Installation Guide for Cisco Security Manager 4.0.1

September 3, 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-23410-01
# CONTENTS

**Preface** ix  
Audience x  
Conventions x  
Product Documentation xi  
Security Manager, Auto Update Server, and Performance Monitor Documentation xi  
Related Documentation xi  
Obtaining Documentation and Submitting a Service Request xii  

## CHAPTER 1  
**Overview** 1-1  
Introduction to Component Applications 1-1  
Common Services 1-1  
Security Manager 1-2  
Auto Update Server 1-2  
Cisco Security Agent 1-3  
Performance Monitor 1-3  
Resource Manager Essentials 1-4  
Introduction to Related Applications 1-4  
Understanding Security Manager Licensing 1-5  
Licensing Overview 1-5  
Effects of Licensing on Installation and Obtaining a License 1-6  
Effect of Enabling Event Management 1-7  

## CHAPTER 2  
**Requirements and Dependencies** 2-1  
Required Services and Ports 2-1  
Server Requirements 2-3  
Understanding Regional and Language Options and Related Settings 2-6  
Client Requirements 2-7  

## CHAPTER 3  
**Preparing a Server for Installation** 3-1  
Best Practices for Enhanced Server Performance and Security 3-1  
Readiness Checklist for Installation 3-4
CHAPTER 4

Installing and Upgrading Server Applications 4-1

Understanding the Required Server User Accounts 4-1
Using Remote Desktop Connection or VNC To Install Server Applications 4-2
Installing Security Manager Server, Common Services, and AUS 4-3
Installing Performance Monitor 4-5
Installing Resource Manager Essentials (RME) 4-7

Upgrading Server Applications 4-9
Ensuring Security Manager Pending Data is Submitted and Approved 4-11
Restoring Changes that You Made to Property Files 4-11
Backing Up the Database for Remote Upgrades 4-12
Backing Up the Server Database By Using the CLI 4-12
Restoring the Server Database 4-13
Making Required Changes After Upgrade 4-14

Migrating Security Manager to a New Computer or Operating System 4-15
Updating Security Manager, Performance Monitor, and RME Licenses 4-16
Obtaining Service Packs and Point Patches 4-17
Adding Applications to the Server’s Home Page 4-18
Uninstalling Server Applications 4-18
Downgrading Server Applications 4-19

CHAPTER 5

Installing and Configuring the Client 5-1

Configuring Web Browser Clients 5-1
Configuring Internet Explorer Settings 5-2
Configuring Firefox Settings 5-3
Editing the Preferences File 5-3
Editing the Size of the Disk Cache 5-3
Disabling the Popup Blocker or Creating a White List 5-4
Enabling JavaScript 5-4
Displaying Online Help on a New Tab in the Most Recent Window and Reusing Existing Windows on Subsequent Requests 5-4
Enabling and Configuring Exceptions in Third-party Tools 5-5

Tips for Installing the Security Manager Client 5-5
Installing the Security Manager Client 5-6
Handling Security Settings That Prevent Installation 5-7
Configuring a Non-Default HTTP or HTTPS Port 5-8
Unable to Upgrade From a Previous Version of the Client 5-8
Patching a Client 5-9
Logging In to the Applications 5-9
Using Multiple Versions of Security Manager with Same ACS  7-23
Authentication Fails When in ACS Mode  7-24
System Administrator Granted Read-Only Access  7-24
ACS Changes Not Appearing in Security Manager  7-25
Devices Configured in ACS Not Appearing in Security Manager  7-25
Working in Security Manager after Cisco Secure ACS Becomes Unreachable  7-25
Restoring Access to Cisco Secure ACS  7-26
Authentication Problems with Multihomed Devices  7-26
Authentication Problems with Devices Behind a NAT Boundary  7-26

APPENDIX A

Troubleshooting  A-1

Startup Requirements for Cisco Security Manager Services  A-1
Comprehensive List of Required TCP and UDP Ports  A-2
Troubleshooting the Security Manager Server  A-4
   Server Problems During Installation  A-4
   Server Problems After Installation  A-5
   Server Problems During Uninstallation  A-8
Troubleshooting the Security Manager Client  A-9
   Client Problems During Installation  A-9
   Client Problems After Installation  A-12
Troubleshooting Bundled Cisco Security Agent  A-15
Running a Server Self-Test  A-17
Collecting Server Troubleshooting Information  A-17
Viewing and Changing Server Process Status  A-18
Restarting All Processes on Your Server  A-18
Reviewing the Server Installation Log File  A-19

APPENDIX B

Bundled Cisco Security Agent: Overview  B-1

The Basics  B-1
Understanding and Managing Security Level Settings  B-2
Uninstalling Bundled Cisco Security Agent  B-2
Cleaning Up an Unclean Agent  B-3
   Manually Removing the CSAgent Version 5.2.0.282  B-4

APPENDIX C

Open Source License Notices for Cisco Security Manager  C-1

Notices  C-1
   OpenSSL/Open SSL Project  C-2
   License Issues  C-2
Axis C-3
  License C-4
Castor C-6
  License C-7
cglib C-9
  License C-9
Velocity C-12
  License C-12
Apache Commons C-15
  Components C-15
  License C-15
ODMG C-18
  Availability C-18
  License C-18
log4j C-19
  License C-19
jdt-compiler-3.1.1.jar C-21
  License C-22
jta-1.1.jar C-25
  License C-25
slf4j-api-1.5.2.jar C-27
  License C-28
Preface

Cisco Security Manager (Security Manager) enables you to manage security policies on Cisco devices in large, medium, or small networks. You can use shareable objects and policies in Security Manager to manage thousands of devices or only a few. Security Manager also supports multiple configuration views that are optimized for different use cases, supports the provisioning of many platform-specific settings, and provides device grouping capabilities.

Note

This guide does the following:

- Lists hardware and software requirements for installing Security Manager and its related applications.
- Explains important concepts about the software applications that you select for installation and the environment in which you install them.
- Describes what you must do after installation so that you can use your newly installed applications successfully.
- Guides you in understanding and troubleshooting problems that might occur during, or as a result of, installation.

Note
Before you install the applications, we recommend that — for the most recent information — you read the release notes on Cisco.com that are most relevant to the actual software components you choose to install. The release notes might contain corrections or additions to this guide or provide other information that affects planning, preparation, installation, or deployment. See Product Documentation, page xi.
Tip
With a Cisco Self-Defending Network, security is integrated throughout the network and protects each endpoint. We recommend that you implement the best practices in the comprehensive Cisco Self-Defending Network strategy. You can learn about the Cisco Self-Defending Network at http://www.cisco.com/go/sdn.

Audience
This document is for network and security personnel who install, configure, deploy, and manage security infrastructure.

Conventions
This document uses the following conventions:

<table>
<thead>
<tr>
<th>Item</th>
<th>Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands and keywords</td>
<td>boldface font</td>
</tr>
<tr>
<td>Variables for which you supply values</td>
<td>italic font</td>
</tr>
<tr>
<td>Displayed session and system information</td>
<td>screen font</td>
</tr>
<tr>
<td>Information you enter</td>
<td>boldface screen font</td>
</tr>
<tr>
<td>Variables you enter</td>
<td>italic screen font</td>
</tr>
<tr>
<td>Menu items and button names</td>
<td>boldface font</td>
</tr>
<tr>
<td>Selecting a menu item in paragraphs</td>
<td>Option &gt; Network Preferences</td>
</tr>
<tr>
<td>Selecting a menu item in tables</td>
<td>Option &gt; Network Preferences</td>
</tr>
</tbody>
</table>

Note
Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

Caution
Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Tip
Means the following information will help you solve a problem. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.


Product Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

- Security Manager, Auto Update Server, and Performance Monitor Documentation, page xi
- Related Documentation, page xi

Security Manager, Auto Update Server, and Performance Monitor Documentation

Table 1 describes available documentation for Cisco Security Manager, Auto Update Server, and Performance Monitor in the reading order that we recommend.

Table 1  Security Manager Documentation

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Available Formats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Also covers Auto Update Server and Performance Monitor.</td>
<td></td>
</tr>
<tr>
<td>Includes support information for Auto Update Server and Performance Monitor.</td>
<td></td>
</tr>
<tr>
<td>Context-sensitive online help</td>
<td>Select an option in the GUI, then click Help.</td>
</tr>
</tbody>
</table>

Related Documentation

Table 2 identifies important documentation for Common Services 3.3 and Resource Manager Essentials 4.3.

