

## Cisco Security Manager 3.3

### **Cisco Security Manager Overview**

Cisco® Security Manager is an enterprise-class management application designed to configure firewall, VPN, and intrusion prevention (IPS) security services on Cisco network and security devices. Cisco Security Manager can be used in networks of all sizes—from small networks to large networks consisting of thousands of devices—by using policy-based management techniques. Cisco Security Manager works in conjunction with the Cisco Security Monitoring, Analysis, and Response System (MARS). Used together, these two products provide a comprehensive security management solution that addresses configuration management, security monitoring, analysis, and mitigation.

### **Cisco Self Defending Network**

The Cisco Self-Defending Network is an architectural solution designed for the evolving security landscape. Security is integrated everywhere and with the help of a lifecycle services approach, enterprises can design, implement, operate, and optimize network platforms that defend critical business processes against attack and disruption, protect privacy, and support policy and regulatory compliance controls. Using the network as the platform keeps people and IT assets safe, makes the organization more resilient and reliable, and enables maximum business impact from IT investment. Cisco Security Manager is a vital piece of the Cisco Self-Defending Network, which enables business initiatives to actively and collaboratively to control known and unknown threats while enforcing closed-loop security policies on all managed Cisco security devices.

### **Collaborative Threat Identification and Mitigation**

The Global correlation features in IPS, Cisco Security MARS, and Cisco Security Manager together provide unmatched network threat identification and mitigation. Global correlation on IPS and MARS provides increased intelligence to detect the security threats seen by your organization. Cisco Security Manager provides control to mitigate these network threats by defining and deploying appropriate security policies.

### **Single Integrated Security Solution**

Cisco Security Manager is an integrated application that manages security across Cisco security appliances, routers, and switches. The broad range of functions can be precisely controlled for specific users through the use of Cisco Security Manager's role-based access control (RBAC) mechanisms. RBAC and Cisco Security Manager's optional workflow feature allow both traditional security operations and network operations teams to use Cisco Security Manager within their respective roles.

### **Increase Security Efficiency and Flexibility**

Cisco Security Manager efficiently manages networks that range from a few devices to thousands of devices. Flexibility is achieved through powerful policy-based management techniques, enabling an efficient "configure-once, deploy-to-many" paradigm. When a setting is changed, Cisco Security Manager automatically applies the change to all affected network devices. The firewall, VPN, and IPS 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 reuse and sharing while retaining the ability to customize device-specific settings as necessary.

### Superior Control and Visibility

Cisco Security Manager provides superior day-to-day security management control and visibility into firewall rule analysis and optimization, VPN configuration, and IPS signature management. Cisco Security Manager and Cisco Security MARS provide real-time views into the security policy events with immediate insight and control of policy settings. This control encourages tighter collaboration between network operations and security operations groups while enabling immediate event verification of newly update policies. Policy event correlation between Cisco Security Manager and Cisco Security MARS enables greater visibility into incident investigation and ultimately speeds resolution time for threat mitigation.

Figures 1 shows some of the collaboration mechanisms between Cisco Security Manager and Cisco Security MARS.

