



# CHAPTER 1

## Overview

---

This chapter contains the following major sections:

- [Introduction to Component Applications, page 1-1](#)
- [Effects of Licensing on Installation, page 1-5](#)
- [Locations of Installed Files on Servers, page 1-7](#)
- [Locations of Installed Files on Client Systems, page 1-7](#)

## Introduction to Component Applications

The Security Manager installer enables you to install certain applications and, when you do, requires that you install certain other applications. This section describes those applications and their interdependencies:

- [Common Services, page 1-2](#)
- [Security Manager, page 1-2](#)
- [Auto Update Server, page 1-3](#)
- [IPS Event Viewer, page 1-4](#)
- [Resource Manager Essentials, page 1-4](#)
- [Cisco Security Agent, page 1-5](#)
- [Performance Monitor, page 1-5](#)

**Common Services**

CiscoWorks Common Services 3.1.1 (Common Services) is required for Security Manager 3.2.1, Resource Manager Essentials 4.1.1, Auto Update Server, and Performance Monitor to work. You can install Security Manager only if Common Services is already installed on your system or if you select Common Services for installation along with Security Manager.

Common Services provides the framework for data storage, login, user role definitions, access privileges, security protocols, and navigation. It also provides the framework for installation, data management, event and message handling, and job and process management. Common Services supplies essential server-side components to Security Manager that include:

- SSL libraries.
- An embedded SQL database.
- The Apache webserver.
- The Tomcat servlet engine.
- The CiscoWorks home page.
- Backup and restore functions.

For more information, see the Common Services documentation.

**Security Manager**

Cisco Security Manager is an enterprise-class management application designed to configure firewall, VPN, and intrusion prevention system (IPS) security services on Cisco network and security devices. Cisco Security Manager can be used in networks of all sizes—from small networks to large networks consisting of thousands of devices—by using policy-based management techniques. Cisco Security Manager works in conjunction with the Cisco Security Monitoring, Analysis, and Response System (MARS). Used together, these two products provide a comprehensive security management solution that addresses configuration management, security monitoring, analysis, and mitigation.

**Note** For more information about Cisco Security MARS, visit <http://www.cisco.com/go/mars>.

To use Security Manager, you must install server *and* client software.

Security Manager offers the following features and capabilities:

- Service-level and device-level provisioning of VPN, firewall, and intrusion-prevention systems from one desktop.
- Device configuration rollback.
- Network visualization in the form of topology maps.
- Workflow mode.
- Predefined and user-defined *FlexConfig* service templates.
- Integrated inventory, credentials, grouping, and shared data building blocks.
- Convenient cross-launch access to related applications.

**Auto Update Server**

If you choose to install Auto Update Server (AUS), you can install it on the same server where you install Security Manager or on a different server, such as a server in your DMZ. AUS and Security Manager can share device inventory information and other data. AUS requires Common Services 3.1.1.

AUS enables you to upgrade device configuration files and software images on PIX Security Appliance (PIX) and Adaptive Security Appliance (ASA) devices that use the auto update feature. AUS supports a pull model of configuration that you can use for device configuration, configuration updates, device OS updates, and periodic configuration verification. In addition:

- Supported devices that use dynamic IP addresses in combination with the Auto Update feature can use AUS to upgrade their configuration files and pass device and status information.
- Cisco IOS routers that use dynamic IP addresses can use AUS in combination with the CNS Gateway protocol to retrieve device IP addresses.

AUS increases the scalability of your remote security networks, reduces the costs involved in maintaining a remote security network, and enables you to manage dynamically addressed remote firewalls.

For more information, see the AUS documentation.

**IPS Event Viewer**

Cisco IPS Event Viewer (IEV) enables you to monitor as many as five individual IPS sensors in small-scale IPS deployments. Any sensor that you will monitor must be in the Security Manager inventory.

IEV installs when you install Security Manager. Its features include:

- Support for IPv6 through SDEE compatibility.
- Customizable reporting.
- Event notification through email or paging.
- Visibility into applied response actions, virtual sensor ID, learned DST OS, and threat rating.