Table 2  Documentation for Related Products

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Cisco.com URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Services Documentation</td>
<td></td>
</tr>
<tr>
<td>Document Title</td>
<td>Cisco.com URL</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Resource Manager Essentials Documentation</strong></td>
<td></td>
</tr>
<tr>
<td>Supported Device Table for LMS 3.2</td>
<td><a href="http://www.cisco.com/en/US/products/sw/cscowork/ps2425/products_device_support_tables_list.html">http://www.cisco.com/en/US/products/sw/cscowork/ps2425/products_device_support_tables_list.html</a></td>
</tr>
<tr>
<td>Supported Image Distribution Features for RME 4.3 Software Management (With LMS 3.2)</td>
<td><a href="http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html">http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html</a></td>
</tr>
<tr>
<td>Supported Image Import Features for RME 4.3 Software Management (With LMS 3.2)</td>
<td><a href="http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html">http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html</a></td>
</tr>
<tr>
<td>Supported Protocols for RME 4.3 Configuration Management (With LMS 3.2)</td>
<td><a href="http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html">http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html</a></td>
</tr>
</tbody>
</table>

**Obtaining Documentation and Submitting a Service Request**

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at this URL:


Subscribe to the *What’s New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
Overview

This chapter contains the following sections:

- Introduction to Component Applications, page 1-1
- Introduction to Related Applications, page 1-4
- Understanding Security Manager Licensing, page 1-5

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 1-1
- Security Manager, page 1-2
- Auto Update Server, page 1-2
- Cisco Security Agent, page 1-3
- Performance Monitor, page 1-3
- Resource Manager Essentials, page 1-4

Common Services

CiscoWorks Common Services 3.3 (Common Services) is required for Security Manager 4.0.1, Resource Manager Essentials 4.3, Auto Update Server 4.0, and Performance Monitor 4.0.1 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 the following:

- SSL libraries
- An embedded SQL database
- The Apache webserver
Chapter 1      Overview

Introduction to Component Applications

The Tomcat servlet engine
The CiscoWorks home page
Backup and restore functions


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.


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 policy objects
- Convenient cross-launch access to related applications:
  - When you install the server software, you also install read-only versions of the following device managers: Adaptive Security Device Manager (ASDM), PIX Device Manager (PDM), Security Device Manager (SDM), and IPS Device Manager (IDM).
  - You can configure a cross launch to RME.
  - You can collect data from Performance Monitor and display it in an inventory status window.
  - You can add ASA and PIX devices from Security Manager to Auto Update Server (AUS).
- Integrated monitoring of events generated by ASA and IPS devices. You can selectively monitor, view, and examine events from ASA and IPS devices by using the Event Viewer feature.

Auto Update Server

If you choose to install 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 uses a browser-based user interface and requires Common Services.
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.

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 about AUS you can refer to the AUS documentation located at the Security Manager site: http://www.cisco.com/go/csmanager.

Cisco Security Agent

Cisco Security Agent provides host-based intrusion prevention. Regarding Security Manager, there are two versions of Cisco Security Agent—external and bundled:

- External Cisco Security Agent—Cisco Security Agent that is not installed as part of the Cisco Security Manager installation.
- Bundled Cisco Security Agent—Cisco Security Agent that is installed as part of the Cisco Security Manager installation. Bundled Cisco Security Agent is sometimes referred to as a “customized, standalone agent” because it is customized for Security Manager and because Management Center for Cisco Security Agents is not installed; thus, it is standalone.

If the server on which you install Security Manager does not already have the external version of Cisco Security Agent installed, the Security Manager installation program takes the following actions:

- On Windows 2003 R2 Enterprise Server (Service Pack 2)—32 bit, the installation program asks you whether or not you want to install Cisco Security Agent; if you do, the Security Manager installer installs the bundled version on your server; this version has pre-defined policies that you cannot change. To learn more about this bundled version, see Appendix B, “Bundled Cisco Security Agent: Overview.”

- On Windows 2008 Enterprise Server (Service Pack 2)—32 bit and Windows 2008 Enterprise Server (Service Pack 2)—64 bit, the installation program does not install Cisco Security Agent.

If the server on which you install Security Manager does already have the external version of Cisco Security Agent installed, the installation program does not ask you whether or not you want to install Cisco Security Agent.

Performance Monitor

Cisco Security Manager includes the companion application Performance Monitor 4.0.1. Performance Monitor is a health and performance monitoring application with a special emphasis on security devices and services. Performance Monitor supports the ability to proactively detect network performance issues before they become critical; helps identify portions of the network which are overloaded and potentially require extra resources; and provides rich historical health and performance information for after-the-fact investigations and analyses. Performance Monitor supports monitoring remote-access VPNs, site-to-site VPNs, firewall, web server load-balancing, and SSL termination. Performance Monitor uses a browser-based user interface.
You can install Performance Monitor only after you install Common Services. Performance Monitor is installed by using a separate installation program, which is available after you install and then start Common Services.

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

For more information about Performance Monitor, you can refer to the Performance Monitor documentation located at the Security Manager site: http://www.cisco.com/go/csmanager.

Resource Manager Essentials

Cisco Security Manager includes the companion application CiscoWorks Resource Manager Essentials (RME). RME provides lifecycle management of Cisco network devices. To support life cycle management, RME provides the ability to manage device inventory and audit changes, configuration files, and software images as well as syslog analysis. RME uses a browser-based user interface.

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

RME is also included with the CiscoWorks LAN Management Solution (LMS). There is useful deployment information about RME included in the CiscoWorks LAN Management Solution Deployment Guide 3.0, although be aware that some information does not apply in the case of RME bundled with Security Manager. For more information, you can refer to http://www.cisco.com/en/US/partner/products/sw/cscowork/ps2073/tsd_products_support_eol_series_home.html.

Introduction to Related Applications

Other applications are available from Cisco that integrate with Security Manager to provide additional features and benefits:

- **Cisco Security Monitoring Analysis and Response System (MARS)**—Security Manager supports cross linkages between policies and events with MARS for firewall and IPS. Using the Security Manager client you highlight specific firewall rules or IPS signatures and request to see the events related to those rules or signatures. Using MARS you can select firewall or IPS events and request to see the matching rule or signature in Security Manager. These policy-event cross-linkages are especially useful for network connectivity troubleshooting, identifying unused rules, and signature tuning activities. The policy-event cross-linkage feature is explained in detail in the User Guide for Cisco Security Manager. For more information about MARS you can visit http://www.cisco.com/go/mars.

- **Cisco Secure Access Control System (ACS)**—You can optionally configure Security Manager to use ACS for authentication and authorization of Security Manager users. ACS supports defining custom user profiles for fine-grained role based authorization control and ability to restrict users to specific sets of devices. For details on configuring Security Manager and ACS integration, see Integrating Security Manager with Cisco Secure ACS, page 7-8. For more information about ACS, visit http://www.cisco.com/go/acs.
Cisco Configuration Engine—Security Manager supports the use of the Cisco Configuration Engine as a mechanism for deploying device configurations. Security Manager deploys the delta configuration file to the Cisco Configuration Engine, where it is stored for later retrieval from the device. Devices such as Cisco IOS routers, PIX Firewalls, and ASA devices that use a Dynamic Host Configuration Protocol (DHCP) server, contact the Cisco Configuration Engine for configuration (and image) updates. You can also use Security Manager with Configuration Engine to manage devices that have static IP addresses. When using static IP addresses, you can discover the device from the network and then deploy configurations through Configuration Engine. For information about the Configuration Engine releases you can use with Security Manager, see the release notes for this version of the product at http://www.cisco.com/en/US/products/ps6498/prod_release_notes_list.html. For more information about the Configuration Engine, visit http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/index.html.

Understanding Security Manager Licensing

It is important to understand Security Manager licensing when planning a deployment of Security Manager to ensure that you have the correct base license and number of device licenses for the number and type of devices you intend to manage. The following topics explain Security Manager licensing and provide some specific license examples:

- Licensing Overview, page 1-5
- Effects of Licensing on Installation and Obtaining a License, page 1-6

Licensing Overview

There are four base versions of Cisco Security Manager Enterprise Edition:

- Standard-5
- Standard-10
- Standard-25
- Professional-50

These base versions provide management for 5, 10, 25, and 50 devices, respectively.

The Professional version supports incremental device license packages available in increments of 50, 100, and 250 devices. The Professional version also includes support for the management of Cisco Catalyst 6500 and 7600 Series switches and associated services modules; the Standard versions do not include this support.

Security Manager consumes a device license when you add any of the following to the device inventory:

- Each physical device
- Each security context
- Each virtual sensor

Advanced Inspection and Prevention Security Services Modules (AIP-SSMs), IDS Network Modules, IPS Advanced Integration Modules (IPS AIM), and any other modules supported for devices other than the AIP-SSC 5 and the Catalyst 6500 or 7600 installed in the host device do not consume a license; however, additional virtual sensors (added after the first sensor) do consume a license.
In the case of a Firewall Services Module (FWSM), the module itself consumes a license and then consumes an additional license for each additional security context. For example, an FWSM with two security contexts would consume three licenses: one for the module, one for the admin context, and one for the second security context.

The following are some additional special cases you should understand with respect to device licensing:

- **Unmanaged Devices**—In Security Manager you can add unmanaged devices to the device inventory. An unmanaged device is a device for which you have deselected Manage in Cisco Security Manager in the device properties. An unmanaged device does not consume a license.

Another class of unmanaged device is an object that is added to a topology map. You can use the Map > Add Map Object command to add different types of objects on the map such as network clouds, firewalls, hosts, networks, and routers. These objects do not appear in the device inventory and do not consume a device license.

- **Active and Standby Servers**—The license allows the use of the software on a single server. A standby Cisco Security Manager server, such as used in a high-availability or disaster recovery configuration, does not require a separate license if only one server is active at any one time.

- **Licensing for RME and Performance Monitor**—Cisco Security Manager also includes a separate license file for RME and Performance Monitor. You are entitled to use these applications for the same number of devices that you have purchased for Cisco Security Manager. When you order a Security Manager base product you receive a second Product Authorization Key (PAK) for the RME and Performance Monitor license.

