

Cisco Security Manager 4.1: Integrated Security Management for Cisco Firewalls, IPS, and VPN Solutions

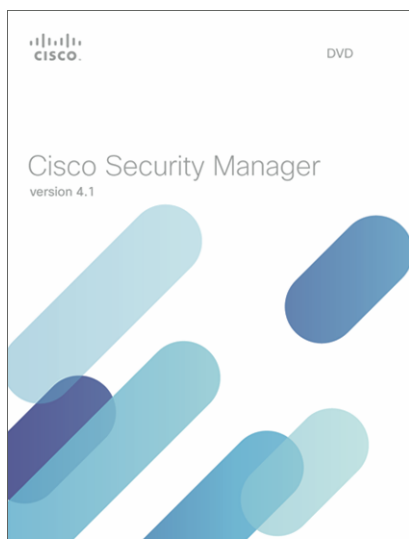
Security Operations Challenges

Businesses are facing daunting new challenges in security operations. The confluence of a growing number of security technologies, with the reduction and redirection of IT headcount once dedicated to security management has resulted in a very challenging operational environment. Security professionals have been stretched to the point where human error now frequently results in security exposure and incidents. Integrated end-to-end tools that enable consistent policy enforcement and quick troubleshooting of security events, in addition to providing summarized reports about the security deployment, are invaluable to operations teams.

Cisco Security Manager Overview

Cisco® Security Manager (CSM) (Figure 1) enables enterprises to manage and scale security operations efficiently and accurately. CSM integrates a powerful suite of capabilities, including policy and object management, event management, reporting, and troubleshooting, which are essential to maintaining security posture in today's ever changing threat environment. Cisco Security Manager supports a range of security solutions, including Cisco ASA 5500 Series Adaptive Security Appliances, Cisco IPS 4200 Series Sensor Appliances, Cisco Secure Routers and the Cisco AnyConnect Secure Mobility Client.

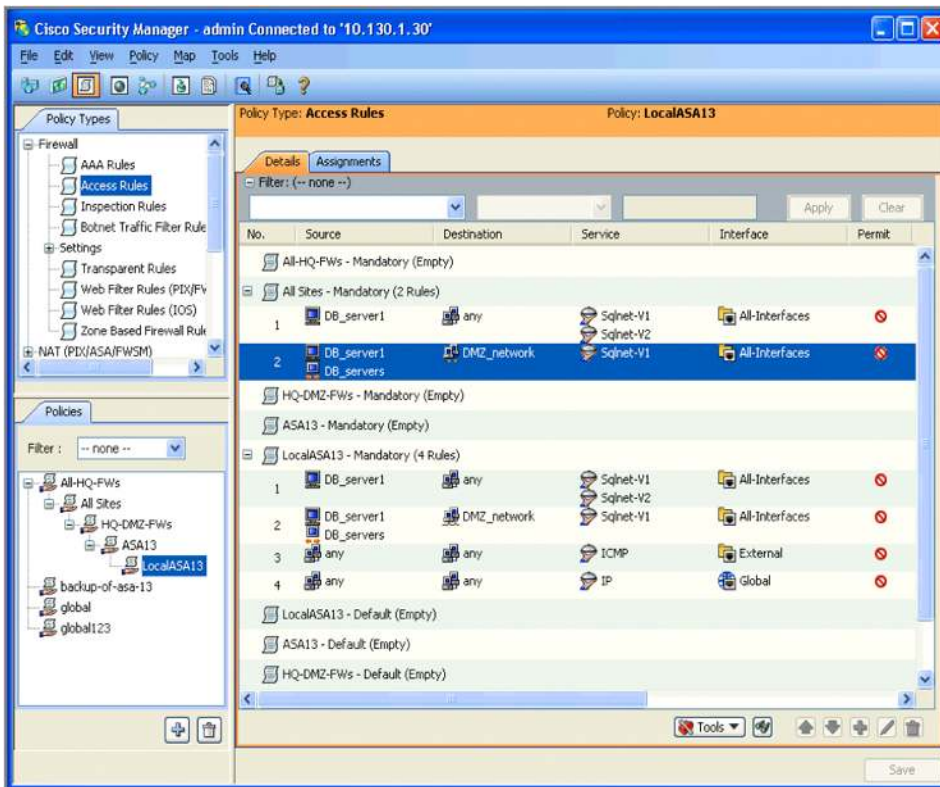
Figure 1. Cisco Security Manager Overview



