Q&A

Cisco Security Manager 3.0

Q. What is Cisco Security Manager?

A. Cisco® Security Manager 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 (MARS) for monitoring and mitigation.

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. See the information later in this document on how the two products can integrate.

Q. What is provided with Cisco Security Manager 3.0?

A. Cisco Security Manager includes the following applications:

- The Cisco Security Manager 3.0 for managing Firewall, VPN and IPS technologies
- The Auto Update Server 3.0 application for pull-based software and configuration deployments
- The CiscoWorks Monitoring Center for Performance 3.0 application for health and performance monitoring of Cisco network devices and security services
- The CiscoWorks Resource Manager Essentials 4.0.3 application for performing detailed inventory management, software image management, and change audits
- The CiscoWorks Common Services 3.0.3 framework, providing functions such as authentication, authorization, accounting and common device repository and grouping services

The Cisco Security Manager 3.0 media kit only includes the CiscoWorks Monitoring Center for Performance 3.0 license key and not the application itself. The application will be available for download from the Download Software link at http://www.cisco.com/go/csmanager within 90 days after the release of Cisco Security Manager 3.0.

The CiscoWorks Management Center for Cisco Security Agents software and license are not included in the Cisco Security Manager 3.0 kit. The management software for Cisco Security Agent will be available separately. For more information, visit http://www.cisco.com/go/csa.

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 3.0 Datasheet available at http://www.cisco.com/go/csmanager.

Q. What security devices 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
- Cisco Catalyst 6500 Series VPN services module
- Cisco Catalyst 6500 Series IDSM2
- Cisco IPS 4200 Series sensors
- Cisco Catalyst 6500 Series IPS services modules
- Cisco IOS IPS router sensor modules

View a detailed listing of the specific device and software versions supported in the document *Supported Devices and OS Versions for Cisco Security Manager 3.0* available at http://www.cisco.com/go/csmanager, under General Information, in Compatibility Information.

Q. What operating systems are supported by the server?

A. The Cisco Security Manager server software can be installed on 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 3.0 Installation Guide available at http://www.cisco.com/go/csmanager under Install and Upgrade, 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 the Cisco Security Monitoring, Analysis, and Response System (CS MARS), which provides a comprehensive solution to identify, manage, and counter security threats. For more information on CS 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.

Q. How is Cisco Security Manager licensed and priced?

A. In general, Cisco Security Manager 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 3.0 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 incremental device license packages available in increments of 50, 100, 500, and 1000 devices. The Professional version includes support for the management of the Catalyst 6500 and its associated services modules, while 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 3.0 Product Bulletin, available http://www.cisco.com/go/csmanager.

Q. What is the sales migration path for CiscoWorks VMS customers?

A. In general anyone with an active CiscoWorks VMS Software Application Support plus Upgrades (SASU) service contract is entitled to Cisco Security Manager with a limited device license at no charge. If you do not have a current SASU, CiscoWorks VMS-to-Cisco Security Manager upgrade part numbers will be offered at a 50 percent discount compared to the equivalent non-upgrade part numbers.

For specifics on the sales migration options, refer to the Cisco Security Manager 3.0 Product Bulletin, available at http://www.cisco.com/go/csmanager.

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 for award-winning support. Technical assistance is provided by Cisco software application experts who are trained in Cisco security software applications and 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 the sales migration options, please refer to the Cisco Security Manager 3.0 Product Bulletin, available at http://www.cisco.com/go/csmanager.

Q. What is the technical migration path for CiscoWorks VMS customers?

A. The Cisco Security Manager application supports many configuration discovery and import features, which helps recreate the management information under Cisco Security Manager.

Users can choose to perform a discovery of individual firewall devices to bring whatever is currently on the device into Cisco Security Manager as policies. Users can also choose which policy types to discover. Note, Cisco Security Manager 3.0 does not support discovery of an existing VPN configuration on the router, however, configurations can be easily recreated using the VPN wizard and then managed by Cisco Security Manager.

The CiscoWorks Management Center for IPS Sensors 3.0 and the CiscoWorks Monitoring Center for Performance 3.0 applications support data migration from their corresponding applications under CiscoWorks VMS 2.3.

Other than the above two applications, Cisco Security Manager does not support data migration for information maintained in a CiscoWorks VMS database.

CiscoWorks VMS customers operating the Sun Microsystems Solaris-SPARC platform operating system will need to switch to a Microsoft Windows compatible server or wait until a later release of Cisco Security Manager that supports a non-Windows environment.

For details on migration strategies, refer to the white paper, *Migrating from CiscoWorks VPN/Security Management Solution to Cisco Security Manager*.

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

A. Cisco recommends using a single tool to manage 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.

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.

Q. Can Cisco Security Manager configure MPLS VPNs?

A. Cisco Security Manager can configure firewalls, IP Security (IPSec) VPNs, 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 (MSSPs)?

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. What deployment enhancements are provided in Cisco Security Manager?

A. Cisco Security Manager can deploy to the device on demand or at a scheduled time. Deployments can be pushed to the actual device or to files.

Deployment to multiple devices happens not sequentially, but in parallel, using multiple threads to make updates faster.

If an error is detected during deployment to multiple devices, the user can choose to continue to deploy to the remaining devices or abort for all devices.

There is a redeploy feature in the Deployment Manager that allows for retry of failed deploys, including unreachable devices.

The user can select whether a deployment should abort if an out-of-band change is detected on the device, or can proceed with the deployment and overwrite the out-of-band change.

If a deployment is aborted due to detecting an out-of-band change, the user can choose to perform a rediscovery to bring whatever is currently on the device back into Cisco Security Manager as policies. This overwrites the policies in the software. The user can choose which policy types to rediscover.

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. In a future version, Cisco will consider providing APIs to access the database.

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 via Cisco Secure 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 3.0 on the same server as CiscoWorks LMS 2.5?

A. We recommend a dedicated server for Cisco Security Manager 3.0. 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. Can CiscoWorks Access Control List Manager (ACLM) coexist on a server with Cisco Security Manager?

A. CiscoWorks ACLM is not included with Cisco Security Manager. And ACLM cannot coexist on the same server as Cisco Security Manager for technical reasons.

However, Cisco Security Manager delivers many of the ACL management capabilities of ACLM (creating, editing and deploying ACLs on multiple Cisco devices). Furthermore, Cisco will consider adding many more ACL management capabilities in the future.

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 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

Printed in the USA C67-60015-00 01.06