## Effects of Licensing on Installation and Obtaining a License

All 3.x and earlier customers need to procure a new license (or licenses) for Security Manager 4.0.1 irrespective of whether they have a valid license for any of the (older) Security Manager 3.x releases. With the exception of incremental licenses, existing Security Manager 3.x licenses are not valid for Security Manager 4.0.1

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 the most recent major release of Security Manager at 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.
Chapter 1  Overview

Effect of Enabling Event Management

- Common Services does not require a license file.
- Auto Update Server does not require a license file.
- The Security Manager media kit contains a combined Software License Claim Certificate for Performance Monitor and RME. When you register Security Manager, you should also obtain the combined license file for Performance Monitor and RME. You can install the applications from the product DVD, or you can obtain the software by going to http://www.cisco.com/go/csmanager, clicking Download Software, and downloading the applications.

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. You must 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.

To learn how to install a license file, see Updating Security Manager, Performance Monitor, and RME Licenses, page 4-16.

**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.

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
- Email: licensing@cisco.com
- http://www.cisco.com/tac

**Effect of Enabling Event Management**

If you enable Event Management on your Security Manager server, you cannot use that server for any of the following services:
- Syslog on CiscoWorks Common Services
- Syslog on CiscoWorks Resource Manager Essentials (RME)
- Syslog on Performance Monitor

During the installation or upgrade of Security Manager, the Common Services syslog service port is changed from 514 to 49514. Later, if Security Manager is uninstalled, the port is not reverted to 514. Additional information regarding ports is available in Table 2-1 on page 2-2 and in Table A-1 on page A-2.

If the amount of RAM available to the operating system is insufficient, Event Viewer is disabled (see details in Table 2-3 on page 2-4); however, the Common Services syslog service port is still changed.
CHAPTER 2

Requirements and Dependencies

You can install and use Security Manager as a standalone product or in combination with several other Cisco Security Management Suite applications, including optional applications that you can select in the Security Manager installer or download from Cisco.com. Requirements for installation and operation vary in relation to the presence of other software on the server and according to the way that you use Security Manager.

Tip

We recommend that you synchronize the date and time settings on all your management servers and all the managed devices in your network. One method is to use an NTP server. Synchronization is important if you want to correlate and analyze log file information from your network.

The sections in this chapter describe requirements and dependencies for installing server applications such as Security Manager, Auto Update Server, Performance Monitor, and RME, and Security Manager client software:

- Required Services and Ports, page 2-1
- Server Requirements, page 2-3
- Client Requirements, page 2-7

Required Services and Ports

You must ensure that required ports are enabled and available for use by Security Manager and its associated applications on your server so that the server can communicate with clients and servers running associated applications.

The ports that need to be open depend on whether you are using CiscoWorks for AAA or an external server (such as ACS), and whether you are configuring Security Manager to interact with certain other applications:

- Basic Required Ports—Table 2-1 lists the basic ports that must be opened, assuming that you have not customized your configuration to use non-default ports. If you are using CiscoWorks for AAA (user authorization) services, and you do not use any of the optional applications, these should be the only ports you need to open.
Table 2-1  Basic Required Ports to Open on the Security Manager Server

<table>
<thead>
<tr>
<th>Communication</th>
<th>Service</th>
<th>Protocol</th>
<th>Port</th>
<th>In</th>
<th>Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Manager Client to the Security Manager Server.</td>
<td>HTTP, HTTPS</td>
<td>TCP</td>
<td>1741/443</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Security Manager Client to device managers included in the product (such as ASDM).</td>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Security Manager to Cisco.com for IPS signature and engine update downloads.</td>
<td>HTTP</td>
<td>TCP</td>
<td>80</td>
<td>—</td>
<td>X</td>
</tr>
<tr>
<td>Security Manager to Cisco.com for IPS signature and engine update downloads.</td>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td>—</td>
<td>X</td>
</tr>
<tr>
<td>Security Manager Server to Devices.</td>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td>—</td>
<td>X</td>
</tr>
<tr>
<td>Security Manager Server to Device for configuration rollback operations on IOS devices.</td>
<td>TFTP</td>
<td>UDP</td>
<td>69</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Security Manager to an e-mail server.</td>
<td>SMTP</td>
<td>TCP</td>
<td>25</td>
<td>—</td>
<td>X</td>
</tr>
<tr>
<td>Syslog service used by the Security Manager Event Viewer.</td>
<td>Syslog</td>
<td>UDP</td>
<td>514</td>
<td>X</td>
<td>—</td>
</tr>
</tbody>
</table>

Tip: HTTPS and SSH ports are required, but open the Telnet port only if you use Telnet as the transport protocol for one or more devices. Because Telnet transmits passwords in clear text, we recommend that you never use Telnet, and that you do not open the Telnet port.

Table 2-2  Ports Required for Optional Server Applications

<table>
<thead>
<tr>
<th>Communication</th>
<th>Service</th>
<th>Protocol</th>
<th>Port</th>
<th>In</th>
<th>Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Manager Server to and from CS-MARS.</td>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Security Manager Server to Cisco Secure Access Control Server (ACS).</td>
<td>HTTPS, HTTPS</td>
<td>TCP</td>
<td>• If port restriction is enabled on the ACS server, allow all ports in the range for HTTP/HTTPS communication.</td>
<td>—</td>
<td>X</td>
</tr>
<tr>
<td>Security Manager Server to an External AAA Server (configurable in a non-ACS mode).</td>
<td>RADIUS, LDAP</td>
<td>Kerberos</td>
<td>1645, 1646, 1812(new), 389, 636 (SSL), 88</td>
<td>—</td>
<td>X</td>
</tr>
</tbody>
</table>

• Ports Required By Optional Applications—If you are using Security Manager with other applications, other ports also need to be opened, as shown in Table 2-2. Open only ports required by applications that you are actually using.
Table 2-2  Ports Required for Optional Server Applications (continued)

<table>
<thead>
<tr>
<th>Communication</th>
<th>Service</th>
<th>Protocol</th>
<th>Port</th>
<th>In</th>
<th>Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Manager Server to Configuration Engine.</td>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Security Manager Server to AUS.</td>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Device to AUS. Used to retrieve images and configurations.</td>
<td>HTTP</td>
<td>TCP</td>
<td>1751</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Security Manager Server to TMS Server.</td>
<td>FTP</td>
<td>TCP</td>
<td>21</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Internet browser running on a client system to the browser interface on the</td>
<td>HTTP,</td>
<td>TCP</td>
<td>1741/443</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Security Manager, AUS, RME, or Performance Monitor server.</td>
<td>HTTPS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance Monitor to device for polling.</td>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Tip: You can configure this port when importing devices. If you use a non-default port, you must open the port you use. You must use a non-default port if WebVPN is configured on the interface.

<table>
<thead>
<tr>
<th>Communication</th>
<th>Service</th>
<th>Protocol</th>
<th>Port</th>
<th>In</th>
<th>Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Monitor to device for SNMP polling.</td>
<td>SNMP</td>
<td>TCP</td>
<td>161</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Device to Performance Monitor for SNMP traps.</td>
<td>SNMP</td>
<td>TCP</td>
<td>162</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Syslog service if you use Performance Monitor or RME for syslog, and you</td>
<td>Syslog</td>
<td>UDP</td>
<td>514</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>install these applications on a separate server than Security Manager.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Server Requirements

Tip: We recommend that you install Security Manager on a dedicated server in a controlled environment. For additional best practices and related guidance, see Chapter 3, “Preparing a Server for Installation.”
To install Security Manager, you must be an Administrator or a user with local administrator rights; this also applies if you are installing the client only. Table 2-3 describes the minimum and recommended server configuration. These requirements vary based on whether you are using Security Manager for device configuration only, or for both device configuration and event management. Typically, if you use event management, you must use a more powerful server.

Unless otherwise noted, the requirements apply to all applications. For example, if you install Performance Monitor on a separate server than Security Manager, the Performance Monitor server needs to meet the configuration-only requirements.

**Recommended Server**

Cisco recommends that you install the application on a Cisco UCS C200 server with an Intel Quadcore Xeon 5500 Series CPU, 16 GB RAM, two 1 TB (minimum) hard drives, and a 1 Gbps network adapter. Use RAID 0 and partition the drives so that Windows and the Security Manager application have a 500 GB partition, and event management storage has a 1.5 TB partition.

**Do not install any application:**

- On a primary or backup domain controller. We do not support any use of Common Services on a Windows domain controller.
- In an encrypted directory. Common Services does not support directory encryption.
- If Terminal Services is enabled in Application mode. In such a case, you must disable Terminal Services, then restart the server before you install. Common Services supports only the Remote Administration mode for Terminal Services.