Security Policy Management

Security administrators can create reusable network objects such as network addresses and services, which are defined once and used any number of times. CSM also allows policies to be defined once and shared across devices. This minimizes errors associated with manual entry of data, and makes the management of security objects and policies more efficient. Administrators can implement both on-demand and scheduled security deployments, and roll back to a previous configuration, if required. Role-based access control and deployment workflows help ensure that compliance processes are followed. See Figure 2.

Figure 2. Security Policy Management



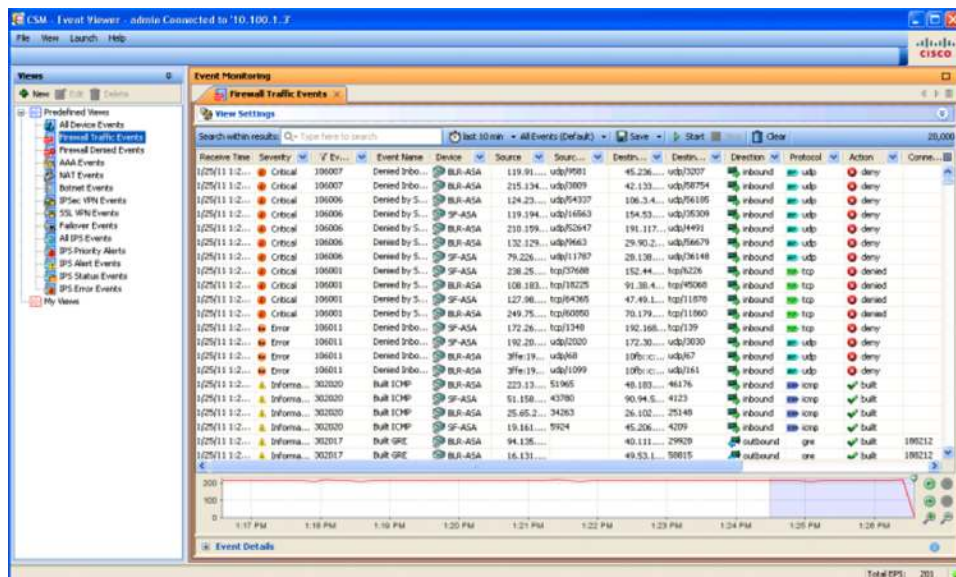
CSM also enables flexible provisioning of IPS signature updates, providing administrators with the ability to incrementally provision new and updated signatures, create IPS policies for those signatures, and then share the policies across devices. Additionally, insight into the Cisco Security Research team's IPS recommendations allows administrators to fine-tune their environment, prior to deploying signature updates. These features allow security teams to significantly cut the amount of time spent on manual tasks, while reducing errors and optimizing their security environment.

- Policy and object sharing enables security rules and objects to be reused
- RBAC and workflow ensures error-free deployments and process compliance
- Flexible deployments and rollback capabilities provide administrators the tools to efficiently implement defined policies
- Provisioning of IPS signature updates and access to Cisco SIO enhance the ability of security teams to keep up with ever-growing security threats

Event Management and Troubleshooting

Integrated event management provides administrators with real-time incident analysis and rapid troubleshooting, while advanced filtering and search capabilities enable them to quickly identify and isolate interesting events. Cross-linkages between the event manager and configuration manager reduce troubleshooting time for firewall rules and IPS signatures. See Figure 3.

Figure 3. Event Management and Troubleshooting



The CSM Event Viewer provides:

- Support for syslog messages created by Cisco ASA appliances, Cisco Firewall Services Module (FWSM), 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
- A pre-bundled 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 eventing for multi-vendor environments, event correlation, and historical event analysis is available at <http://www.cisco.com/go/securitypartners>.

Reporting

CSM 4.1 includes a new report manager, which generates system reports from events received by CSM, and displays them as either charts or data grids. It also allows administrators to define and save custom reports using advanced report criteria, to meet their specific reporting needs. All report data and charts can be exported to PDF and Excel, and they can be scheduled for email delivery as PDF or CSV files. See Figure 4 and Table 1 for a list of system reports.

