Cisco Security Manager 3.1

Q. What is Cisco Security Manager?

A. The Cisco® Security Manager application centrally provisions all aspects of device configurations and security policies for firewalls, VPNs, and intrusion prevention system (IPS) devices. It also supports advanced settings that are not strictly related to security, such as quality of service (QoS) routing and Simple Network Management Protocol (SNMP).

Cisco Security Manager is part of the Cisco Security Management Suite, which also includes Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) for monitoring and mitigation.

Q. What's new in Cisco Security Manager 3.1?

A. Cisco Security Manager 3.1 includes several new features, listed below.

- **Native IPS management**

  No more cross-launch of the Management Center for IPS: all IPS management can be done natively in Cisco Security Manager, using the same interface as other components

- **VPN discovery**

  Existing IP Security (IPsec) VPNs on the network can be imported into Cisco Security Manager

- **SSL VPN configuration support on both Cisco ASA and Cisco IOS Software-based appliances**

  You can use the Cisco Security Manager wizard to quickly configure SSL VPN. Full customization is also provided for advanced users

- **Device manager cross-launch**

  Now you can launch embedded read-only device managers (Cisco Router and Security Device Manager [SDM], Cisco Adaptive Security Device Manager [ASDM], Cisco IDS Device Manager, and Cisco IDS Event Viewer) directly on Cisco Security Manager to check device status and view security events. You can even correlate the events back into Cisco Security Manager to see which rule triggered the events.

- **Native Cisco Catalyst 6500/7600 Series management and ACL configuration**

  All VLAN/VLAN group management is now natively built into Cisco Security Manager, so there is just one stop for configuring interfaces, VLANs, groups for the FWSM, and virtual contexts. You can also configure Layer 3 access control lists (ACLs) and VLAN ACLs on this tool, or even configure your services modules.

- **Inventory report with device status**

  The inventory report shows the managed devices, OS version, policies, etc. You can also see the device status when integrated with MCP(Monitoring Center for Performance). The report is also available in PDF.

- **Detailed activity report**

  This report provides detailed information, including the exact changes users made in their configuration task, down to the atomic configuration fields. The report is also provided in PDF format.

- **High availability**

  Cisco Security Manager 3.1 supports high availability and disaster recovery deployment configurations by using Symantec VERITAS software solutions. Cisco includes a detailed high availability and disaster recovery installation guide for Cisco Security Manager 3.1 and agent software for VERITAS Cluster Server at no extra charge. Customers are responsible for obtaining the necessary VERITAS software.

- **Rule table enhancements, folders, and local rules**

  The most frequently used component in Cisco Security Manager, rule table, has been enhanced to help users gain more efficiency out of day-to-day operations.

- **Rule combiner**

  The rule combiner automatically combines rules and reduce the total number of rules on the table.

- **Advanced Cisco IOS Software interface and platform settings discovery**

  Cisco Security Manager 3.1 offers more configuration support for Cisco IOS Software-based platforms.

- **Management protocol connectivity test**

  Users can test the network connectivity and credentials before actually importing the devices from the live network.

- **Support for Cisco ASA Software 7.2; the Cisco ASA 5505 Adaptive Security Appliance; Cisco Firewall Services Module 3.2; AIM III; Cisco IPS Sensor Software 6.0; Cisco IOS IPS 5.0**

Q. What versions of Cisco IPS Sensor Software does Cisco Security Manager 3.1 support?

A. Cisco Security Manager supports Cisco IPS Sensor Software Versions 5.1 and 6.0, and supports Cisco IOS IPS Release 12.4(11)T2 and later.

Q. What versions of Cisco IPS Sensor Software can Cisco Security Manager use to update IPS signatures?

A. While Cisco Security Manager provisions Cisco IPS Sensor Software Version 5.1 and later, signature updates are only viable on Cisco IPS Sensor Software 5.1(5)E1, 6.0(1)E1 or later.

Q. What are the new features in Cisco Security Manager 3.1 relative to IPS management?

A. Cisco Security Manager 3.1 fully integrates IPS management while adding support for Cisco IPS Sensor Software Version 6.0 and Cisco IOS IPS Release 12.4(11)T2. Cisco Security Manager significantly reduces deployment times of IPS signature updates and IPS-based policies. It adds extensive usability by including a new signature update wizard that allows insight and editing of signature updates before deployment.

