

Cisco Security Manager 4.3

Q. What is Cisco Security Manager?

A. 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.

Q. Who should deploy Cisco Security Manager?

A. Cisco Security Manager is designed to meet the security management needs of small to large enterprise environments that employ Cisco security devices. 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.

Q. What's new in Cisco Security Manager 4.3?

A. Cisco Security Manager 4.3 provides several enhancements. Major new features in this release include:

- Health and performance monitoring of Cisco ASA and IPS devices, providing continuous analysis of the security environment and sending alerts when preset thresholds are reached.
- Software image upgrade, which greatly simplifies and streamlines image upgrades for individual or groups of ASA firewalls using an intuitive wizard.
- API-based access for Cisco Security Manager policy configuration data, which enables organizations to securely share information with other essential network services such as compliance and advanced security analysis systems.
- Reduction of administrative overhead in networks that have a large number of devices. Ticketing integration enables changes made in multiple ticketing systems to be easily queried for audit.
- A variety of efficiency and usability features, including: global search of devices, policies, and policy objects; search of usage information about objects; auto-conflict detection; policy object management; and support for Cisco ASA 5500-X Series midrange security appliances and Cisco IPS 4300 Series sensors.

Q. What are the image management capabilities?

A. Cisco Security Manager 4.3 introduces the capability to upgrade firewall software images directly using an intuitive wizard, instead of with CiscoWorks Resource Manager Essentials (RME). A software image repository enables images to be imported from Cisco's online software website or from the local file system. Using software bundling, downloaded images that are tested to be "good" can be grouped together such that all subsequent device upgrades can use the validated image set. All image deployments validate whether the devices have enough storage space for the new images. Cisco Security Manager understands the firewall failover pairs and deploys to the pair in a sequential manner to help ensure that either the primary or the failover device is up at all times during the upgrade process. 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.

- Q.** What are the health and performance monitoring capabilities?
- A.** Cisco Security Manager 4.3 introduces new capabilities to monitor health and performance of firewalls, intrusion prevention systems (IPSs), and VPNs. A simple color-coded interface enables quick identification of the devices that are in critical condition. Integrated sparkline charts for commonly monitored attributes (CPU, memory utilization, and so on) enable rapid identification of the health and performance trends of all the devices. Detailed charts can be used to get more information about health, traffic, and performance metrics of the devices.

Customizable alert notifications are particularly useful for enterprise-class customers monitoring a large number of security devices. Cisco Security Manager can be configured to send alerts when preset thresholds are reached. Notifications can be set for such events as critical firewall failover, IPS sensor application failures, or excessive CPU or memory utilization.

- Q.** What are the ticketing capabilities?
- A.** Cisco Security Manager 4.3 introduces the capability using with Cisco Security Manager can be loosely integrated with trouble ticketing systems such as Remedy and BMC. Administrators tagging their change sessions with a ticket identifier can track all the changes made in the session with the same ticket identifier, enabling them to be easily queried for audit.
- Q.** What are the API capabilities?
- A.** 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. Several security compliance vendors, including Tufin, AlgoSec, and Skybox, have updated their products to work with the new APIs in Cisco Security Manager.
- Q.** What kind of training is available for Cisco Security Manager 4.3?
- A.** Visit <http://www.cisco.com/go/csmanager> for Cisco Security Manager 4.3 data sheets, bulletins, and deployment guides. In addition, Cisco will provide a new learning course, as well as related online videos and webinars.
- Q.** What is the upgrade path for existing Cisco Security Manager customers?
- A.** Existing Cisco Security Manager 4.X customers with valid software support can obtain an upgrade to Cisco Security Manager 4.3. Customers with Version 3.X will first need to upgrade to Cisco Security Manager 4.0 by purchasing Cisco Security Manager 4.0 upgrade licenses. There is no direct upgrade path from Cisco Security Manager 3.X to Cisco Security Manager 4.3. The upgrade procedure from Cisco Security Manager 3.X to Cisco Security Manager 4.0 is covered in the [Cisco Security Manager 4.0 Product Bulletin](#).
- Q.** Is Cisco Security Manager 4.3 supported on VMware?
- A.** Yes. Cisco Security Manager 4.3 is supported on VMware ESX/ESXi Server 5.0.
- Q.** Does Cisco Security Manager 4.3 support Cisco ASA CX Context-Aware Security?
- A.** No. the management solution for [Cisco ASA CX](#) is [Cisco Prime™ Security Manager](#).

-
- Q.** What support options are available for Cisco Security Manager?
- A.** Cisco Security Manager is eligible for technical support service coverage under Cisco Software Application Support (SAS).

For details on Cisco SAS coverage, visit:

http://www.cisco.com/en/US/products/svcs/ps3034/ps2827/ps2993/serv_group_home.html.

Cisco Software Application Support plus Upgrades (SASU) is not available for Cisco Security Manager.

- Q.** What options are available to evaluate Cisco Security Manager?
- A.** Anybody with a valid Cisco.com account can download Cisco Security Manager and use the software for up to 90 days in evaluation mode. Visit <http://www.cisco.com/go/csmanager> and select the Download Software link.

Note: This download does not include CiscoWorks Resource Manager Essentials (RME).

- Q.** Where can I find a technical Q&A for Cisco Security Manager?
- A.** An updated version of the “FAQs and Troubleshooting Guide for Cisco Security Manager 4.X” is available at: http://www.cisco.com/en/US/products/ps6498/prod_troubleshooting_guides_list.html.

For specific recommendations on deploying Cisco Security Manager, download the latest deployment guide at: http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.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 or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: 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. (1110R)