Figure 4. Reporting

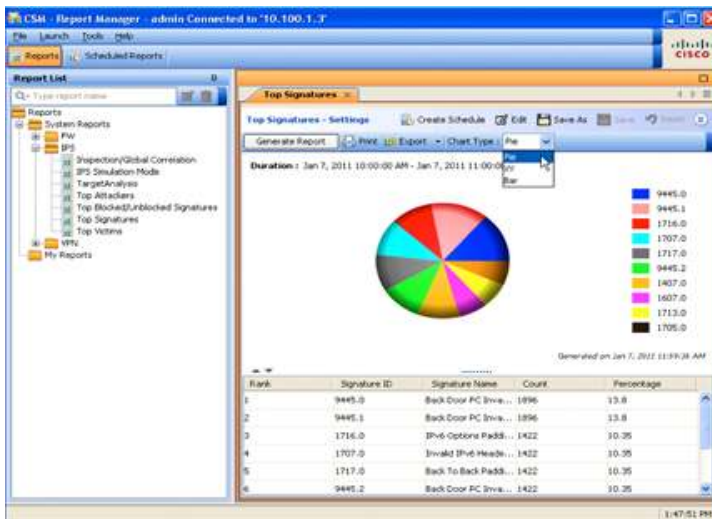


Table 1. System Reports

Firewall	IPS	VPN
<ul style="list-style-type: none"> • Top Infected Hosts • Top Malware Ports • Top Malware Sites • Top Destinations • Top Services • Top Sources 	<ul style="list-style-type: none"> • Inspection/Global Correlation • IPS Simulation Mode • Target Analysis • Top Attackers • Top Blocked/Unblocked Signatures • Top Signatures • Top Victims 	<ul style="list-style-type: none"> • Top Bandwidth Users (SSL/IPsec) • Top Duration Users (SSL/IPsec) • Top Throughput Users (SSL/IPsec) • User Report • VPN Device Usage Report

Cisco Security Manager Use Cases

Table 2. Cisco Security Manager Primary Use Cases

Feature	Benefit
Firewall Management	<ul style="list-style-type: none"> • Powerful object and rule sharing capabilities enable administrators to efficiently and consistently maintain their firewall estate • Innovative 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 • To ease configuration, device information can be imported from a device repository or configuration file, or added in the software; additionally, firewall policies can be discovered from the device itself—this feature simplifies initial security management setup • Consumption of ASA/FWSM syslog events • System-generated and customized reports, including firewall traffic and botnet reports

Feature	Benefit
IPS Management	<ul style="list-style-type: none"> • Incremental provisioning of new and updated signatures • Insight into the Cisco IPS Security Research Team's recommended defaults allows customers to tune their environment before distributing the signature update • IPS signature policies and event action filters can be inherited and assigned to any device—all other IPS polices can be assigned to and shared with other IPS devices; IPS management also includes policy rollback, a configuration archive, and cloning or creation of signatures • IPS update administration and IPS subscription licensing updates allow users to manage IPS software, signature updates, and licensing based on local and shared polices • Consumption and viewing of IPS SDEE events • System and custom IPS reports, including top attackers, top signatures
Site-to-Site VPN Management	<ul style="list-style-type: none"> • Easy configuration of site-to-site, hub-and-spoke, full-mesh, and extranet VPNs • Support for Group Encrypted Transport VPN (GET VPN), Dynamic Multipoint VPN (DMVPN), and Generic Routing Encapsulation (GRE) • Support for a variety of site-to-site IPsec VPN configurations, including dynamic IP, hierarchical certificates, and preshared keys • Extranet IPsec VPN support for establishing tunnels to partner networks and third party devices
Cisco AnyConnect Management	<ul style="list-style-type: none"> • Enables large scale Cisco AnyConnect deployments via policy sharing across multiple ASAs • Supports advanced configurations of Cisco Secure Desktop • Provisioning of IPsec Remote Access and SSL VPNs • Multiple system reports tailored for remote access administration

Technical Specifications

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

Device Support

Table 3 summarizes the device product families supported by Cisco Security Manager. For a detailed list, including supported device software versions, see "Supported Devices and OS Versions for Cisco Security Manager 4.1" at http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html.