**Note** Ethereal is a network protocol analyzer (a *packet sniffer*) for Windows that you can use to examine data from a live network or a file. The Security Manager installer *does not* install Ethereal. However, if you install Ethereal on a server where IEV is installed, you can start the Ethereal application from the IEV Tools menu to view summaries or detailed information for any packet, including the reconstructed stream of a TCP session. Also, if you have configured the sensor *capturePacket* parameter, IEV uses Ethereal to display the trigger packet. If you install IEV on a server where Ethereal is already installed, you need to specify the directory where Ethereal was installed from the IEV main menu. After you install IEV, you must reconfigure it if you install Ethereal, move the Ethereal executable file, or uninstall Ethereal. See the IEV documentation for detailed instructions.

The first time that you start IEV from Security Manager Client, important files are copied from your server to a subdirectory below the folder where you installed Security Manager Client. (These files are uninstalled when you uninstall Security Manager Client.) You can run one session at a time of IEV from a client system. However, multiple client systems can start and run sessions to one server simultaneously.

To enable communication between IEV server and IEV client, you need to modify the Cisco Security Agent or any other anti-virus and network firewall software policies on the Security Manager server to configure TCP ports 60002 and 60003 as open ports. If the server has a preexisting installation of the full Cisco Security Agent, the standalone agent is not installed on the system when you install Security Manager. In such a case, configure the Cisco Security Agent network services to accept connections on TCP ports 60002 and 60003. However, if the server on which you install Security Manager was not previously installed with the full, commercial version of Cisco Security Agent, the Security Manager installer installs a customized, standalone agent on your server and opens the necessary TCP ports for communication between IEV server and IEV client.

When you start IEV client from the Security Manager client system, IEV client automatically opens TCP port 5001 to establish communication with the IEV server.

You must configure IEV before you can use its full feature set. See the IEV documentation for detailed instructions.

**Resource Manager Essentials**

Cisco Security Manager includes the companion application Resource Manager Essentials 4.1.1 (RME).

You are licensed to use the same number of devices in RME that you license for Security Manager.

RME provides network monitoring and fault information that you can use to track devices critical to network uptime and application availability. RME also provides tools that you can use to rapidly and reliably deploy Cisco software images and view configurations of Cisco routers and switches. RME automates software maintenance to help you maintain and control your network.

RME 4.1.1 is available only as an upgrade from RME 4.1. For detailed information about installing RME, see [Chapter 7, “Installing and Upgrading RME.”](#)

**Cisco Security Agent**

Cisco Security Agent provides host-based intrusion prevention.

If the server on which you install Security Manager is *not* protected by the fully configurable, commercial version of Cisco Security Agent when you start to install Security Manager, the Security Manager installer automatically installs a customized, standalone agent on your server, with predefined policies that you cannot change. To learn about this standalone agent, see [Appendix B, “Cisco Security Agent: Standalone Agent Overview.”](#)

If the server has a preexisting installation of the full Cisco Security Agent, the standalone agent is *not* installed. In this case, we recommend that you import into your full agent version all policies that you find on the Security Manager installation DVD (in \csm3\_2\_1\_win\_server\CSA\CISMCSA3.2.1\_policies.export). If you import these policies, you must reconcile them with any conflicting policies that your organization configures. To learn more, see the Cisco Security Agent documentation on Cisco.com.

**Performance Monitor**

Cisco Security Manager includes the companion application Performance Monitor 3.2.1.

Performance Monitor monitors and troubleshoots the health and performance of services that contribute to network security. It enables you to isolate, analyze, and troubleshoot events in your network as they occur, so that you can increase service availability.

You can install Performance Monitor only after you install Common Services using the Security Manager installer, or you can choose not to install Performance Monitor. Performance Monitor has its own separate installer.

The Security Manager media kit contains a combined Software License Claim Certificate for Performance Monitor and RME. To obtain Performance Monitor, look for instructions at <http://www.cisco.com/go/csmanager>. The downloadable binary package for Performance Monitor includes detailed documentation to help you install and use the software.

## Effects of Licensing on Installation

The terms of your Security Manager software license determine many things, including the features that are available to you and the number of devices that you can manage. For licensing purposes, the device count includes any physical device, security context, virtual sensor, or Catalyst security services module that uses an IP address. Failover pairs count as one device.

When you upgrade from an earlier release, Security Manager does not prompt you for a license; instead, it retains your license and continues to enforce its terms. If you upgrade during a free evaluation, the remaining time in your evaluation period does not change.