The following table explains the minimum and recommended server configurations.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating System</strong></td>
<td>Strongly Recommended: Windows 2008 Enterprise Server (Service Pack 2)—64 bit.</td>
</tr>
<tr>
<td></td>
<td>Alternate operating systems that also are supported:</td>
</tr>
<tr>
<td></td>
<td>- Windows 2003 R2 Enterprise Server (Service Pack 2)—32 bit.</td>
</tr>
<tr>
<td></td>
<td>- Windows 2008 Enterprise Server (Service Pack 2)—32 bit.</td>
</tr>
<tr>
<td></td>
<td>English and Japanese are the only supported languages. For complete information, see Understanding Regional and Language Options and Related Settings, page 2-6.</td>
</tr>
<tr>
<td></td>
<td>Microsoft ODBC Driver Manager 3.510 or later is also required so that your server can work with Sybase database files. To confirm the installed ODBC version, find and right-click ODBC32.DLL, then select Properties from the shortcut menu. The file version is listed under the Version tab.</td>
</tr>
</tbody>
</table>
Chapter 2  Requirements and Dependencies

Server Requirements

Table 2-3  Minimum and Recommended Server Requirements (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Hardware</td>
<td>• Processor requirements differ based on whether you are using Security Manager for device configuration only or for configuration and event management:</td>
</tr>
<tr>
<td></td>
<td>• Configuration only (or AUS, RME, or Performance Monitor only)—A dual-core processor is the minimum requirement. A quad-core or higher processor is</td>
</tr>
<tr>
<td></td>
<td>recommended. Higher cores typically result in improved performance.</td>
</tr>
<tr>
<td></td>
<td>• Configuration and Event Management—A quad-core processor is the minimum requirement. Higher cores typically result in improved performance.</td>
</tr>
<tr>
<td></td>
<td>• Color monitor with at least 1280 x 1024 resolution and a video card capable of 16-bit colors. For AUS-, Performance Monitor-, and RME-only servers,</td>
</tr>
<tr>
<td></td>
<td>you can get by with 1024 x 768 resolution.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) RAID 0 or RAID 10.</td>
</tr>
<tr>
<td></td>
<td>• DVD-ROM drive.</td>
</tr>
<tr>
<td></td>
<td>• 1 Gbps.</td>
</tr>
<tr>
<td></td>
<td>• Keyboard.</td>
</tr>
<tr>
<td></td>
<td>• Mouse.</td>
</tr>
<tr>
<td>Memory (RAM)</td>
<td>The minimum memory requirements differ based on operating system and whether you are using Security Manager for device configuration only or for configuration and event management. If you install AUS, RME, or Performance Monitor on the same system with Security Manager, the same minimums apply.</td>
</tr>
<tr>
<td></td>
<td>• Configuration only:</td>
</tr>
<tr>
<td></td>
<td>• 32-bit OS (Windows Server 2003 or 2008)—Minimum: 4 GB. Recommended: 8 GB.</td>
</tr>
<tr>
<td></td>
<td>• 64-bit OS (Windows Server 2008)—Minimum: 8 GB. Recommended: 12 GB.</td>
</tr>
<tr>
<td></td>
<td>• Configuration and Event Management:</td>
</tr>
<tr>
<td></td>
<td>• 32-bit OS (Windows Server 2003 or 2008)—Minimum: 8 GB. Recommended: 8 GB.</td>
</tr>
<tr>
<td></td>
<td>• 64-bit OS (Windows Server 2008)—Minimum: 12 GB. Recommended: 16 GB.</td>
</tr>
<tr>
<td></td>
<td>If the amount of RAM available to the operating system is less than or equal to 4 GB, Event Management is disabled during installation. Although not recommended, you can enable Event Management for low memory systems from the Security Manager client after completing the installation (select Tools &gt; Security Manager Administration &gt; Event Management). Keep in mind that enabling Event Management on a system with low memory can severely affect the performance of the entire application.</td>
</tr>
<tr>
<td></td>
<td>If you install AUS, RME, or Performance Monitor on separate servers, the following minimums apply:</td>
</tr>
<tr>
<td></td>
<td>• AUS- or Performance Monitor-only server—4 GB. We recommend more than 4 GB if you are using a 64-bit server.</td>
</tr>
<tr>
<td></td>
<td>• RME-only server—3 GB.</td>
</tr>
<tr>
<td>File system</td>
<td>NTFS.</td>
</tr>
<tr>
<td>Disk Optimization</td>
<td>Diskeeper 2010 Server.</td>
</tr>
</tbody>
</table>
### Understanding Regional and Language Options and Related Settings

Security Manager supports only the U.S., English and Japanese versions of Windows. From the Start Menu, open the Control Panel for Windows, open the panel where you configure region and language settings, then set the default locale. (We do not support English as the language in any Japanese version of Windows.)

---

**Table 2-3 Minimum and Recommended Server Requirements (continued)**

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard drive space</td>
<td>The minimum hard drive space requirements differ based on whether you are using Security Manager for device configuration only or for configuration and event management. Note that you cannot install the application if there is less than 5 GB of available disk space.</td>
</tr>
<tr>
<td></td>
<td>• Configuration only—40 GB.</td>
</tr>
<tr>
<td></td>
<td>• Configuration and Event Management—1 TB.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>A sustained 10,000 events per second (EPS) consumes about 86 GB of compressed disk space per day. Log rollover happens when 90% of the disk space allocated for events is filled. Smaller disk size causes quicker roll overs. Based on your expected EPS rate and rollover requirements, you can increase or decrease the minimum disk size when using Event Management.</td>
</tr>
<tr>
<td>IP address</td>
<td>One static IP address. Dynamic addresses are not supported.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>If the server has more than one IP address, you do not need to disable any of the multiple network interface cards before installation.</td>
</tr>
<tr>
<td>Swap Size</td>
<td>4096 MB.</td>
</tr>
<tr>
<td>Antivirus</td>
<td>Real-time protection disabled.</td>
</tr>
<tr>
<td>Browser</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Internet Explorer 6.0 Service Pack 2 (when running on Windows Server 2003).</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer 8 is supported only in Compatibility View. To use Compatibility View, open Internet Explorer 8, go to Tools &gt; Compatibility View Settings, and add the Security Manager server as a “website to be displayed in Compatibility View.”</td>
</tr>
<tr>
<td></td>
<td>– Exception: Firefox 3.0.8 is not supported on Windows Server 2008.</td>
</tr>
<tr>
<td>Optional Virtualization Software</td>
<td>You can optionally install the application on a system running VMware ESX 3.5 (update 2). You should allocate at least the same amount of memory to the virtual machine you use with Security Manager as you would for a non-virtualized server. Use of recent generation CPUs with technology designed to improve virtualization performance is recommended (for example, Intel-VT or AMD-V CPUs).</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>Allocate two or more CPUs to the VM image. Some processes, such as system backup, can take an unreasonably long time to complete if you use one CPU.</td>
</tr>
</tbody>
</table>
In addition, the Regional and Language Options in the server operating system (Windows Server 2003 or Windows Server 2008) must be set correctly. Also, peripheral devices such as keyboards that use other languages can affect the way Security Manager functions.

The following list contains the Regional and Language Options and related settings that you must adhere to in order to successfully install Security Manager:

- The server locale must be U.S. English or Japanese.
- You must avoid using peripheral devices such as keyboards that use other languages; these devices must not even be connected to the server.
- You must take care not to disturb the server settings while using a non-console RDP session to the server; as documented in http://support.microsoft.com/kb/924852, connecting to the server by using a non-console RDP can lead to the locale of the RDP client machine being applied to the server.
- You must check the Regional and Language Options and verify that the language selected for non-Unicode programs is English (United States); the path to that selection is Control Panel > Regional and Language Options > Advanced > Language for non-Unicode Programs.

### Client Requirements

Table 2-4 describes Security Manager Client requirements and restrictions.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>System hardware</td>
<td>• One CPU with a minimum speed of 2 GHz.</td>
</tr>
<tr>
<td></td>
<td>• Color monitor with at least 1280 x 1024 resolution and a video card capable of 16-bit colors.</td>
</tr>
<tr>
<td></td>
<td>• Keyboard.</td>
</tr>
<tr>
<td></td>
<td>• Mouse.</td>
</tr>
<tr>
<td>System software</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• Windows XP (Service Pack 3).</td>
</tr>
<tr>
<td></td>
<td>• Windows Vista (Service Pack 2).</td>
</tr>
<tr>
<td></td>
<td>• Windows 2003 Enterprise R2 Server (Service Pack 2).</td>
</tr>
<tr>
<td></td>
<td>• Windows 2008 Enterprise Server (Service Pack 2)—32-bit and 64-bit.</td>
</tr>
<tr>
<td>Note</td>
<td>Security Manager supports only the U.S. English and Japanese versions of Windows. From the Start Menu, open the Control Panel for Windows, open the panel where you configure region and language settings, then set the default locale. (We do not support English as the language in any Japanese version of Windows.)</td>
</tr>
<tr>
<td>Memory (RAM)</td>
<td>Minimum: 1 GB; Recommended: 2 GB.</td>
</tr>
<tr>
<td>Virtual Memory/ Swap Space</td>
<td>512 MB.</td>
</tr>
<tr>
<td>Hard Drive Space</td>
<td>10 GB free disk space.</td>
</tr>
</tbody>
</table>
### Client Requirements

#### Browser

- One of the following:
  - Microsoft Internet Explorer 6.0 Service Pack 2 (when running on Windows XP or Windows Server 2003).
  - Internet Explorer 8 is supported only in Compatibility View. To use Compatibility View, open Internet Explorer 8, go to Tools > Compatibility View Settings, and add the Security Manager server as a "website to be displayed in Compatibility View."
  - Firefox 2.0.x (when running on Windows XP or Windows Server 2003).
    - Exception: Firefox 3.0.8 is not supported on Windows Server 2008.

#### Java

- JRE 1.6 Update 14. This is used for applications that are hosted in a browser window.
  The Security Manager client includes an embedded and completely isolated version of Java. This Java version does not interfere with your browser settings or with other Java-based applications.
  To verify the installed versions of java, do one of the following:
    - Internet Explorer—Select Tools > Sun Java Console.
    - Firefox—Select Tools > Web Development > Java Console.
    - From a prompt—Enter `java -version`.