**Figure 1.** Cisco Security Manager IPS Policy to Cisco Security MARS Event Collaboration

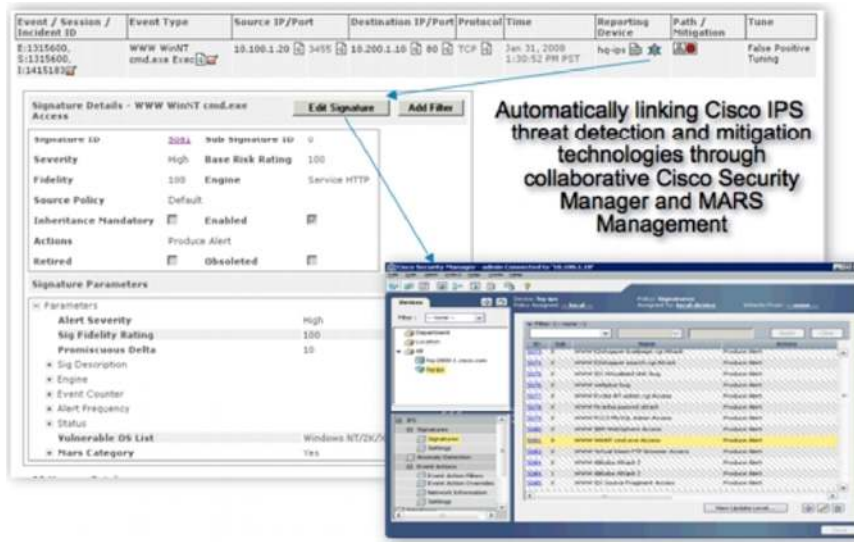


Table 1 provides a list of features and benefits of Cisco Security Manager 3.3.

**Table 1.** Cisco Security Manager 3.3 Features and Benefits

Feature	Benefit
<b>VPN Configuration</b>	<ul style="list-style-type: none"> <li>• The VPN Wizard provides easy configuration of site-to-site, hub-and-spoke, full-mesh, and extranet VPNs.</li> <li>• Support for Group Encrypted Transport VPN (GETVPN), Dynamic Multipoint VPN (DMVPN) and generic routing encapsulation (GRE) IP Security (IPsec), both with dynamic IP and hierarchical certificates, enables common VPN deployment scenarios for customers</li> <li>• VPN and Easy VPN services can be configured remotely enabling centralized management</li> <li>• Zero touch deployment with secure device provisioning</li> <li>• Configurations for automatic failover and load-balancing for head-ends are supported thereby increasing robustness of deployments</li> <li>• Support for SSL VPN on the ASA 5500 Series provides added flexibility in VPN deployments</li> </ul>