Table 3. Highlights of Security Solutions Supported by Cisco Security Manager

Device Support Highlights
Cisco ASA 5500 Series Adaptive Security Appliances
Cisco IPS Sensors
Cisco Catalyst 6500 Series Firewall Services Module (FWSM)
Cisco AnyConnect Secure Mobility Client
Cisco Integrated Services Routers
Cisco 1000 Series Aggregation Service Routers (ASR)

Cisco Security Manager UCS Bundles

Cisco Security Manager UCS Server bundles deliver an integrated security management solution for ASA, IPS and VPN devices. The bundles include the following components for a complete, scalable security management solution:

- Cisco Security Manager 4.1 Software
- Cisco Unified Computing System C210 M2 Server
- Windows Server 2008 Enterprise R2 Operating System

All components have been pre-tested to ensure compatibility, and are purchased as a single solution – eliminating guesswork and speeding time to deployment. The Cisco Security Manager UCS Server bundles provide the following benefits:

- **Ease of Procurement:** Eliminates the delays associated with procuring separate hardware and software components from multiple vendors
- **Decreased Complexity:** Each bundle includes a UCS server with the Operating System and Cisco Security Manager pre-installed, for a comprehensive package that's guaranteed to work together
- **Reduced Time-to-Deployment:** Bundle components have been pre-tested and are purchased as a single solution – eliminating guesswork and ensuring fast, predictable deployment of network security management at a competitive price point

Ordering Information

A summary of licensing options is provided in Table 4. For complete ordering details please refer to the Cisco Security Manager 4.1 Product Bulletin at <http://www.cisco.com/go/csmanager>.

Table 4. Summary of Licensing Options for the Cisco Manager 4.1

Cisco Security Manager Standard Edition	
L-CSMST5-4.1-K9	Cisco Security Manager 4.1 Standard—5 Device Limit
L-CSMST10-4.1-K9	Cisco Security Manager 4.1 Standard—10 Device Limit
L-CSMST25-4.1-K9	Cisco Security Manager 4.1 Standard—25 Device Limit
Cisco Security Manager Professional Edition	
L-CSMPR50-4.1-K9	Cisco Security Manager 4.1 Professional with 50 Device License
L-CSMPR100-4.1-K9	Cisco Security Manager 4.1 Professional with 100 Device License
L-CSMPR250-4.1-K9	Cisco Security Manager 4.1 Professional with 250 Device License
Cisco Security Manager Incremental Device Licenses	
L-CSMPR-LIC-50	Cisco Security Manager Pro—Incremental 50 Device License
L-CSMPR-LIC-100	Cisco Security Manager Pro—Incremental 100 Device License
L-CSMPR-LIC-250	Cisco Security Manager Pro—Incremental 250 Device License
Cisco Security Manager UCS Server Bundles	
CSM4-UCS1-50-K9	Cisco Security Manager UCS Server bundle to manage 50 devices
CSM4-UCS1-150-K9	Cisco Security Manager UCS Server bundle to manage 150 devices

Note: The Incremental Device Licenses are only available to customers who have bought the 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.

- **Cisco Security Intelligence Operations (SIO) Service** provides a central location for early warning threat and vulnerability intelligence and analysis, Cisco IPS signatures, and mitigation techniques.
- **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 minor software releases.
- **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.

For More Information

For more information about Cisco Security Manager 4.1 or Cisco Security Manager UCS Server bundles, visit <http://www.cisco.com/go/csmanager>, or contact your account manager or a Cisco Authorized Technology Provider.

Related Products and Services

For more information about Cisco Security please visit the links below:

- Cisco ASA 5500 Series Adaptive Security Appliances
<http://www.cisco.com/go/asa>
- Cisco Intrusion Prevention System
<http://www.cisco.com/go/ips>
- Cisco AnyConnect Secure Mobility Client
<http://www.cisco.com/go/anyconnect>
- Cisco Security Intelligence Operations
<http://www.cisco.com/security>
- Cisco Advanced Services for Security
http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International 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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

Printed in USA

C78-647451-02 08/11