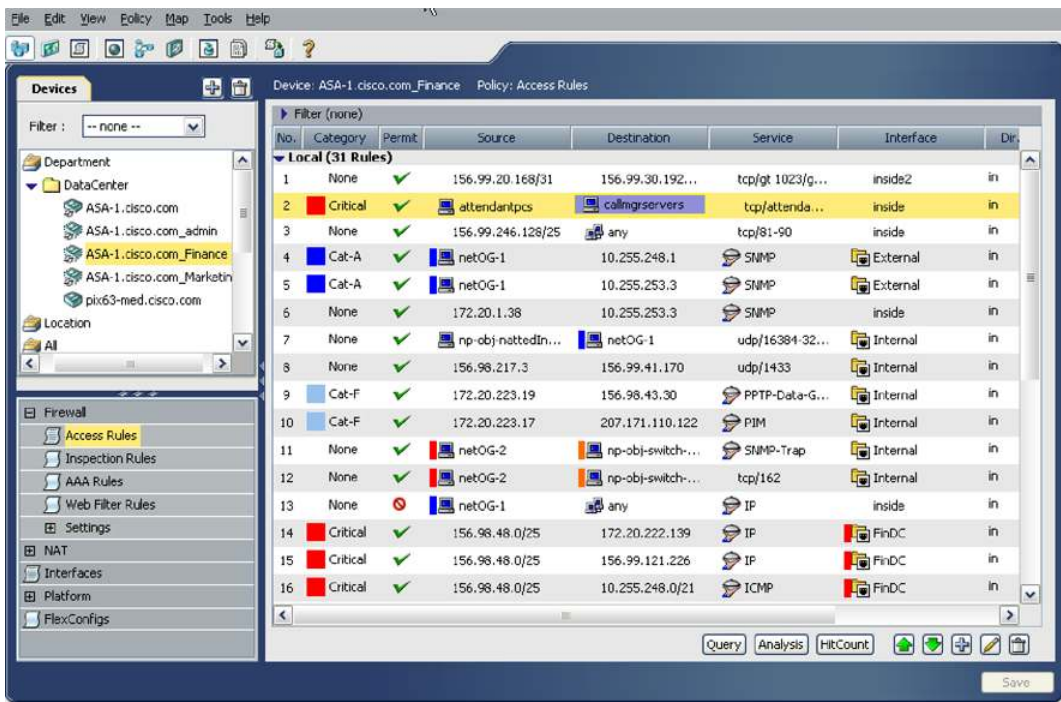
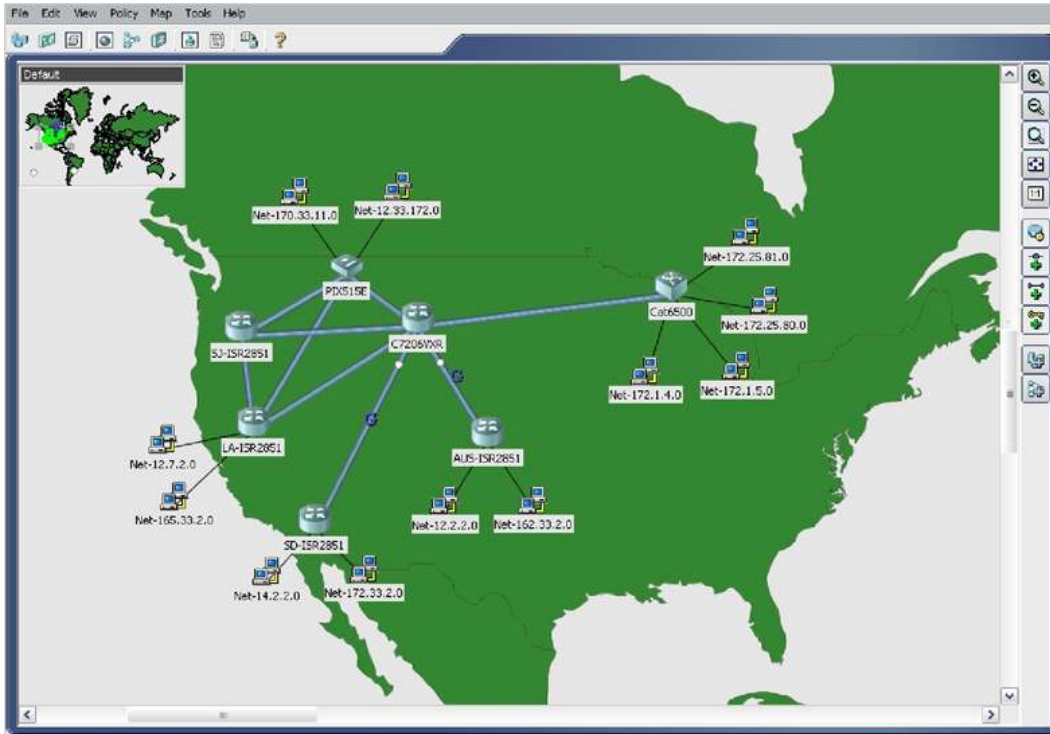


Figure 2. The Map-Centric View Allows You to Manage Policies and Devices Visually



Cisco Security Manager includes “JumpStart”, a built-in interactive tutorial that helps new users quickly learn about Cisco Security Manager features and concepts (Figure 3).