Feature	Benefit
<b>Firewall Configuration</b>	<ul style="list-style-type: none"> <li>• Administrators can centrally 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</li> <li>• Administrators can now deploy their Zone-Based Firewall (ZBF) related policy settings on supported device platforms.</li> <li>• Botnet Traffic filter support on ASA platform enables application layer inspection and blocks phone home activity by Botnets</li> <li>• Content Filtering support for IOS-based device platform allows traffic filtering based on deep content inspection</li> <li>• CSM software provides a single rule table for all platforms. Customers can manage these different device platforms through one management tool.</li> <li>• The policy query feature displays which rules match a specific source, destination, and service flow, including wildcards. This feature allows the administrator to define policies more efficiently.</li> <li>• 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. This feature simplifies initial security management set up.</li> <li>• Interface roles allow a user to apply a rule policy on groups of interfaces in a scalable manner. This feature provides more flexibility in managing a group of devices centrally using CSM.</li> </ul>
<b>IPS Configuration</b>	<ul style="list-style-type: none"> <li>• Cisco Security Manager enables administrators to easily and effectively manage IPS solution-based configuration and update policies for Cisco IPS 4200 Series sensors, the Cisco ASA Advanced Inspection and Prevention Security Services Module (AIP-SSM), the Cisco ASA Advanced Inspection and Prevention Security Services Card (AIP-SSC), the Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2 (IDSM-2), the Cisco IDS Network Module, the Cisco IPS AIM, and Cisco IOS IPS.</li> <li>• Cisco IPS Sensor Software Versions 7.0 and 6.2: The Cisco IPS solution combines an inline, intrusion prevention service with innovative technologies that improve accuracy. Cisco IPS Sensor Software accurately identifies, classifies, and stops malicious traffic, including worms, spyware and adware, network viruses, and application abuse, before they affect business continuity.</li> <li>• New Features in Cisco IPS Sensor software version 7.0 including Global Correlation and Reputation score based policies settings. These features enable cross correlation of security threats and enhance security in a network.</li> <li>• Cisco IOS IPS is an inline, deep-packet-inspection-based feature that enables Cisco IOS Software to effectively mitigate a wide range of network attacks. As a core facet of the Self-Defending Network, Cisco IOS IPS enables the network to defend itself with the intelligence to accurately identify, classify, and stop or block malicious or damaging traffic in real time.</li> <li>• Insight into Cisco IPS signature updates allows for incremental provisioning of new and updated signatures, as well as insight into IntelliShield before deploying to your enterprise. This allows for immediate insight into the Cisco IPS Security Research Team's recommended defaults, and allows customers to tune to their environment before distributing the signature update.</li> <li>• The Cisco IPS Update Wizard allows efficient automatic IPS updates, scheduling, and distribution of policies with status and details notification.</li> <li>• Cross-collaboration with Cisco Security MARS enables event/anomaly investigation with immediate insight into policy deployment changes. This collaboration enables policy launching of historic and real-time events, encouraging tighter collaboration between network operations and security operations teams while keeping Cisco Security Manager policies in band. Insight and cross-collaboration decreases event investigation and troubleshooting, thus speeding resolution time. Cisco Security Manager and Cisco Security MARS collaboration enables interactive IPS event action filter creation, thus reducing your network's vulnerability exposure.</li> <li>• IPS signature policies and event action filters can be inheritable and assignable to any device. All other IPS policies can be assignable and shared with other IPS devices. IPS management also includes policy rollback, a configuration archive, and cloning or creation of signatures. Copying policies between devices allows for effective management and reduces TCO by reducing deployment efforts.</li> <li>• IPS update administration and IPS subscription licensing updates streamline the distribution and allow users to manage IPS software, signature updates, and licensing based on local and shared policies.</li> <li>• NTLmV2 proxy authentication for IPS licensing and signature updates supports Windows based client authentication</li> <li>• CSV export for select IPS features such as signatures, event action filters, signature deltas etc facilitates storage and exchange of these data between different CSM server instances.</li> </ul>
<b>Bulk Operation Feature</b>	<p>CSM 3.3 has introduced bulk operation feature that reduce administrative overhead while managing a network with large number of devices including the following features:</p> <ul style="list-style-type: none"> <li>• Bulk import and export of policy objects</li> <li>• Bulk addition for offline devices</li> <li>• Bulk import of device level overrides</li> </ul>
<b>Integrated Security Services Management</b>	<p>Cisco Security Manager enables the management of integrated security services, including quality of service (QoS) for VPN, routing, Network Admission Control (NAC), and more.</p>
<b>Flexible Device Grouping Options</b>	<p>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.</p>
<b>Multiple Application Views</b>	<p>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 services modules and security contexts. The policy-centric view enables highly efficient and scalable multidevice management.</p>
<b>Policy Object Manager</b>	<p>Reusable 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.</p>

Feature	Benefit
<b>Deployment Manager with Flexible Deployment Options</b>	Cisco Security Manager supports both on-demand and scheduled deployments to a device or to files.
<b>Rollback</b>	Cisco Security Manager provides the ability to roll back to a previous configuration, if required.
<b>Role-Based Access Control</b>	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 Access Control Server (ACS).
<b>Workflow</b>	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).
<b>Distributed Deployment Methodologies (Auto Update Server, Cisco Network Services Configuration Engine)</b>	Cisco Security Manager simplifies updates to large numbers of remote firewalls, which may have dynamic addresses or Network Address Translation (NAT) addresses. This is a valuable feature for customers that have remote locations with intermittent networks links and minimal technical staff at the remote site.
<b>Operational Management</b>	The included companion application, Resource Manager Essentials (RME), helps with operational functions such as software distribution or device inventory reporting.
<b>Health and Performance Monitoring</b>	The included companion application, Performance Monitor, provides health and performance monitoring data for Cisco VPN network devices and specific security services.