#### Windows user account

- You must log into the workstation with a Windows user account that has Administrator privileges to use the Security Manager client.
  Although the some features of the client might work with lesser privileges, Administrator users only are fully supported.
Preparing a Server for Installation

After you verify that the target server meets the requirements described in Chapter 2, “Requirements and Dependencies,” you can use these checklists to prepare and optimize your server for installation:

- Readiness Checklist for Installation, page 3-4

Best Practices for Enhanced Server Performance and Security

A framework of best practices, recommendations, and other preparatory tasks can enable your Security Manager server to run faster and more reliably than it might do otherwise.

⚠️ Caution ⚠️

We do not make any assurances that completing the tasks in this checklist improves the performance of every server. Nonetheless, if you choose not to complete these tasks, Security Manager might not operate as designed.

You can use this checklist to track your progress while you complete the recommended tasks.

<table>
<thead>
<tr>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Find and organize the installer applications for any recommended updates, patches, service packs, hot fixes, and security software to install on the server.</td>
</tr>
<tr>
<td>2. Upgrade the server BIOS if an upgrade is available.</td>
</tr>
</tbody>
</table>
| 3. If you plan to install Security Manager on a server that you have used for any other purpose, first back up all important server data, then use a boot CD or DVD to wipe all data from the server.  
   We do not support installation or coexistence on one server of Security Manager 4.0.1 and any release of Common Services earlier than 3.3. Nor do we support coexistence with any third-party software or other Cisco software, unless we state explicitly otherwise in this guide or at http://www.cisco.com/go/csmanager. |
| 4. Perform a clean installation of only the baseline server OS, without any manufacturer customizations for server management. |
| 5. Install any required OS service packs and OS patches on the target server. To check which service packs or updates are required for the version of Windows that you use, select Start > Run, then enter wupdmgr. |
## Task

1. **Install any recommended updates for drivers and firmware on the target server.**

2. **Scan the system for malware.** To secure the target server and its OS, scan the system for viruses, Trojan horses, spyware, key-loggers, and other malware, then mitigate all related problems that you find.

3. **Resolve security product conflicts.** Study and work to resolve any known incompatibilities or limitations among your security tools, such as popup blockers, antivirus scanners, and Cisco Security Agent or similar products from other companies. When you understand the conflicts and interactions among those products, decide which of them to install, uninstall, or disable temporarily, and consider whether you must follow a sequence. For example:
   - If your organization uses any host-based intrusion prevention utility from a company other than Cisco, you must not install that utility on the target server until after you install Security Manager. Otherwise, it might interfere with the installation of Cisco Security Agent, which is installed automatically in most cases as part of the Security Manager installation. If you want to use a server where another IPS utility is installed, uninstall it, then install Security Manager, then uninstall Cisco Security Agent, and then re-install the utility.
   - If any version of Cisco Security Agent is installed on a Security Manager server, the server relies on a set of agent policies specific to Security Manager servers. However, the customized, standalone agent that includes those policies is installed only if the target server has no pre-existing installation of the full version of Cisco Security Agent. The full agent version does not include the specific policies that a Security Manager server requires. If you prefer the full agent to the standalone agent, you must import into your full agent all the exported agent policies that you find on the Security Manager installation DVD (in its `\csm<version>_win_server\CSA subfolder`). We recommend that you do not uninstall the standalone agent until or unless you obtain equivalent server security through another method that you trust. If you import policies from the file on the DVD, you must reconcile those imported policies with any conflicting policies that your organization has configured generally for its managed agents.

4. **“Harden” user accounts.** To protect the target server against brute force attacks, disable the guest user account, rename the administrator user account, and remove as many other user accounts as is practical in your administrative environment.

5. **Use a strong password for the administrator user account and any other user accounts that remain.** A strong password has at least eight characters and contains numbers, letters (both uppercase and lowercase), and symbols. Tip: You can use the Local Security Settings tool to require strong passwords. Select **Start > Administrative Tools > Local Security Policy.**
<table>
<thead>
<tr>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>11. <strong>Remove unused, unneeded, and incompatible applications.</strong> For example:</td>
</tr>
<tr>
<td>- Microsoft Internet Information Server (IIS) is not compatible with Security Manager. If IIS is installed, you must uninstall it before you install Security Manager.</td>
</tr>
<tr>
<td>- We do not support the coexistence of Security Manager with any third-party software or other Cisco software (including any CiscoWorks-branded “solution” or “bundle,” such as the LAN Management Solution (LMS)), unless we state explicitly otherwise in this guide or at <a href="http://www.cisco.com/go/csmanager">http://www.cisco.com/go/csmanager</a>. We do support the installation of Security Manager, AUS, Performance Monitor and RME on the same server, but we recommend that configuration only for very small networks; also, you must install CiscoWorks Common Services before installing any of those products.</td>
</tr>
<tr>
<td>- We do not support the installation or coexistence of this version of Security Manager on a server with any release of Common Services earlier than 3.3.</td>
</tr>
<tr>
<td>- We do not support the coexistence of Security Manager on a server with any CD-ONE components (including CiscoView Device Manager) that you do not receive when you purchase Security Manager.</td>
</tr>
<tr>
<td>- We do not support the coexistence of Security Manager on the same server with Cisco Secure ACS for Windows.</td>
</tr>
<tr>
<td>- We do not support the coexistence of Security Manager on the same server with the full version of Cisco IPS Event Viewer.</td>
</tr>
<tr>
<td>12. <strong>Disable unused and unneeded services.</strong> At a minimum, Windows requires the following services to run: DNS Client, Event Log, Plug &amp; Play, Protected Storage, and Security Accounts Manager.</td>
</tr>
<tr>
<td>Check your software and server hardware documentation to learn if your particular server requires any other services.</td>
</tr>
<tr>
<td>13. <strong>Disable all network protocols except TCP and UDP.</strong> Any protocol can be used to gain access to your server. Limiting the network protocols limits the access points to your server.</td>
</tr>
<tr>
<td>14. <strong>Avoid creating network shares.</strong> If you must create a network share, secure the shared resources with strong passwords.</td>
</tr>
<tr>
<td><strong>Note</strong> We strongly discourage network shares. We recommend that you disable NETBIOS completely.</td>
</tr>
<tr>
<td>15. <strong>Configure server boot settings.</strong> Set a zero-second startup time, set Windows to load by default, and enable automatic reboot in cases of system failure.</td>
</tr>
</tbody>
</table>
Readiness Checklist for Installation

You must complete the following tasks before you install Security Manager.

1. Disable security applications temporarily. For example, you must temporarily disable any antivirus software on the target server before you install Security Manager. Installation cannot run while these programs are active.

2. Carefully consider the date and time settings that you apply to your server. Ideally, use an NTP server to synchronize the server date and time settings with those of the devices you expect to manage. Also, if you use Security Manager in conjunction with a Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance, the NTP server that you use should be the same one that your Cisco Security MARS appliance uses. Synchronized times are especially important in Cisco Security MARS because timestamp information is essential to accurately reconstruct what transpires on your network.

3. Confirm that required services and ports are enabled and available for use by Security Manager. See Required Services and Ports, page 2-1.

4. If Terminal Services is enabled in Application Mode, disable Terminal Services and reboot the server. Installation of Security Manager on a system with Terminal Services enabled in Application Mode is not supported. Terminal Services enabled in Remote Administration Mode is supported.

5. Disable any domain controller service (primary or backup) that is running.

6. Confirm that the target directory for installation is not encrypted. Any attempt to install Security Manager in an encrypted directory will fail.

7. If you are performing a fresh install, you should place your license file on the target server before installation. You will be prompted to select this file during installation.

8. If you have not done so already, uninstall IIS. It is not compatible with Security Manager.

9. Disable every active instance of Sybase on your server, including Cisco Secure ACS for Windows if it is present. You can choose whether to re-enable or restart Sybase after you install Security Manager, but remember we do not support the coexistence of Security Manager on the same server with Cisco Secure ACS for Windows.
### Readiness Factor

<table>
<thead>
<tr>
<th>✓</th>
<th>If the Cisco Security Manager client is already installed on the server, the client needs to be stopped. This condition is checked during installation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>Disable FIPS-compliant encryption. Federal Information Processing Standard (FIPS)-compliant encryption algorithms sometimes are enabled for group security policy on Windows Server 2008. When FIPS compliance is turned on, the SSL authentication may fail on CiscoWorks Server. You should disable FIPS compliance for CiscoWorks to work properly.</td>
</tr>
</tbody>
</table>

**Procedure**

To enable or disable FIPS on Windows Server 2008, follow these steps:

2. Click Local Policies > Security Options.
4. Right-click the selected policy and click Properties.
5. Select Enabled or Disabled to enable or disable FIPS compliant algorithms.
6. Click Apply.

You must reboot the server for the changes to take effect.
Installing and Upgrading Server Applications

The following topics explain how to install the Security Manager server software and other server applications, such as Common Services, AUS, Performance Monitor, and RME.