Figure 3. The Cisco Security Manager “JumpStart” Interactive Tutorial



Cisco Security Manager allows security policies to be configured per device, per device group, or globally. Security policies can be applied to Cisco ASA 5500 Series adaptive security appliances, Cisco PIX® security appliances, Cisco IPS 4200 Series sensors, Cisco Catalyst® 6500 Series services modules, and Cisco router platforms running a Cisco IOS® Software security software image.

Table 1 provides a list of features and benefits of Cisco Security Manager 3.01.

Table 1. Cisco Security Manager 3.01 Features and Benefits

Feature	Benefit
Scalable network management	<p>Cisco Security Manager is suitable for efficiently managing networks that range from a few devices to thousands of devices. Scalability is achieved through powerful policy-based management techniques, which allows defining settings once and then optionally assigning the settings to individual devices, groups of devices, or across the enterprise. When a setting is changed, Cisco Security Manager automatically applies the change to all affected network devices. The firewall or VPN policies are platform-neutral, and can be applied across different device platforms such as Cisco routers, security appliances, or services modules. Cisco Security Manager also provides flexible device-level overrides, which allows policy re-use and sharing while retaining the ability to customize device-specific settings as necessary.</p>
VPN provisioning	<p>A VPN wizard provides easy configuration of site-to-site, hub-and-spoke, full-mesh, and extranet VPNs.</p> <ul style="list-style-type: none"> • Cisco Security Manager supports Dynamic Multipoint VPN (DMVPN) and generic routing encapsulation (GRE) IP Security (IPsec), both with dynamic IP and hierarchical certificates. • VPN and Easy VPN services can be configured remotely. • The support of secure device provisioning enables zero-touch deployment. • Configurations for automatic failover and load-balancing for headends are supported.
Firewall provisioning	<p>Cisco Security Manager enables administrators to configure policies for Cisco ASA 5500 Series appliances, Cisco PIX appliances, Cisco Catalyst 6500 Series firewall services modules, and Cisco integrated services router platforms running a Cisco IOS Software security image.</p> <ul style="list-style-type: none"> • The software provides a single rule table for all platforms. Customers benefit from being able to manage these devices through one solution. • The rule analysis feature reports firewall rules that overlap or conflict with other rules. • The object grouping feature dramatically compresses the number of access rules required to implement a particular security policy. Object grouping uses an algorithm to group objects of a similar type so that a single access rule can apply to all objects in the group. • The software helps identify and delete rules that have no effect on the network. • The access control list (ACL) hit count feature checks to ensure traffic is flowing correctly. • The policy query feature displays which rules match a specific source, destination, and service flow, including wildcards. • To ease configuration, device information can be imported from a device repository, imported from a configuration file, or added in the software. Additionally, firewall policies can be discovered from the device itself. • Interface roles allow a user to apply a rule policy on groups of interfaces in a scalable manner.

