Cisco Security Manager 4.3

Businesses are facing daunting new challenges in security operations. The growing number and increasing complexity of security technologies, combined with the reduction and redirection of IT headcount once dedicated to security management, has dramatically increased the potential for human error, which can lead to security exposures and incidents. To counteract these challenges, it's invaluable for security operations teams to have an integrated, end-to-end management solution that enables consistent policy enforcement, allows rapid troubleshooting of security events, and delivers summarized reports across the security deployment.

Cisco® Security Manager is a comprehensive management solution that enables advanced management and rapid troubleshooting of multiple security devices. Cisco Security Manager provides scalable, centralized management from which administrators can efficiently manage a wide range of Cisco security devices, gain visibility across the network deployment, and securely share information with other essential network services such as compliance systems and advanced security analysis systems. Designed to maximize operational efficiency, Cisco Security Manager also includes a powerful suite of automated capabilities, such as health and performance monitoring, software image management, auto-conflict detection, and integration of trouble tickets.

Cisco Security Manager supports a wide range of Cisco security devices, including Cisco ASA 5500 Series Adaptive Security Appliances, Cisco IPS 4200 and 4300 Series Sensors, Cisco Secure Routers, and the Cisco AnyConnect™ Secure Mobility Client.

Features and Benefits

Table 1 summarizes additional Cisco Security Manager 4.3 features and benefits.

Table 1.   Cisco Security Manager 4.3 Features and Benefits

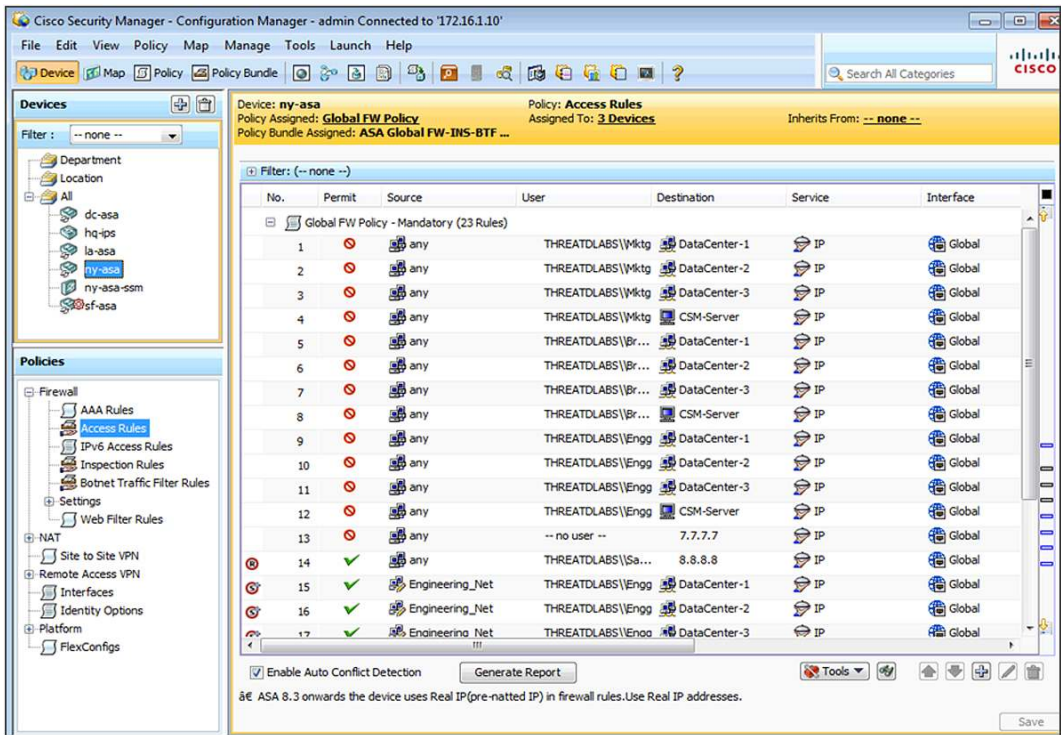| Feature	Benefit
Firewall Configuration	
Manages the Cisco Security Deployment	Enables centralized management of the Cisco security environment, including: • Cisco ASA 5500 Series Adaptive Security Appliances • Cisco IPS 4200 and 4300 Series Sensor Appliances • Cisco AnyConnect Secure Mobility Client • Cisco Secure Routers • Cisco Catalyst® 6500 Series Firewall Services Modules (FWSM) and ASA Services Modules (ASASM) • Cisco Integrated Services Router (ISR) platforms running a Cisco IOS® Software security image
Zone-based Policies	Enables zone-based firewall (ZBF) policy settings to be deployed on supported device platforms
Botnet Traffic Filter	Supports the Botnet Traffic Filter on the Cisco ASA platform, for application-layer inspection and blockage of "phone-home" activity by botnets
Content Filtering	Supports content filtering on Cisco IOS Software-based device platforms to filter traffic based on deep content inspection Enables the management of multiple device platforms using a single rule table
Efficient Policy Definition	Increases the efficiency with which administrators can define policies by clearly displaying which rules match a specific source, destination, and service flow, including wildcards