**Note**

For complete information on the types of licenses available and the various supported upgrade paths, as well as information about the Cisco Software Application Support service agreement contracts that you can purchase, see the product bulletin for this version of Security Manager at [http://www.cisco.com/en/US/products/ps6498/prod\\_bulletins\\_list.html](http://www.cisco.com/en/US/products/ps6498/prod_bulletins_list.html).

Two license types, Standard and Professional, are available, in addition to a free 90-day evaluation period that is restricted to 50 devices.

- Security Manager has one base license file and as many other, additional licenses as you might purchase. To obtain the base license, you must have (or obtain) a Cisco.com user ID, and you must register your copy of the software on Cisco.com. When registering, you must provide the Product Authorization Key (PAK) that is attached to the *Software License Claim Certificate* inside the shipped software package.
  - If you are a registered Cisco.com user, start here:  
<http://www.cisco.com/go/license>
  - If you are not a registered Cisco.com user, start here:  
<http://tools.cisco.com/RPF/register/register.do>

After registration, the base software license is sent to the email address that you provided during registration. Keep the license in a secure location.

- Common Services does not require a license file.
- Auto Update Server does not require a license file.
- The Resource Manager Essentials license is a separate file from the Security Manager license file. For instructions on how to obtain and install the license file, see the *User Guide for CiscoWorks Common Services 3.1* at the following URL:  
[http://www.cisco.com/en/US/docs/net\\_mgmt/ciscoverks\\_common\\_services\\_software/3.1/user/guide/admin.html#wp386416](http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_common_services_software/3.1/user/guide/admin.html#wp386416).

License limits are imposed when you exceed the allotted time (in the case of the evaluation license), or the number of devices that your license allows you to manage. The evaluation license provides the same privileges as the Professional Edition license. It is important that you register Security Manager as soon as you can within the first 90 days, and for the number of devices that you need, to ensure uninterrupted use of the product. Each time you start the application you are reminded of how many days remain on your evaluation license, and you are prompted to upgrade during the evaluation period. At the end of the evaluation period, you cannot log in until you upgrade your license.

**Note**

This note applies only if you have not purchased a permanent license. If you perform an inline upgrade to Security Manager 3.2.1 from a previous version of Security Manager on your server, you must copy the 3.2.1 license file to the `..NMSROOT\etc\licenses\CSM` folder to replace the existing older license file before starting the installation of 3.2.1. This operation is necessary because the license file format has changed in Security Manager 3.2 and the format in the previous version is not compatible with 3.2. However, this issue will not affect if you are upgrading from CSM 3.2 to CSM 3.2.1.

If you do not overwrite the existing evaluation license file with the 3.2 license file, you are prompted to select a permanent license file while starting the Security Manager client after upgrade. If you have not purchased a permanent license, contact Cisco TAC to obtain a new evaluation license.

When you back up a Security Manager 3.2.1 database from one server and restore it to a different server, the validity period of the evaluation license after upgrade is retained as the same period that remained before upgrade or backup. For example, if you used Security Manager installed with an evaluation license for 10 days before upgrading to Security Manager 3.2.1, the license would be valid for only 80 days after the upgrade.

To learn how to install a license file in the Security Manager GUI, see the “Managing the Security Manager Server” chapter in the *User Guide for Cisco Security Manager 3.2.1*.

**Note**

When installing a license, you must stage the license file on a disk that is local to your Security Manager server. Security Manager does not see mapped drives if you use it to browse directories on your server. Windows imposes this limitation, which serves to improve Security Manager performance and security. For more information, log in to your Cisco.com account, then use Bug Toolkit to learn about [CSCsb43414](#).

**Getting Help with Licensing**

For licensing problems with Security Manager, contact the Licensing Department in the Cisco Technical Assistance Center (TAC):

- Phone: +1 (800) 553-2447
- E-Mail: [licensing@cisco.com](mailto:licensing@cisco.com)
- <http://www.cisco.com/tac>

## Locations of Installed Files on Servers

*NMSROOT* is the path to the Security Manager installation directory. The default is C:\Program Files\CSCOpX.

The Security Manager installer application creates and stores files on your target server. Some of those files are specific to Security Manager, while others deal with other applications.

## Locations of Installed Files on Client Systems

The Cisco Security Manager Client installer application creates and stores files on client systems. The default location for those files is C:\Program Files\Cisco Systems\Cisco Security Manager Client.