Q. What is provided with Cisco Security Manager 3.1?

A. Cisco Security Manager 3.1 includes the following applications:

- Cisco Security Manager 3.1 for managing firewall, VPN, and IPS technologies

- The Auto Update Server 3.1 application for pull-based software and configuration deployments
- The CiscoWorks Monitoring Center for Performance 3.1 application for health and performance monitoring of Cisco network devices and security services
- The CiscoWorks Resource Manager Essentials (RME) 4.0.5 application for performing detailed inventory management, software image management, and change audits
- The CiscoWorks Common Services 3.0.5 framework, providing functions such as authentication, authorization, accounting (AAA) and common device repository and grouping services

Q. What are the features and benefits of Cisco Security Manager?

A. A summary of the features and benefits of Cisco Security Manager are provided in the Cisco Security Manager data sheet, available at http://www.cisco.com/go/csmanager.

Q. What security devices and platforms are supported?

A. Cisco Security Manager supports the following devices:

- Cisco PIX® security appliances
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco integrated services routers
- Cisco Catalyst® 6500 Series Firewall Services Module (FWSM)
- Cisco Catalyst 6500 Series VPN Services Module and VPN Shared Port Adapter
- Cisco Catalyst 6500 Series IDS Services Module 2 (IDSM2)
- Cisco IPS 4200 Series Sensors
- Cisco IPS Module for Access Routers

For a full list of device and software versions supported by Cisco Security Manager, refer to the document entitled “Supported Devices and OS Versions for Cisco Security Manager 3.1.” This document is available at http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html.

Q. What operating systems are supported by the server?

A. The Cisco Security Manager server software can be installed on Microsoft Windows 2000 and Windows 2003. A detailed listing of the supported server and client operating systems, as well as server and client hardware requirements, can be found in the Cisco Security Manager 3.1 Installation Guide, available at http://www.cisco.com/go/csmanager under Install and Upgrade, and then under Install and Upgrade Guides.

Q. What monitoring does Cisco Security Manager provide?

A. If you have Cisco Security Manager and a service contract, you can download the CiscoWorks Monitoring Center for Performance application, which provides health and performance monitoring of Cisco network devices and security services.

Cisco Security Manager software does not include security event monitoring. Customers should consider using Cisco Security MARS, which provides a comprehensive solution to identify, manage, and counter security threats. For more information on Cisco Security MARS, go to http://www.cisco.com/go/mars.

Q. Does Cisco Security Manager have integration points with Cisco Security MARS?

A. Cisco Security MARS can display the corresponding firewall rules related to a syslog message received from the firewall device. Cisco Security MARS accomplishes the display of the rules by performing a query using HTTPS to Cisco Security Manager for the rules information. This integration feature is available with Cisco Security MARS 4.2 and beyond.

Q. How is Cisco Security Manager licensed and priced?

A. As with Cisco Security Manager 3.0, Cisco Security Manager 3.1 is priced based on the number of devices that will be managed and whether management for Cisco Catalyst 6500 Series services modules is required. Cisco Security Manager 3.1 has three base versions:

- Cisco Security Manager Enterprise Edition (Standard-5)
- Cisco Security Manager Enterprise Edition (Standard-25)
- Cisco Security Manager Enterprise Edition (Professional-50)

The Standard versions provide support for 5 and 25 devices, respectively. The Professional version includes support for 50 devices and supports additional device license packages available in increments of 50, 100, 500, and 1000 devices. The Professional version includes support for the management of Cisco Catalyst 6500 Series Switches and associated services modules; the Standard versions do not include this support.

More details on the Cisco Security Manager licensing model and specific product part numbers can be found in the Cisco Security Manager 3.1 product bulletin, available at http://www.cisco.com/go/csmanager.

Q. Can Cisco Security Manager be used with device managers?

A. Cisco recommends using a single tool to configure a device to avoid conflicts in configurations. However, Cisco Security Manager can detect any out-of-band changes on a device during deployment. At that point, users can choose to stop the deployment, overwrite the out-of-band changes, or import the newly discovered device configuration. Cisco Security Manager 3.1 also embeds the read-only device managers just for monitoring purposes, so that users can check device health and welfare status or look at the events logging on per device basis.

