



Guide to User Documentation for Cisco Security Manager 3.3.1

Revised: November 2, 2009

Cisco Security Manager is part of the Cisco Security Management Suite, which delivers comprehensive policy administration and enforcement for the Cisco Self-Defending Network. The suite also includes the Cisco Security Monitoring, Analysis, and Response System (MARS), which is available separately.

This document identifies and links to the various documents available for Cisco Security Manager (Security Manager), Auto Update Server (AUS), and Performance Monitor, and contains the following sections:

- [Documentation Set, page 2](#)
- [How to Get Started with Security Manager, page 4](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2009 Cisco Systems, Inc. All rights reserved.

Documentation Set

The entire documentation set for Cisco Security Manager is at http://www.cisco.com/en/US/products/ps6498/tsd_products_support_series_home.html.

**Note**

We sometimes update the documentation after initial release. Please continue to check Cisco.com for updates.

The documentation set for 3.3.1 includes:

Configuration Examples

Information about specific configuration scenarios and how they are implemented using Cisco Security Manager.

- *Applying Zone-based Firewall Policies in Cisco Security Manager*
http://www.cisco.com/en/US/products/ps6498/prod_configuration_examples_list.html
- *Migrating from 1800/2800/3800 ISRs to 1900/2900/3900 ISRs Using Cisco Security Manager 3.3.1*
http://www.cisco.com/en/US/products/ps6498/prod_configuration_examples_list.html
- *Configuring Cisco IOS Content Filtering Using Cisco Security Manager Version 3.3 in Cisco IOS Software Releases 12.4(15)XZ and Later*
http://www.cisco.com/en/US/products/ps6643/prod_white_papers_list.html

Data Sheets

Synopsis of Cisco Security Manager features and benefits, including new features.

- *Cisco Security Manager 3.3.1*
http://www.cisco.com/en/US/products/ps6498/products_data_sheets_list.html

Release Notes

Product overview, important notes, and known problems.

- *Release Notes for Cisco Security Manager 3.3.1*
http://www.cisco.com/en/US/products/ps6498/prod_release_notes_list.html

Installation and Upgrade Guides

Requirements and procedures for installing Security Manager, Auto Update Server, and Performance Monitor on a Windows server and for installing dedicated client software for Security Manager on a Windows PC. Includes pre- and post-installation guidelines and troubleshooting information.

- *Installation Guide for Cisco Security Manager 3.3.1*
http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html



Note Please refer to the *Release Notes for Cisco Security Manager 3.3.1* for important installation notes.

User Guides

Individual user guides for Security Manager, Auto Update Server, and Performance Monitor that provide conceptual and procedural information can be found at the following locations:

- *User Guide for Cisco Security Manager 3.3.1*
http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html
- *User Guide for Auto Update Server 3.3.1*
http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html
- *User Guide for Cisco Performance Monitor 3.3.1*
http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html

Online Help

Context-sensitive online help is accessible from the Help menu or by clicking the Help button on any page or dialog box.

Supported Devices Tables

Complete list of devices and software supported by Security Manager, Auto Update Server, and Performance Monitor.

- *Supported Devices and Software Versions for Cisco Security Manager 3.3.1*
http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html

Troubleshooting Guide

Frequently asked questions together with troubleshooting information. This information is generated by customer queries and developer input and is updated on an ongoing basis.

- *FAQ and Troubleshooting Guide for Cisco Security Manager 3.3.1*
http://www.cisco.com/en/US/products/ps6498/prod_troubleshooting_guides_list.html

How to Get Started with Security Manager

To get up and running quickly with Security Manager, we recommend the following:

- **Plan your installation.**

To understand which applications are available for installation and to plan your installation, we strongly recommend you begin by reviewing the installation guide overview. See the “Overview” chapter at http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.3.1/installation/guide/overv.html.

- **Get an overview of Cisco Security Manager.**

For a general product overview, see “Product Overview” at http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.3.1/user/guide/wfplan.html#wp59554.

**Tip**

For an interactive overview of Security Manager features, see the interactive JumpStart tutorial that opens when you start Security Manager for the first time. You can also access the JumpStart tutorial by selecting **Help > JumpStart**.

- **Review Getting Started checklist.**

To get up and running most efficiently, work through the “Getting Started with Security Manager” chapter at http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.3.1/user/guide/wfplan.html.

- **Define essential settings.**

Use Security Manager to define many application-wide settings that customize your working environment such as deployment method. See “Completing the Initial Security Manager Configuration” at http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.3.1/user/guide/wfplan.html#wp60179.

- **Manage user authentication and authorization.**

- To define user roles and permissions, see “Setting Up User Permissions” at http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.3.1/installation/guide/aduser.html#wp607539.
- To integrate Security Manager with Cisco Secure ACS, see “Integrating Security Manager with Cisco Secure ACS” at http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.3.1/installation/guide/aduser.html#wp607977.

- **Bootstrap your devices.**

To enable communication between Security Manager and devices, you must configure transport settings on the devices before you add them to the inventory. See the “Preparing Devices for Management” chapter at http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.3.1/user/guide/ivprep.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)