Feature	Benefit
Simplified Setup	Streamlines configuration and simplifies initial security management setup by enabling device information to be imported from a device repository or configuration file, added in the software, or discovered from the device itself
Streamlined Operations	Significantly reduces manual tasks while reducing errors and optimizing the security environment, through: • Rule Conflict Detection, Hit Count Analysis, Rule Combiner, and other powerful tools to analyze and optimize rule sets • Role-based access control (RBAC) and workflow to help ensure error-free deployments and process compliance
Interface Roles	Enables rule policies to be applied to groups of interfaces and centrally managed, to maximize flexibility and scalability
IPS Configuration	
Configuration And Update Policies	Enables administrators to easily and effectively manage intrusion protection system (IPS)-based configuration and update policies for: • Cisco IPS 4200 and 4300 Series Sensors • Cisco ASA Advanced Inspection and Prevention Security Services Module (AIP-SSM) • Cisco ASA Advanced Inspection and Prevention Security Services Card (AIP-SSC) • Cisco Catalyst® 6500 Series Intrusion Detection System Services Module 2 (IDSM-2) • Cisco IDS Network Module • Cisco IPS Advanced Integration Module (AIM) • Cisco IOS IPS
Signature Updates	Enables incremental provisioning of new and updated signatures before deploying them to the enterprise
Threat Research	Allows administrators to tune to their environment based on insights gained from Security Intelligence Operations (SIO), the Cisco IntelliShield Alert Manager Service, and Cisco IPS Security Research Team recommendations before distributing the signature update
Update Wizard	Enables efficient, automatic IPS updates, scheduling, and distribution of policies with status and detail notification
Reusable Policies	Enables IPS signature policies and event action filters to be inheritable and assignable to any device; all other IPS polices can be assigned to and shared with other IPS devices
Policy Rollback	Includes IPS policy rollback, a configuration archive, and cloning or creation of signatures
CSV Export	Comma-separated value (CSV) export for select IPS features such as signatures, event action filters, and signature delta settings facilitates storage and exchange of this data between different Cisco Security Manager server instances
VPN Configuration	
VPN Wizard	Provides easy configuration of site-to-site, hub-and-spoke, full-mesh, and extranet VPNs
Supports Common VPN Deployment Scenarios	Enables common VPN deployment scenarios with support for Group Encrypted Transport VPN (GET VPN), Dynamic Multipoint VPN (DMVPN), and generic routing encapsulation (GRE) IP Security (IPsec), both with dynamic IP and hierarchical certificates
Remote Configuration	Enables centralized management of VPNs
Efficiency and Usability Features	
Ticketing Integration	Changes made in multiple ticketing systems can be tagged with a single ticket identifier, enabling them to be easily queried for audit
Global Search	Enables all devices, policies, and policy objects in the configuration database using a particular IP address or service to be found
Find Usage	Enables administrators to quickly find usage information about objects by pointing to the exact rules that use a particular policy object, in addition to providing details about all the policies that use the object
Auto-Conflict Detection	Provides a clear picture about rule conflicts, to simplify rule optimization and troubleshooting
Integrated Event Management	Enables administrators to monitor status and troubleshoot security issues, including: • Receipt of syslog messages from Cisco ASA appliances and Security Device Event Exchange (SDEE) messages from Cisco IPS sensors • Real-time and historical event viewing • Cross-linkages to firewall access rules and IPS signatures for quick navigation to the source policies • Prebundled set of views for firewall, IPS, and VPN monitoring • Customizable views for monitoring select devices or a select time range • Intuitive GUI controls for searching, sorting, and filtering events • Administrative options to turn event collection on or off for select security devices