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

**Table 2.** Server Requirements and Technical Specifications

Component	Requirement
<b>System Hardware</b>	<ul style="list-style-type: none"> <li>• Minimum: One CPU <math>\geq</math> 2GHz; Recommended: Two CPUs <math>\geq</math> 2 GHz or One dual-core CPU <math>\geq</math> 2 GHz</li> <li>• Color monitor with at least 1280x1024 resolution and a video card capable of 16-bit colors</li> <li>• DVD-ROM drive</li> <li>• 100BASE-T (100 Mbps) or faster network connection; single interface only</li> <li>• Keyboard</li> <li>• Mouse</li> </ul>
<b>File System</b>	NTFS
<b>Memory (RAM)</b>	Minimum: 2 GB; Recommended: 4 GB.
<b>System Software</b>	<p>One of the following:</p> <ul style="list-style-type: none"> <li>• Microsoft Windows 2003 Server editions:</li> <li>• Enterprise Edition with SP1 or SP2</li> <li>• Standard Edition with SP1 or SP2</li> <li>• R2 Enterprise Edition with SP1 or SP2</li> <li>• R2 Standard Edition with SP1 or SP2</li> </ul> <p><b>Note:</b> 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>
<b>Browser</b>	<p>One of the following:</p> <ul style="list-style-type: none"> <li>• Microsoft Internet Explorer 6.0 SP2</li> <li>• Microsoft Internet Explorer 7.0</li> <li>• Firefox 2.0</li> </ul>
<b>Compression Software</b>	WinZip 9.0 or compatible
<b>Hard Drive Space</b>	20 GB
<b>IP Address</b>	<p>At least 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>
<b>Optional Virtualization Software</b>	VMware ESX Server 3.5

**Table 3.** Client Requirements and Technical Specifications

Component	Requirement
<b>System Hardware</b>	<ul style="list-style-type: none"> <li>• One CPU <math>\geq</math> 2 GHz.</li> <li>• Color monitor with at least 1280x1024 resolution and a video card capable of 16-bit colors</li> <li>• Keyboard</li> <li>• Mouse</li> </ul>
<b>Memory (RAM)</b>	Minimum: 1 GB; Recommended: 2 GB
<b>Virtual Memory/Swap Space</b>	512 MB
<b>Hard Drive Space</b>	10 GB
<b>Operating System</b>	<p>One of the following:</p> <ul style="list-style-type: none"> <li>• Microsoft Windows Vista Business Edition or Enterprise Edition with SP1</li> <li>• Microsoft Windows XP Professional with SP1 or SP2 or SP3</li> <li>• Microsoft Windows 2003 Server editions: <ul style="list-style-type: none"> <li>• Enterprise Edition with SP1 or SP2</li> <li>• Standard Edition with SP1 or SP2</li> <li>• R2 Enterprise Edition with SP1 or SP2</li> <li>• R2 Standard Edition with SP1 or SP2</li> </ul> </li> </ul> <p><b>Note:</b> 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>
<b>Browser</b>	<p>One of the following:</p> <ul style="list-style-type: none"> <li>• Microsoft Internet Explorer 6.0 SP2</li> <li>• Microsoft Internet Explorer 7.0</li> <li>• Firefox 2.0</li> </ul>
<b>Java</b>	<p>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.</p> <p>If you try to open Cisco Security 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.</p>

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 summarizes the device product families supported by Cisco Security Manager. For a detailed list, including supported device software versions, refer to the document entitled "Supported Devices and OS Versions for Cisco Security Manager 3.3." This document is available at [http://www.cisco.com/en/US/products/ps6498/products\\_device\\_support\\_tables\\_list.html](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 (including 800, 1800, 2800 and 3800 Series)
Cisco Integrated Services Routers Generation 2 (including 1900, 2900 and 3900 Series)— <i>needs CSM version 3.3.1 or higher</i>
Cisco 1000 Series Aggregation Service Routers
Cisco 7600 Series Routers
Cisco 7500 Series Routers
Cisco 7300 Series Routers
Cisco 7200 Series Routers
Cisco 7100 Series Routers
Cisco 3200 Series Routers
Cisco 2600 Series Routers
Cisco Catalyst 6500 Series Firewall Services Modules (FWSMs)