- Understanding the Required Server User Accounts, page 4-1
- Using Remote Desktop Connection or VNC To Install Server Applications, page 4-2
- Installing Security Manager Server, Common Services, and AUS, page 4-3
- Installing Performance Monitor, page 4-5
- Installing Resource Manager Essentials (RME), page 4-7
- Upgrading Server Applications, page 4-9
- Migrating Security Manager to a New Computer or Operating System, page 4-15
- Updating Security Manager, Performance Monitor, and RME Licenses, page 4-16
- Obtaining Service Packs and Point Patches, page 4-17
- Adding Applications to the Server’s Home Page, page 4-18
- Uninstalling Server Applications, page 4-18
- Downgrading Server Applications, page 4-19

Understanding the Required Server User Accounts

CiscoWorks Common Services and Security Manager use a multilevel security system that allows access to certain features only to users who have the required authorization. For this reason, there are three predefined user accounts that are created on any system on which you install an application that runs on top of Common Services:

- **admin** — The admin user account is equivalent to a Windows administrator and provides access to all Common Services, Security Manager, and other application tasks. You must enter the password during installation. You can use this account to initially log in to the server and to create other user accounts for normal day-to-day use of the applications.
- **casuser** — The casuser user account is equivalent to a Windows administrator and provides access to all Common Services and Security Manager tasks. You do not normally use this account directly.

Do not modify casuser (the default service account) or directory permissions that are established during the installation of the product. Doing so can lead to problems with your being able to do the following:

- Logging in to the web server
Using Remote Desktop Connection or VNC To Install Server Applications

We recommend that you install server applications when you are logged directly into the server. However, if you must do a remote installation (logging in through another workstation), consider the following tips:

- Do not attempt to install the software from a remote disk. The software installer must either be on the product DVD running on a DVD drive in the server, or the program must reside on a directly connected disk drive. The installation might appear to succeed from a remote disk, but it does not actually succeed.
- You can use Virtual Network Computing (VNC) to install the software.
- You can use Remote Desktop Connection to install the software. However, you might find that Cisco Security Agent does not stop automatically when trying to install Security Manager while two or more Remote Desktop Connection sessions are simultaneously open. This is due to a limitation of Remote Desktop Connection—the first administrator who opens a Remote Desktop Connection session is always the one who receives the query about stopping the Cisco Security Agent service. If you install Security Manager over a Remote Desktop Connection session and are not the first administrator logged in, you do not receive the query. A workaround is to enter the command `net stop CSAgent` before installing Security Manager. Otherwise, ensure that yours is the first, or only, Remote Desktop Connection session during installation.
Installing Security Manager Server, Common Services, and AUS

The main Security Manager installation program can install the following applications:

- **CiscoWorks Common Services 3.3**—This is the foundation software that is required by any of the server applications. You must install Common Services 3.3 (if it is not already installed) when you install Security Manager, AUS, Performance Monitor, or RME.

- **Cisco Security Manager 4.0.1**—This is the main server software for Security Manager.
  
  If the server does not already have a full, standalone version of Cisco Security Agent installed, the installation program takes the following actions:
  
  - On Windows 2003 R2 Enterprise Server (Service Pack 2)—32 bit, the installation program asks you whether or not you want to install Cisco Security Agent.
  - On Windows 2008 Enterprise Server (Service Pack 2)—32 bit, the installation program does not install Cisco Security Agent.
  - On Windows 2008 Enterprise Server (Service Pack 2)—64 bit, the installation program does not install Cisco Security Agent.

- **Auto Update Server 4.0**

- **Cisco Security Manager client 4.0.1**—The client software for interacting with the Security Manager server. You can install this on the same computer as the server, but you should not use this setup as the regular way of using Security Manager. For more information on recommended client installation and setup, see Chapter 5, “Installing and Configuring the Client.”

Use the following procedure to install or re-install these applications. If you are upgrading from a previous version of any of these applications, before proceeding, see Upgrading Server Applications, page 4-9.

**Before You Begin**

- All 3.x and earlier customers need to procure a new license (or licenses) for Security Manager 4.0.1 irrespective of whether they have a valid license for any of the (older) Security Manager 3.x releases. With the exception of incremental licenses, existing Security Manager 3.x licenses are not valid for Security Manager 4.0.1.

- If you are installing the product as an upgrade to an existing version of the application that is already installed on the server, run a backup as described in Backing Up the Database for Remote Upgrades, page 4-12. Ensure that the backup completes successfully, and that your existing applications are functioning normally before installing an upgrade.

- If you have a permanent license for Security Manager, copy it to the server. The license file must be on the server to select it during installation. Do not place the file in any folder in which you will install the product.

- Ensure that you go through the Readiness Checklist for Installation, page 3-4.

- Ensure that the server meets the requirements listed in Server Requirements, page 2-3.

- We recommend that you install Security Manager on a dedicated server in a controlled environment. Installing other software applications can interfere with the normal operation of Security Manager and is not supported.

- If you re-install Common Services after installing Security Manager server or AUS, you must also re-install Security Manager or AUS.

- Do not change the system time after installing Common Services. Such changes might affect the working of some time-dependent features.
If you want to use Cisco Secure Access Control Server (ACS) to provide AAA services for user access to Security Manager or AUS, wait until you install the applications before you configure Common Services to use ACS. For information on configuring ACS control, see Integrating Security Manager with Cisco Secure ACS, page 7-8.

If you install Security Manager or AUS after configuring Common Services to use ACS, you are told during installation that the application that you are installing requires new tasks to be registered with ACS. Select Yes if you have not already registered the application (on this or another server) with ACS. If you have already registered the application, if you select Yes, you lose any customized user roles configured in ACS for the application, so you should select No. All Security Manager and AUS servers that use the same ACS server share user roles.

Procedure
To install Security Manager Server, Common Services, AUS, or more than one of these applications using the main Security Manager installation program, follow these steps:

Step 1 Obtain or locate the installation program. You can do any of the following:

- Insert the Security Manager installation DVD into the server’s DVD drive. If the installation application does not automatically start, run the Setup.exe file in the csm<version>_win_server folder.
  - Using your choice of file compression utilities, such as WinZip or the Compressed (zipped) Folders Extraction Wizard, which is provided with Windows Server 2003, extract all the files in the compressed software installation file to a temporary directory. Use a directory that does not have an excessively long path name; for instance, C: is a better choice than C:\Documents and Settings\Administrator\Desktop. Start the installation program, Setup.exe, which normally unzips to the same directory as the compressed file.
  - If an error message states that the file contents cannot be unpacked, we recommend that you empty the Temp directory, scan for viruses, delete the C:\Program Files\Common Files\InstallShield directory, then reboot and retry.

Step 2 Follow the installation wizard instructions. During installation, you are asked for the following information:

- Backup location—If some version of Common Services, Security Manager, or AUS is already installed, the installation program allows you to perform a database backup during the installation. If you elect to perform the backup, select the location to use for the backup. However, it is typically better practice to perform a backup before starting the installation.
- Destination folder—The folder in which you want to install the application. Accept the default unless you have a compelling reason to install it elsewhere. If you specify a folder other than the default folder, make sure that it does not contain any files and that it has fewer than 256 characters in its pathname.
- Applications—The applications you want to install. You must select Common Services to install Security Manager or AUS unless Common Services is already installed.
- License information—Select one of the following:
  - License File Location—Enter the full pathname of the license file or click Browse to find it. You can specify the permanent license file if you have previously staged it on the server.
  - Evaluation Only—Enables the free 90-day evaluation period.
• Admin password—The password for the admin user account, at least 5 characters. For more information on this and the system identity and casuser accounts, see Understanding the Required Server User Accounts, page 4-1.

• System Identity user—The username and password for the account you want to use as the system identity user. When installing Cisco Security Management Suite applications on multiple servers, use the same system identity user account on all servers.

• Create casuser—Whether to create the casuser account on new installations. You must create this user account.

Step 3 After the installation is complete, restart the server if it does not restart automatically.

Note On an infrequent and random basis, Windows on VMware ESX stops responding (stalls) during the restart after installation. If this occurs, reboot the instance of VMware ESX using VMware GUI controls.

Installing Performance Monitor

You can install Performance Monitor 4.0.1 on the following:

• A standalone server, after you install CiscoWorks Common Services 3.3. This is the recommended configuration.

• The same server on which you installed Security Manager, AUS, RME, or all three, after you install CiscoWorks Common Services 3.3. However, if you use or enable Event Management, please read Effect of Enabling Event Management, page 1-7; you cannot enable Event Management on your Security Manager server if you want to use syslog on MCP or syslog on RME on that server.

Tip This configuration is recommended only for small networks.

The Performance Monitor license is a separate file from the Security Manager license file and includes the license for RME 4.3, too. You can install the license either before or after you install Performance Monitor. For instructions on how to obtain the license file, see Effects of Licensing on Installation and Obtaining a License, page 1-6.

Before You Begin
If you are installing on a system that already has Performance Monitor, Common Services, or other CiscoWorks applications, consider the following recommendations before installing Performance Monitor on the server:
• If you have a permanent license for Performance Monitor, copy it to the server. The license file must be on the server to select it during installation.

• Back up Common Services. The backup includes data for all installed applications that use Common Services. The Performance Monitor installation program does not perform a backup during the installation. For information on performing a backup, see Backing Up the Database for Remote Upgrades, page 4-12.

• If you install Common Services and Performance Monitor on a server, and then re-install Common Services later, you must also re-install Performance Monitor.

• If you want to use Cisco Secure Access Control Server (ACS) to provide AAA services for user access to Performance Monitor, wait until you install Performance Monitor before you configure Common Services to use ACS. For information on configuring ACS control, see Integrating Security Manager with Cisco Secure ACS, page 7-8.