Feature	Benefit
Report Manager	Supports system reports and the creation of predefined reports, all of which can be: • Viewed as charts and grids • Exported to PDF/Excel • Scheduled for delivery via email
Bulk Operations	Reduces administrative overhead in networks that have a large number of devices. The feature includes: • Bulk import and export of policy objects • Bulk addition for offline devices • Bulk import of device-level overrides
Device Grouping	Allows administrators to create and define device groups based on business function or location, and then manage all devices in a group as a single device
Policy Object Manager	Objects such as network addresses, services, device settings, time ranges, or VPN parameters can be defined once and then used any number of times to avoid manual entry of values
Other Capabilities	
Third-Party Device Support	Supports "unmanaged" endpoints and third-party devices
Security Services Management	Enables the management of integrated security services, including quality of service (QoS) for VPN, routing, and Network Admission Control (NAC)
Multiple Application Views	Provides multiple views into the application to support different use cases and experience levels
Flexible Deployment Options	Security deployments can be implemented on either an on-demand or scheduled basis
Rollback	Deployments can be rolled back to a previous configuration if required
Role-Based Access Control	Up to five administrator roles can be defined and enforced; additional roles are available with the optional Cisco Secure Access Control Server (ACS)
Workflow	Specific tasks can be assigned to each administrator during the deployment of a policy, with formal change control and tracking
Distributed Deployment	Includes the Auto Update Server and the Cisco Network Services Configuration Engine to simplify updates to large numbers of remote firewalls, which may have dynamic addresses or NAT addresses
Operational Management	Includes CiscoWorks Resource Manager Essentials (RME) to assist with operational functions such as software distribution or device inventory reporting
Health and Performance Monitoring	Continuously analyzes the security environment and sends alerts when preset thresholds are reached

Integrated Policy and Object Management

Cisco Security Manager helps enable the reuse of security rules and objects, and enhances the ability to monitor security threats from throughout the deployment, minimizing the potential for errors, and maximizing efficiency. Administrators can implement security deployments on either an on-demand or scheduled basis, and can roll back to a previous configuration if required. Role-based access control and deployment workflows help ensure that compliance processes are followed (see Figure 1).
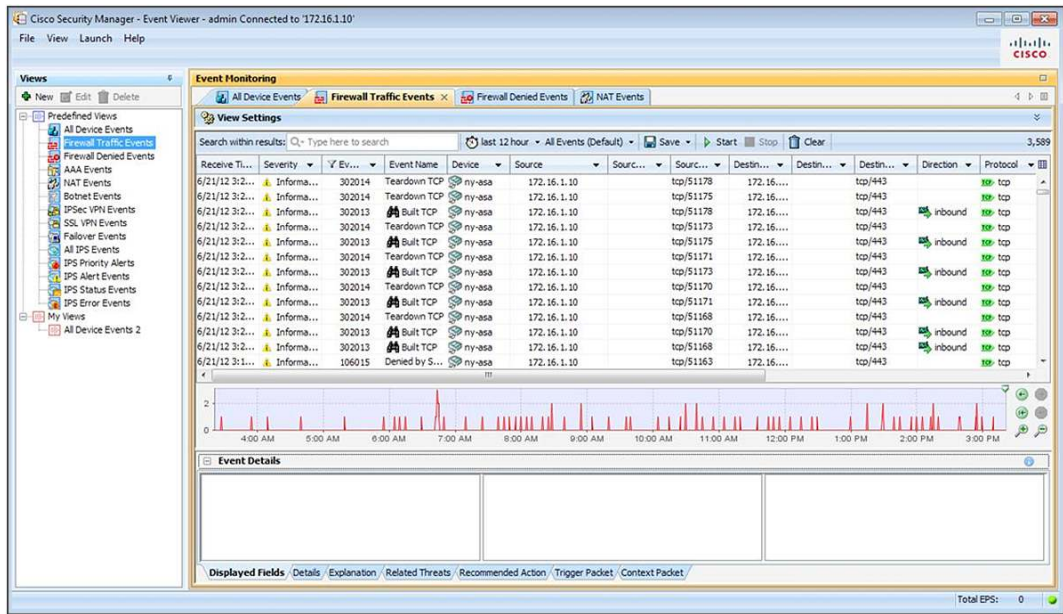
Figure 1. Security Policy Management with Cisco Security Manager 4.3