IPS provisioning	<p>Cisco Security Manager supports the following with the IPS Manager for IPS Sensors:</p> <ul style="list-style-type: none"> • Cisco IPS Sensor Software—An inline, network-based software solution designed to accurately identify, classify, and stop malicious traffic, including worms, spyware and adware, network viruses, and application abuse, before it affects business continuity. • Cisco IOS IPS—Inline intrusion capabilities make Cisco IOS IPS the first system in the industry to provide an inline, deep-packet-inspection-based IPS solution that helps Cisco routers effectively mitigate a wide range of network attacks without compromising traffic-forwarding performance. Able to accurately identify, classify, and stop malicious or damaging traffic in real time, Cisco IOS IPS is a core component of the Cisco Self-Defending Network. Cisco IOS IPS can drop traffic, send an alarm, or reset a connection, enabling a router to respond immediately to security threats. The IPS Manager provides in-depth configuration of Cisco IOS IPS. • Single-interface, multi-VLAN IPS configuration—With the introduction of inline support, the IPS Manager now gives the user the ability to assign VLAN pairs to a single interface. • Rate limiting configuration—Allows an IPS device to limit certain types of traffic by preventing it from using excessive bandwidth. This feature can also signal external devices, such as Cisco IOS routers, to perform rate limiting to accomplish the same function. • Auto-apply signature update—Allows the user to download and automatically update Cisco IPS sensors with signature updates, minor releases, and patches from Cisco.com. • Copy signature wizard—The ability to copy signature tunings from one device to many devices. • Global event configurations—Globally apply event action overrides, event action filters, and event variables to all Cisco IPS sensors. • Out-of-band configuration detection—The IPS Manager detects out-of-band configuration changes made to devices by other management components. Once an out-of-band configuration is detected, users can be notified via the Sensor Health and Welfare feature.
Integrated security services management	Cisco Security Manager enables the management of integrated security services, including quality of service (QoS) for VPN, routing, Network Admission Control (NAC), and more.
Flexible device grouping options	Users can create and define device groups based on business function or location to accurately represent their organizational structure. All devices in a group can be managed as easily as a single device.
Multiple application views	Cisco Security Manager provides multiple views into the application to support different use cases and experience levels. The device-centric view is useful for novice users or those more familiar with using single device managers. The map-centric view helps in visualizing the topologies of VPNs or containment relationships between Cisco Catalyst 6500 Series service modules and security contexts. The policy-centric view excels at performing highly efficient and scalable multi-device management.
Policy object manager	Re-usable objects can be created (for example, to represent network addresses, services, device settings, time ranges, or VPN parameters). Objects can be defined once and used any number of times to avoid manually entering values.
Deployment manager—flexible deployment options	Cisco Security Manager supports both on-demand and scheduled deployments to a device or to files.
Rollback	Cisco Security Manager provides the ability to roll back to a previous configuration, if required.
Role-based access control	With Cisco Security Manager, access rights can be defined for multiple administrators, with appropriate controls. Cisco Security Manager is delivered with five user roles; additional roles are available with the optional Cisco Secure ACS.
Workflow	Cisco Security Manager optionally allows assigning specific tasks to each administrator during the deployment of a policy, with formal change control and tracking. The workflow helps improve staff collaboration (for example, between network and security operations).
Distributed deployment methodologies—Auto Update Server, Cisco Network Services Configuration Engine	Cisco Security Manager simplifies updates to large numbers of remote firewalls, which may have dynamic addresses or NAT addresses. This is a valuable feature for customers with remote locations with intermittent networks links and minimal technical staff at the remote site.
Operational management	Cisco Security Manager helps with operational functions such as software distribution or device inventory reporting. The software integrates with the Device and Credentials Repository (DCR) and CiscoWorks Resource Manager Essentials (RME).
Health and performance monitoring	Customers with a Cisco Security Manager service contract can download the CiscoWorks Monitoring Center for Performance application when available from Cisco.com. This application provides health and performance monitoring data for Cisco network devices and specific security services.

Changes in Cisco Security Manager 3.01

Cisco Security Manager 3.01 is a minor software update that makes the following enhancements to Cisco Security Manager 3.0:

- Added support for Cisco Catalyst 6500 Series Firewall Services Module 3.1
- Added support for Cisco ASA Software 7.1 and Cisco PIX Software 7.1

- Added support for the Cisco 7600 Series/Cisco Catalyst 6500 Series IPsec VPN Shared Port Adapter device
- Added support for the management of Cisco Catalyst 6500 Series router access control lists (ACLs)
- Added support for the configuration of Network Time Protocol (NTP) and syslog on Cisco IOS routers
- Includes an updated version of CiscoWorks RME (Version 4.04)
- Includes fixes to several known software bugs

Cisco Security Manager 3.01 also enforces the licensing key, which controls how many devices can be added in the software. If the license limit is exceeded in Version 3.0, an upgrade to Version 3.01 will prevent a new device from being added in the management software. Operators can purchase an increased license key to allow management of more devices. This does not require a re-installation of the software. Operators can use the Cisco Security Manager administrator options to easily add a new key. The licensing purchase options are listed in the product bulletin at:

http://www.cisco.com/en/US/products/ps6498/prod_bulletins_list.html

Table 2 lists the minimum server requirements for Cisco Security Manager. Table 3 provides the minimum client requirements.