Supported Devices
Cisco Catalyst 6500 Series VPN Services Modules (VPNSMs)
Cisco 7600 Series/Catalyst 6500 Series IPsec VPN Shared Port Adapters (VPNSPAs)
Cisco Catalyst 6500 Series IDSM-2
Cisco IPS 4200 Series Sensors
Cisco AIP-SSM for Cisco ASA 5500 Series Adaptive Security Appliances
Cisco AIP-SSC for Cisco ASA 5500 Series Adaptive Security Appliances
Cisco IPS AIM for Integrated Services Routers
Cisco IPS Module for Access Routers (NM-CIDS)
Cisco Catalyst 3550, 3560, 3560E, 3750, 3750 Metro, 4500, 4948, and 4948 10GE Desktop Switches

For a list of devices supported by the optional CiscoWorks RME 4.2, view the Supported Devices Tables for LMS 3.1 available at [http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products\\_device\\_support\\_tables\\_list.html](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 ordering details. The bulletin is published at <http://www.cisco.com/go/csmanager>.

## Cisco Services

Cisco takes a lifecycle approach to services, and with its partners, provides a broad portfolio of security services so enterprises can design, implement, operate, and optimize network platforms that defend critical business processes against attack and disruption, protect privacy, and support policy and regulatory compliance controls.

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, visit [http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv\\_group\\_home.html](http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html).

- **Cisco Security Optimization Service** helps integrate security into the core network infrastructure. The network infrastructure is the foundation of the agile and adaptive business. The Cisco Security Optimization Service supports the continuously evolving security system to meet ever-changing security threats through a combination of planning and assessments, design, performance tuning, and ongoing support for system changes.
- **The Cisco Security Center** provides a single location for early warning threat intelligence threat and vulnerability analysis, Cisco IPS signatures and mitigation techniques. Visit and bookmark the Cisco Security Center at <http://www.cisco.com/security>.
- **Cisco Security Intellishield Alert Manager Service** provides a customizable, Web-based threat and vulnerability alert service that allows organizations to easily access timely, accurate, and credible information about potential vulnerabilities in their environment.

Cisco Security Manager software is eligible for technical support service coverage under Cisco Software Application Support (SAS). Cisco SAS service agreement features include:

- Unlimited access to the Cisco Technical Assistance Center (TAC) for award-winning support. Technical assistance is provided by Cisco software application experts who are trained in Cisco security software applications. Support is available 24 hours per day, 7 days per week, 365 days per year worldwide.

- Registered access to Cisco.com, a robust repository of application tools and technical documents to assist in diagnosing network security problems, understanding new technologies, and staying current with innovative software enhancements. Utilities, white papers, application design data sheets, configuration documents, and case management tools help expand your in-house technical capabilities.
- Access to application software bug fixes and maintenance and minor software releases.

### For More Information

For more information about Cisco Security Manager 3.3, visit <http://www.cisco.com/go/csmanager>, or contact your account manager or a Cisco Authorized Technology Provider. You may also send e-mail to [ask-csmanager@cisco.com](mailto:ask-csmanager@cisco.com).

For more information about Cisco Security MARS, visit <http://www.cisco.com/go/mars>.



Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

Asia Pacific Headquarters  
Cisco Systems (USA) Pte. Ltd.  
Singapore

Europe Headquarters  
Cisco Systems (transitions) BV  
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

CCDE, CCENT, CCS, Cisco IaaS, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nexus Connect, Cisco Prime, Cisco Security, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Hio for Coda, Hio Mind, Hiperate (Design), Hip Ultra, Hip Video, Hip Video (Design), Incident Broadband, and Welcome to the Human Network are trademarks. Changing the Way We Work, Live, Play and Learn, Cisco Capital, Cisco Capital (Design), Cisco Financial (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks, and Access Register, Almond, All built, AsyncOS, Bringing the Meeting to You, Catalyst, CCDA, CCDE, CCIE, CCIP, CCNA, CCNP, CCS, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumina, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Goals, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, Fireport, FireSwitch, Event Center, Explorer, Follow Me Browsing, GainMedia, IYX, OS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Online Sound, MGX, Networker, Networking Academy, PCNow, PX, PowerKEY, PowerPanel, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROBA, SenderBase, SMI (Text), Spectrum Expert, StackWise, WebEx, and the WebEx logo 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. (0910)