Event Management and Troubleshooting

Integrated event management helps enable viewing of real-time and historical events for rapid incident analysis and troubleshooting, and provides rapid navigation from events to source policies. In addition, advanced filtering and search capabilities enable administrators to quickly identify and isolate interesting events. Cross-linkages between the Event Manager and Configuration Manager reduce troubleshooting time for firewall rules, as well as for IPS signatures. (see Figure 2).

Figure 2. Event Management and Troubleshooting with Cisco Security Manager

The Event Manager in Cisco Security Manager provides:

- Support for syslog messages created by Cisco ASA appliances, the Cisco Firewall Services Module (FWSM), and Cisco Catalyst 6500 Series ASA Services Module, as well as Security Device Event Exchange (SDEE) messages from Cisco IPS sensors
- Real-time and historical event viewing
- Cross-linkages to firewall access rules and IPS signatures, for quick navigation to the source policies
- A prebundled set of views for firewall, IPS, and VPN
- Customizable views for monitoring select devices or a select time range
- Intuitive GUI controls for searching, sorting, and filtering events
- Administrative options to turn event collection on or off for select security devices
- Tools such as ping, traceroute, and packet tracer for further troubleshooting capabilities

More information on event management for multivendor environments, event correlation, and historical event analysis is available at: http://www.cisco.com/go/securitypartners.

Reporting

Cisco Security Manager (Figure 3) generates detailed system reports based on events and other essential information gathered from throughout the security deployment. Table 1 lists the available system reports. In addition, administrators can define and save predefined reports to meet specific reporting needs. Whether system-generated or predefined, all reports can be exported and scheduled for email delivery as PDF or CSV files.