If you install Performance Monitor after configuring Common Services to use ACS, you are told during installation that the application that you are installing requires new tasks to be registered with ACS. Select Yes if you have not already registered Performance Monitor (on this or another server) with ACS. If you have already registered Performance Monitor and you select Yes, you lose any customized user roles configured in ACS for the application, so you should select No. All Performance Monitor servers that use the same ACS server share user roles.

The following procedure contains additional steps to follow if you install Performance Monitor after configuring Common Services to use ACS.

Procedure
To install Performance Monitor, follow these steps:

Step 1 If the server does not already have CiscoWorks Common Services 3.3 installed, use the Security Manager installation DVD to install Common Services. For installation instructions, see Installing Security Manager Server, Common Services, and AUS, page 4-3. Performance Monitor cannot function without Common Services 3.3, and Common Services must be installed or upgraded to version 3.3 before you install Performance Monitor.

Step 2 Obtain or locate the installation program. You can do either of the following:

• Insert the Security Manager installation DVD into the server’s DVD drive. The installation program is mcp<version>\Setup.exe.

• Log in to your Cisco.com account and go to the Security Manager home page at http://www.cisco.com/go/csmanager. Click Download Software and download the installation utility for Performance Monitor.

Step 3 To start the installation, double-click the installation program and then follow the prompts.

Step 4 When you are prompted to select the licensing information, select one of the following:

• License File Location—Enter the full pathname of the license file or click Browse to find it. You can specify the permanent license file if you have staged it on the server.

• Evaluation Only—Enables the free 90-day evaluation period.

Performance Monitor with ACS
If you have not already configured Common Services to use ACS, skip the remaining steps in this procedure. However, if you install Performance Monitor after configuring Common Services to use ACS, you must complete the following additional steps in this procedure:

Step 5 Log in to the ACS server.
Step 6 On the ACS Server, navigate to Shared Profile Components. Verify that Performance Monitor is shown in the list of applications.

Step 7 On the ACS Server, navigate to Group Setup. Select the group name that you used to configure Security Manager.

Step 8 Click Edit Settings.

Step 9 On the Group Setup page, look for Performance Monitor. Check the check box to include Performance Monitor for ACS integration.

Step 10 Also on the Group Setup page, go to the next section (Performance Monitor).

Step 11 Click the Assign a Performance Monitor on a per Network Device Group Basis radio button.

Step 12 In the Device Group drop-down menu, select CSM_Servers.

Step 13 In the Performance Monitor drop-down menu, select System Administrator.

Step 14 Click Submit + Restart.

Step 15 On the Security Manager server, restart the Daemon Manager.

Step 16 Allow several minutes for the Daemons to start, or verify that they have, and log in to the Performance Monitor server.

Installing Resource Manager Essentials (RME)

You can install RME 4.3 on the following:

- A standalone server, after you install CiscoWorks Common Services 3.3. This is the recommended configuration.

- The same server on which you installed Security Manager, AUS, MCP, or all three, after you install CiscoWorks Common Services 3.3. However, if you use or enable Event Management, please read Effect of Enabling Event Management, page 1-7; you cannot enable Event Management on your Security Manager server if you want to use syslog on RME or syslog on MCP on that server.

Tip This configuration is recommended only for small networks.

The RME license is a separate file from the Security Manager license file and includes the license for Performance Monitor too. You can install the license either before or after you install RME. For instructions on how to obtain the license file, see Effects of Licensing on Installation and Obtaining a License, page 1-6.

Before You Begin

If you are installing on a system that already has RME, Common Services, or other CiscoWorks applications, consider the following recommendations before installing RME on the server:

- If you have a permanent license for RME, copy it to the server. The license file must be on the server to select it during installation.

- Back up Common Services. The backup includes data for all installed applications that use Common Services. The RME installation program does not perform a backup during the installation. For information on performing a backup, see Backing Up the Database for Remote Upgrades, page 4-12.
If you install Common Services and RME on a server, then re-install Common Services later, you must also re-install RME.

If you want to use Cisco Secure Access Control Server (ACS) to provide AAA services for user access to RME, wait until you install RME before you configure Common Services to use ACS. For information on configuring ACS control, see Integrating Security Manager with Cisco Secure ACS, page 7-8.

If you install RME after configuring Common Services to use ACS, you are told during installation that the application that you are installing requires new tasks to be registered with ACS. Select Yes if you have not already registered RME (on this or another server) with ACS. If you have already registered RME and you select Yes, you lose any customized user roles configured in ACS for the application, so you should select No. All RME servers that use the same ACS server share user roles.

Procedure
To install RME, follow these steps:

Step 1
If the server does not already have CiscoWorks Common Services 3.3 installed, use the Security Manager installation DVD to install Common Services. For installation instructions, see Installing Security Manager Server, Common Services, and AUS, page 4-3. RME cannot function without Common Services 3.3, and Common Services must be installed or upgraded to version 3.3 before you install RME.

Restart the system after installing Common Services before you install RME, or the Common Services installation might fail.

Step 2
Obtain or locate the installation program. You can do any of the following:

- Insert the Security Manager installation DVD into the server’s DVD drive. The installation program is rme<version>/Setup.exe.
- Log in to your Cisco.com account and go to the Security Manager home page at http://www.cisco.com/go/csmanager. Click Download Software and download the installation utility for RME.

Step 3
If McAfee VirusScan is installed on your server, confirm that VirusScan and the VirusScan feature “On-Access Scan” are running.

If VirusScan is installed but turned off, or if its On-Access Scan feature has been turned off, problems might prevent you from installing RME. In addition, any RME installations that fail for this reason might prevent Security Manager from operating correctly if it is also installed on the server (in which case you must re-install Security Manager).

Step 4
To start the installation, double-click the installation program and then follow the prompts.

During installation, you are asked for the following information:

- License information—Select one of the following:
  - License File Location—Enter the full pathname of the license file or click Browse to find it. You can specify the permanent license file if you have previously staged it on the server.
  - Evaluation Only—Enables the free 90-day evaluation period.

- Setup type (Typical or Custom)—Select Typical. The only difference between typical and custom is that a custom installation allows you to specify the database password, which is randomly generated during a typical installation. If you specify a database password, use a minimum of five characters and a maximum of 15 characters, do not start the password with a number, and do not insert spaces between characters. This password is also used while restoring or troubleshooting the database.
Restart CiscoWorks Daemons—You are asked whether you want to restart the CiscoWorks daemons. Answer Yes.

Upgrading Server Applications

Application upgrade refers to the process of installing a newer version of an application while preserving the data from the older version. There are three types of upgrade paths:

- Local—You simply install the newer version on the same server that is running the old version without first uninstalling the old version. Your existing data is maintained and available in the newly installed version. Keep the following in mind when doing local upgrades:
  - Before you use this method, ensure that all applications that you are upgrading are functioning correctly. Also, perform a backup of the database and ensure that it completes successfully before installing the upgraded applications.
  - You cannot use this method if you are also upgrading the operating system on the server, for example, going from Windows 2003 to Windows 2008. If you are doing a Security Manager upgrade while also doing an operating system upgrade, use the remote backup/restore upgrade method instead. If you are upgrading the operating system while maintaining the same Security Manager release, follow the procedure described in Migrating Security Manager to a New Computer or Operating System, page 4-15.

- Remote (backup/restore)—You install the newer version on a clean server (one that does not have the older application installed) and you then restore the database from a backup created from the older version. Use this procedure if you want to install on a new server or if you prefer to clean off your server before doing an installation (in which case you create the backup before uninstalling the application).

  Note: Before creating a backup of a server that is running the Security Manager server application, you must ensure that all pending data is committed. See Ensuring Security Manager Pending Data is Submitted and Approved, page 4-11.

- Indirect—If you have an older version of the application that is not supported for local or remote upgrade, you must perform a two-step process. First, you upgrade to a version that is supported for local or remote upgrade, then you perform the local or remote upgrade. Download the interim version from Cisco.com.

  If your version is not listed for indirect upgrade in the following table, you need to do three or more interim upgrade steps if you want to preserve your older data. For example, to upgrade from Performance Monitor 3.0, you must first upgrade to 3.2, from which you can upgrade to 4.0, and then to 4.0.1. For another example, Security Manager 3.0.x, you would need to upgrade to 3.1.1, then to 4.0, before upgrading to 4.0.1.

Normally when you upgrade from an earlier version of an application, both the evaluation and permanent licenses are preserved. However, all 3.x and earlier customers need to procure a new license (or licenses) for Security Manager 4.0.1 irrespective of whether they have a valid license for any of the (older) Security Manager 3.x releases. With the exception of incremental licenses, existing Security Manager 3.x licenses are not valid for Security Manager 4.0.1.

Table 4-1 explains the software versions that are supported for each upgrade path.
Security Manager 3.x users cannot upgrade directly to Security Manager 4.0.1. They must first upgrade to 4.0 and then to 4.0.1.