Table 2. Server Requirements and Restrictions

Component	Minimum Requirement
System hardware	<ul style="list-style-type: none"> • IBM PC-compatible with a 2-GHz or faster processor • Color monitor with at least 1024 x 768 resolution and a video card capable of 16-bit colors • DVD-ROM drive • 100BASE-T (100 Mbps) or faster network connection; single interface only • Keyboard • Mouse
File system	<ul style="list-style-type: none"> • NTFS
Memory (RAM)	<ul style="list-style-type: none"> • 2 GB
System software	<p>One of the following:</p> <ul style="list-style-type: none"> • Microsoft Windows 2003 Server: <ul style="list-style-type: none"> ◦ Enterprise Edition with SP1 ◦ Standard Edition with SP1 • Microsoft Windows 2000: <ul style="list-style-type: none"> ◦ Advanced Server with SP4 ◦ Server with SP4 ◦ Professional with SP4 <p>Note: Cisco Security Manager supports only the U.S. English and Japanese versions of Windows. Microsoft ODBC Driver Manager 3.510 or later is also required, so your server can work with Sybase database files.</p>
Browser	<p>One of the following:</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer 6.0 (6.0.2600) • Microsoft Internet Explorer 6.0 with SP1 (6.0.2800) • Mozilla 1.7 or 1.7.5
Compression software	WinZip 9.0 or compatible
Hard drive space	20 GB
IP address	<p>One static IP address</p> <p>If the server has more than one IP address, disable all but one address. The Cisco Security Manager installer displays a warning if it detects any dynamic IP addresses on the target server. Dynamic addresses are not supported.</p>

Table 3. Client Requirements and Restrictions

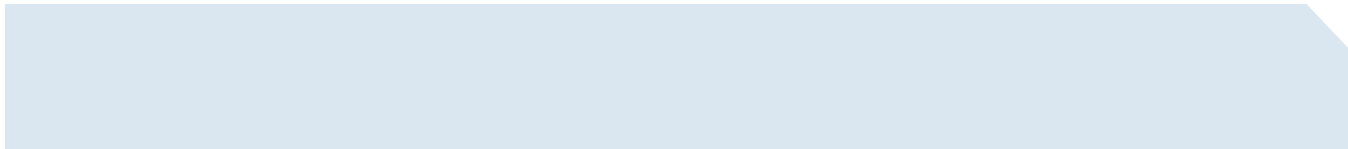
Component	Minimum Requirement
System hardware	<ul style="list-style-type: none">• IBM PC-compatible with a 1-GHz or faster processor• Color monitor with video card set to 24-bit color depth• Keyboard• Mouse
Memory (RAM)	1 GB
Virtual memory/ swap space	512 MB
Hard drive space	10 GB
Operating system	One of the following: <ul style="list-style-type: none">• Microsoft Windows XP Professional with SP1 or higher• Microsoft Windows 2003:<ul style="list-style-type: none">◦ Server Edition with SP1◦ Enterprise Edition with SP1• Microsoft Windows 2000:<ul style="list-style-type: none">◦ Advanced Server with SP4◦ Professional with SP4 <p>Note: The Cisco Security Manager Client supports only the U.S. English and Japanese versions of Windows. It does not support any other language version.</p>
Browser	One of the following: <ul style="list-style-type: none">• Microsoft Internet Explorer 6.0 (6.0.2600)• Microsoft Internet Explorer 6.0 with SP1 (6.0.2800)• Mozilla 1.7 or 1.7.5
Java	The Cisco Security Manager Client includes an embedded and completely isolated version of Java. This Java version does not interfere with your browser settings or with other Java-based applications. If you try to open IPS Manager but do not have the required version of Java, your Cisco Security Manager server will display a message that tells you how to download and install the required Java version.

For more information on Cisco Security Manager hardware and software requirements, refer to the Cisco Security Manager Installation Guide at <http://www.cisco.com/go/csmanager>.

Table 4 lists some of the device product families supported by Cisco Security Manager. For a full list, refer to the document Supported Devices and OS Versions for Cisco Security Manager available at http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html.

Table 4. Overview of Cisco Devices Supported by Cisco Security Manager

Supported Devices
Cisco PIX Security Appliances
Cisco ASA 5500 Series Adaptive Security Appliances
Cisco Integrated Services Routers
Cisco 7600 Series Routers
Cisco 7500 Series Routers
Cisco 7300 Series Routers
Cisco 7200 Series Routers
Cisco 7100 Series Routers
Cisco Catalyst 6500 Series Firewall Services Modules
Cisco Catalyst 6500 Series VPN Services Modules
Cisco 7600 Series/Catalyst 6500 Series IPsec VPN Shared Port Adapters



Cisco Catalyst 6500 Series IDSM-2
Cisco IPS 4200 Series Sensors
Cisco Catalyst 6500 Series IPS Services Modules
Cisco IOS IPS Router Sensor Modules

For a list of devices supported by the optional CiscoWorks RME 4.04, view the compatibility documentation at:
http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html.

ORDERING INFORMATION

The Cisco Security Manager product bulletin describes the licensing options and the ordering details. The bulletin is published under product literature at <http://www.cisco.com/go/csmanager>.



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.com Website at 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 © 2006 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, 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, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, 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, 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. (0601R)