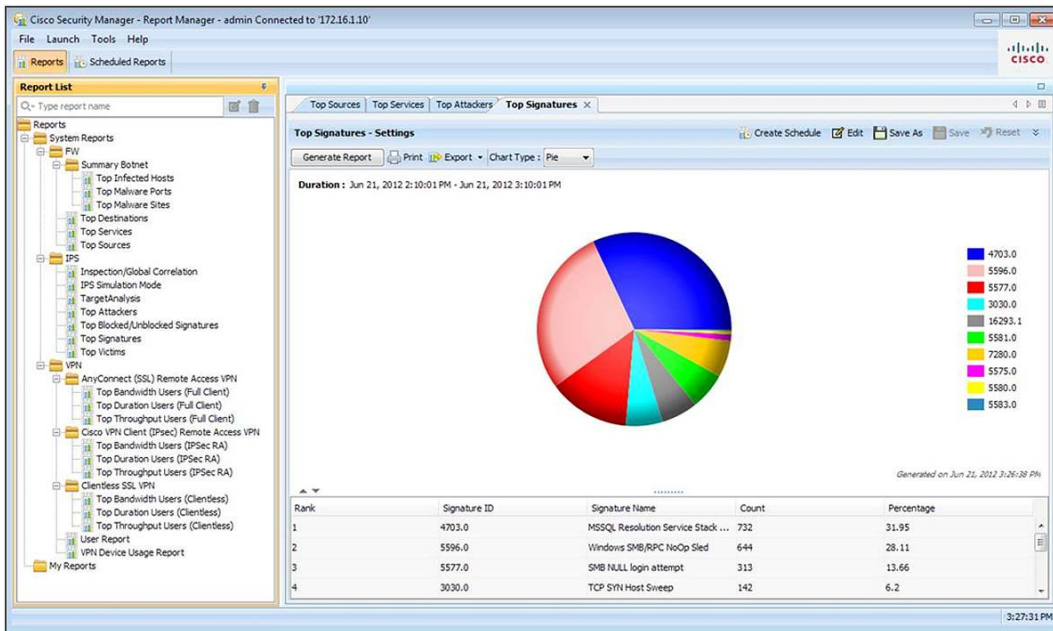**Figure 3.**   Report Manager in Cisco Security Manager
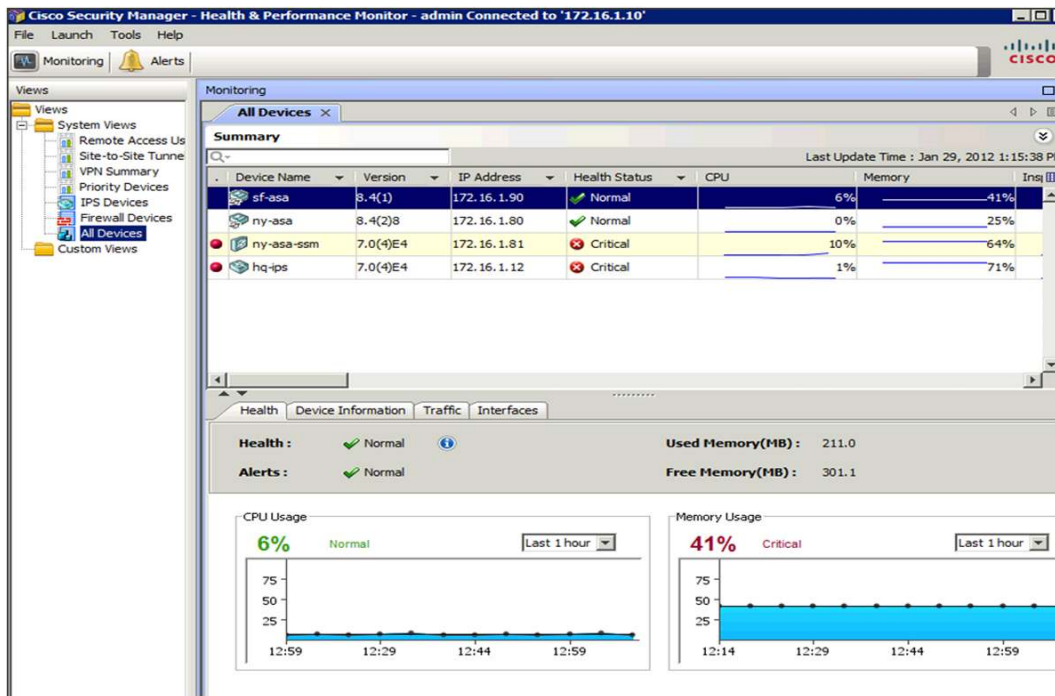

Table 2.   Cisco Security Manager System Reports

Firewall	IPS	VPN
• Top Infected Hosts	• Inspection/Global Correlation	• Top Bandwidth Users (SSL/IPsec)
• Top Malware Ports	• IPS Simulation Mode	• Top Duration Users (SSL/IPsec)
• Top Malware Sites	• Target Analysis	• Top Throughput Users (SSL/IPsec)
• Top Destinations	• Top Attackers	• User Report
• Top Services	• Top Blocked/Unblocked Signatures	• VPN Device Usage Report
• Top Sources	• Top Signatures	
	• Top Victims	

Health and Performance Monitoring

The integrated Health and Performance Monitor can help administrators increase their productivity by continuously analyzing the security environment and sending alerts when preset thresholds are reached. Customizable alert notifications can be set for such events as critical firewall failover, IPS sensor application failures, or excessive CPU or memory utilization.