Q. What backup and restore functions are available?

A. Backup and restore functions are provided for the Cisco Security Manager server. In addition, Cisco Security Manager can keep historical copies of device configurations. A rollback is possible to any previously archived configuration on a per-device basis (but rollback for a policy is not supported in this release). The rollback of the last job activity is also possible. High-availability capability is also provided in Cisco Security Manager 3.1 for local cluster or remote data replication.

Q. Can Cisco Security Manager configure MPLS VPNs?

A. Cisco Security Manager can configure firewalls, IPsec VPNs, and basic routing and virtual routing and forwarding (VRF)-aware security features, but cannot configure Multiprotocol Label Switching (MPLS) VPNs.

Q. Is Cisco Security Manager suitable for managed security service providers?

A. Cisco Security Manager has a primary focus on the enterprise market rather than the managed security service provider market. However, there are some enterprise features in Cisco Security Manager that could be valuable for MSSPs. These include role-based access

control (RBAC), which is the ability to create user-defined groups of devices with access controls and workflow with tracking of approvals.

Q. Does Cisco Security Manager integrate with third-party products?

A. There are no exposed APIs that can be used by third-party vendors in this release.

Q. Can I export configuration data?

A. Cisco includes a relational database at no additional cost to store the configuration data. There is no export capability for this data. There is a configuration archive where you can see all previously detected configurations on a device. It is possible to manually cut and paste from this archive into a file.

Q. What RBAC is supported in Cisco Security Manager?

A. RBAC is supported through Cisco Secure Access Control Server (ACS). It is necessary to run Cisco Secure ACS 3.1 or higher. The user can define groups of users, devices, and rights; these three variables can be combined any way you like.

Q. Can I install Cisco Security Manager 3.1 on the same server as CiscoWorks LAN Management Solution (LMS) 2.5?

A. We recommend a dedicated server for Cisco Security Manager 3.1. Coexistence on the same server is not supported.

Q. Is Cisco Security Manager supported with VMware?

A. Cisco Security Manager may work with VMware. However, it is not rigorously tested or supported by Cisco.

Q. Does Cisco Security Manager 3.1 support high availability? How?

A. Cisco Security Manager 3.1 supports high availability and disaster recovery deployment configurations by using Symantec VERITAS software solutions. A variety of configurations are possible that can be tailored to meet the customer's availability and recovery objectives as well as budget constraints. Cisco includes a detailed high availability and disaster recovery installation guide for Cisco Security Manager 3.1 and agent software for VERITAS Cluster Server at no extra charge. Customers are responsible for obtaining the necessary VERITAS software.

Q. Will Cisco Security Manager 3.1 pricing be different from earlier versions?

A. No. The pricing will remain the same for Cisco Security Manager 3.1.

Q. Is there one part number I can use to order Cisco Security MARS and Cisco Security Manager together?

A. There is no single part number you can use to order both products. You now have the flexibility to order and deploy each product independently, according to the specific needs of your network. You can choose the optimum number of Cisco Security Manager device licenses and optimum size of Cisco Security MARS appliance to meet your network sizing requirements.

The products are designed to be interoperable.

Q. How does Cisco Security Manager compare with the Cisco Configuration Assurance Solution?

A. Cisco Security Manager is optimized for configuration management of security services such as firewall, VPN, and intrusion protection system (IPS) on Cisco network devices. The Cisco Configuration Assurance Solution focuses on auditing the compliance of device configurations

according to your established regulatory and IT governance requirements. As such, the audit and compliance-management features of the Cisco Configuration Assurance Solution greatly complement the configuration management features of Cisco Security Manager. For further information about the Cisco Configuration Assurance Solution please visit http://www.cisco.com/en/US/products/ps6364/index.html.

Q. What is the support offering for Cisco Security Manager?

A. Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, please visit http://www.cisco.com/go/services/security.

Cisco Security Manager software is eligible for technical support service coverage under Cisco Software Application Support (SAS). 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 datasheets, 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 specifics on sales migration options, please refer to the Cisco Security Manager 3.1 product bulletin, available at http://www.cisco.com/go/csmanager.

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.

Printed in USA C67-401649-00 4/07