Using a simple color-coded interface, administrators can immediately identify any devices that are in critical condition, and view commonly monitored attributes (for example, CPU or memory utilization) to rapidly ascertain the general health and performance of all devices across the security deployment. Detailed charts can be used to gain additional insights regarding health, traffic, and performance metrics of each device, as desired. Figure 4 shows the primary monitoring interface.
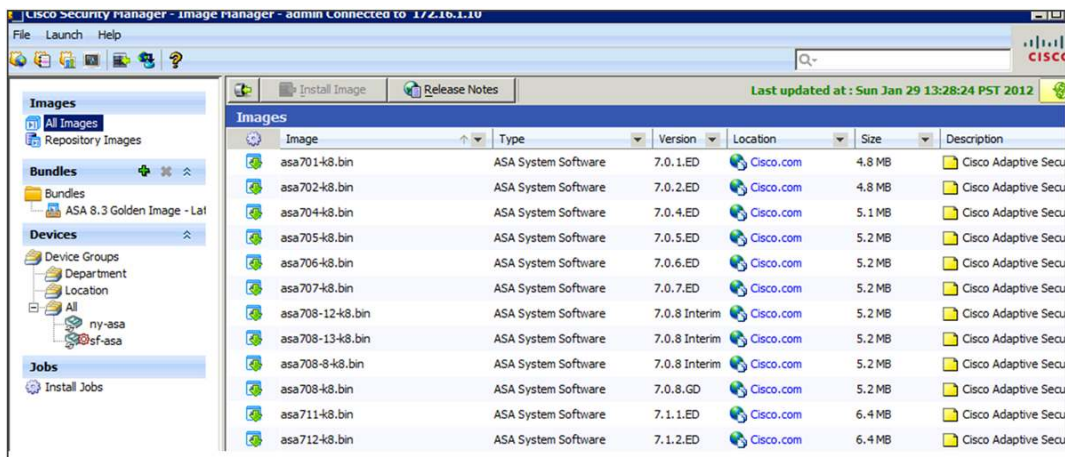
Figure 4.   Health and Performance Monitor in Cisco Security Manager

Software Image Upgrade

Firewall software images can be upgraded using an intuitive wizard. The wizard will lead administrators through the steps required to download the images, create the image bundle, and ensure that the image is appropriate for each device. The tool will then perform the backup, take the devices down, and perform the update. The updates can be performed on each firewall individually, or updates can be run in groups to maximize speed and efficiency. The process is automated, so it can be run overnight or during noncritical times to minimize disruption to the operating environment. Figure 5 shows the primary image management interface of Cisco Security Manager.

Figure 5.   Software Image Upgrade in Cisco Security Manager

API-Based Access to Cisco Security Manager

API-based access enables Cisco Security Manager to securely share information with other essential network services such as compliance and advanced security analysis systems to streamline their security operations and compliance. Using representational state transfer, external firewall compliance systems can directly request access to data from any security device managed by Cisco Security Manager.

Technical Specifications

Detailed hardware specifications and sizing guidelines for Cisco Security Manager 4.3 are available at: http://www.cisco.com/go/csmanager.

Device Support

Table 2 summarizes the device product families supported by Cisco Security Manager 4.3. For a detailed list, including supported device software versions, see "Supported Devices and OS Versions for Cisco Security Manager 4.3" at: http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html.

Table 3.   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 G2 (including 1900, 2900, and 3900 Series)
Cisco ASR 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)
Cisco Catalyst 6500 Series VPN Services Modules (VPN SMs)
Cisco 7600 Series/Catalyst 6500 Series IPsec VPN Shared Port Adapters (VPN SPAs)
Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2 (IDSM-2)
Cisco IPS 4200 Series Sensors
Cisco AIP-SSM for Cisco ASA 5500 Series
Cisco AIP-SSC for Cisco ASA 5500 Series
Cisco IPS AIM for Integrated Services Routers
Cisco IPS Module for Access Routers Network Module - Cisco Intrusion Detection System (NM-CIDS)
Cisco Catalyst 3550, 3560, 3560E, 3750, 3750 Metro, 4500, 4948, and 4948 10 Gigabit Ethernet Switches

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 Security Manager Standard Edition
Cisco Security Manager Professional Edition

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.

- **Cisco Security Intelligence Operations (SIO)** provides a central location for early warning threat and vulnerability intelligence and analysis**,** Cisco IPS signatures, and mitigation techniques. Visit and bookmark Cisco SIO 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 Software Application Support (SAS) Service** keeps Cisco Security Manager up and running with around-the-clock access to technical support and software updates.
- **Cisco Security Optimization Service** helps organizations maintain peak network health. The network infrastructure is the foundation of an 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.

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

- Unlimited access to the Cisco Technical Assistance Center (TAC) for award-winning support. Technical assistance is provided by Cisco software application experts trained in Cisco security software applications. Support is available 24 hours a day, 7 days a week, 365 days a 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 4.3, visit http://www.cisco.com/en/US/products/ps6498/index.html**Error! Hyperlink reference not valid.**, or contact your

account manager or a Cisco Authorized Technology Provider. You may also send an email to ask-csmanager@cisco.com.

Printed in USA
C78-711505-00   07/12