### Table 4-1 Application Upgrade Paths

<table>
<thead>
<tr>
<th>Upgrade Path</th>
<th>Applications</th>
<th>Supported Older Versions</th>
<th>Upgrade Procedure</th>
</tr>
</thead>
</table>
| Local        | Security Manager 4.0.1  
               | Auto Update Server 4.0 | 4.0              | Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 4-11.  
               |               |             | Then, install the software; see Installing Security Manager Server, Common Services, and AUS, page 4-3.  
               |               |             | Finally, make any required post-upgrade changes; see Making Required Changes After Upgrade, page 4-14. |
|              | Performance Monitor 4.0.1 | 4.0 | (Recommended) Back up your database; see Backing Up the Database for Remote Upgrades, page 4-12.  
               |               |             | Then, install the software; see Installing Performance Monitor, page 4-5 |
|              | RME 4.3 | 4.2 | (Recommended) Back up your database; see Backing Up the Database for Remote Upgrades, page 4-12.  
               |               |             | Then, install the software; see Installing Resource Manager Essentials (RME), page 4-7 |
| Remote       | Security Manager 4.0.1  
               | Auto Update Server 4.0 | 4.0              | 1. Back up the database; see Backing Up the Database for Remote Upgrades, page 4-12.  
               |               |             | 2. Install the application, see:  
               |               |             |   Installing Security Manager Server, Common Services, and AUS, page 4-3  
               |               |             |   Installing Performance Monitor, page 4-5  
               |               |             |   Installing Resource Manager Essentials (RME), page 4-7  
               | Performance Monitor 4.0.1 | 4.0 | 3. If necessary, transfer the database backup to the server.  
               | RME 4.3 | 4.2 | 4. Recover the database; see Restoring the Server Database, page 4-13.  
               |               |             | 5. Finally, make any required post-upgrade changes; see Making Required Changes After Upgrade, page 4-14. |
| Indirect     | Security Manager 4.0.1 | 3.2.2, 3.3, and 3.3.1 | First, upgrade to 4.0 and carefully follow the data migration instructions in the installation guide’s chapter on upgrade for 4.0.  
               |               |             | Then, use the local or remote upgrade path. |
|              | Performance Monitor 4.0.1 | 3.2.2, 3.3, and 3.3.1 | First upgrade to version 4.0, then use the local or remote upgrade path. See the installation guide for 4.0 |
|              | RME 4.3 | Not applicable. | Not applicable. The earliest supported RME release was 4.0.3, which is supported for local or remote upgrade. |
Ensuring Security Manager Pending Data is Submitted and Approved

Before you can successfully upgrade Security Manager, you must ensure that the existing Security Manager database does not contain any pending data, which is data that has not been committed to the database. You cannot restore a database from an earlier version of Security Manager if it has pending data; you can only restore a database that has pending data on a system running the same version as the backup.

Each user must submit or discard changes. If you are using Workflow mode with an approver, these submissions must also be approved. You might want to also perform a deployment after all data is committed so that all device configurations are synchronized with the Security Manager database.

- In non-Workflow mode:
  - To commit changes, select File > Submit.
  - To discard uncommitted changes, select File > Discard.
  - If you need to commit or discard changes for another user, you can take over that user’s session. To take over a session, select Tools > Security Manager Administration > Take Over User Session, select the session, then click Take Over Session.

- In Workflow mode:
  - To commit and approve changes, select Tools > Activity Manager. From the Activity Manager window, select an activity and click Approve. If you are using an activity approver, click Submit and have the approver approve the activity.
  - To discard uncommitted changes, select Tools > Activity Manager. From the Activity Manager window, select the activity, then click Discard. Only an activity in the Edit or Edit Open state can be discarded.

Restoring Changes that You Made to Property Files

All Security Manager installations have some property files that contain data that you usually change during use:

- $NMSROOT\MDC\athena\config\csm.properties
- $NMSROOT\MDC\athena\config\DCS.properties
- $NMSROOT\MDC\athena\config\taskmgr.prop

$NMSROOT is the full pathname of the Common Services installation directory (the default is C:\Program Files\CSCOpx).

If you run an upgrade or install a service pack on your current installation, Security Manager does the following:

- Installs new files in association with the upgrade or service pack.
- Compares the new files with the files that you modified during use.
- Warns you if the new files are different from the files that you changed during use. If they are, Security Manager does the following:
  - Stores the files that you changed during use, naming them <filename>.org.
  - Stores diff files for your convenience, naming them <filename>.diff.
If you receive a warning about new files being different from the files that you modified during use, use the information in `<filename>.org` and `<filename>.diff` to restore the changes that you made to property files before upgrade or service pack installation.

### Backing Up the Database for Remote Upgrades

CiscoWorks Common Services manages the database for all server applications, and it is the Common Services backup/restore utilities that are used for backing up and restoring the database. Thus, when you create a backup, you are creating a backup for all CiscoWorks applications installed on the server.

**Tip**
The backup procedure backs up the database only. If you need to back up the event data store, use the data store copy steps described in *Migrating Security Manager to a New Computer or Operating System*, page 4-15.

**Step 1**
If you are backing up a server that is running Security Manager, you can get to the backup page using a shortcut in the Security Manager client: **Tools > Backup**. Also, ensure that pending data is committed (see **Ensuring Security Manager Pending Data is Submitted and Approved**, page 4-11).

For servers that are not running Security Manager, to get to the backup page:

a. Log in to the Cisco Security Management Server desktop on the server (see **Logging In to Server Applications Using a Web Browser**, page 5-10).

b. Click the **Server Administration** panel. CiscoWorks Common Services is opened on the **Server > Admin** tab.

(If you log in to the CiscoWorks home page, select **Common Services > Server > Admin**.)

c. From the Server tab, select **Admin > Backup**.

**Step 2**
Select **Immediate** for Frequency, complete the other fields as desired, and click **Apply** to back up your data.

### Backing Up the Server Database By Using the CLI

The procedure in this section describes how to back up the server database by executing a script from the Windows command line on the server.

While backing up the database, both Common Services and Security Manager processes will be shut down and restarted. Because Security Manager can take several minutes to fully restart, users might be able to start their client before the restart is complete. If this happens, they might see the message “error loading page” in device policy windows.

A single backup script is used to back up all applications installed on a CiscoWorks server; you cannot back up individual applications.

**Tip**
The backup command backs up the database only. If you need to back up the event data store, use the data store copy steps described in *Migrating Security Manager to a New Computer or Operating System*, page 4-15.
Step 1  Ensure that pending data is committed (see Ensuring Security Manager Pending Data is Submitted and Approved, page 4-11).

Step 2  Back up the database by entering the following command:

```bash
$NMSROOT\bin\perl $NMSROOT\bin\backup.pl backup_directory [log_filename [email=email_address [number_of_generations [compress]]]]
```

where:

- `$NMSROOT`—The full pathname of the Common Services installation directory (the default is `C:\Program Files\CSCOpx`).
- `backup_directory`—The directory where you want to create the backup. For example, `C:\Backups`.
- `log_filename`—(Optional) The log file for messages generated during backup. Include the path if you want it created somewhere other than the current directory. For example, `C:\BackupLogs`. If you do not specify a name, the log is `$NMSROOT\log\dbbackup.log`.
- `email=email_address`—(Optional) The email address where you want notifications sent. If you do not want to specify an email address, but you need to specify a subsequent parameter, enter `email` without the equal sign or address. You must configure SMTP settings in CiscoWorks Common Services to enable notifications.
- `number_of_generations`—(Optional) The maximum number of backup generations to keep in the backup directory. When the maximum is reached, old backups are deleted. The default is 0, which does not limit the number of generations kept.
- `compress`—(Optional) Whether you want the backup file to be compressed. If you do not enter this keyword, the backup is not compressed if `VMS_FILEBACKUP_COMPRESS=NO` is specified in the `backup.properties` file. Otherwise, the backup is still compressed. We recommend compressing backups.

For example, the following command assumes you are in the directory containing the perl and `backup.pl` commands. It creates a compressed backup and log file in the `backups` directory and sends notifications to `admin@domain.com`. You must specify a backup generation to include the `compress` parameter; if you specify any parameter after the log file parameter, you must include values for all preceding parameters.

```bash
perl backup.pl C:\backups C:\backups\backup.log email=admin@domain.com 0 compress
```

Step 3  Examine the log file to verify that the database was backed up.

---

**Restoring the Server Database**

You can restore your database by running a script from the command line. You have to shut down and restart CiscoWorks while restoring data. This procedure describes how you can restore the backed up database on your server. A single backup and restore facility exists to back up and restore all applications installed on a CiscoWorks server; you cannot back up or restore individual applications.

If you install the applications on multiple servers, ensure that you recover the database backup that contains data appropriate for the installed applications.

**Tips**

- You can restore backups taken from previous releases of the application if the backup is from a version supported for direct local inline upgrade to this version of the application. For information on which versions are supported for upgrade, see Upgrading Server Applications, page 4-9.
The restore command restores the database only. If you need to restore the event data store, use the data store copy steps described in Migrating Security Manager to a New Computer or Operating System, page 4-15.

Procedure

Step 1
Stop all processes by entering the following at the command line:

```
net stop crmdmgtd
```

Step 2
Restore the database by entering the following command:

```
$NMSROOT\bin\perl $NMSROOT\bin\restorebackup.pl [-t temporary_directory] [-gen generationNumber] -d backup_directory [-h]
```

where:

- `$NMSROOT`—The full pathname of the Common Services installation directory (the default is C:\Program Files\CSCOpx).
- `-t temporary_directory`—(Optional) This is the directory or folder used by the restore program to store its temporary files. By default this directory is `$NMSROOT\tempBackupData`.
- `-gen generationNumber`—(Optional) The backup generation number you want to recover. By default, it is the latest generation. If generations 1 through 5 exist, 5 will be the latest.
- `-d backup_directory`—The backup directory that contains the backup to restore.
- `-h`—(Optional) Provides help. When used with `-d BackupDirectory`, help shows the correct syntax along with available suites and generations.

For example, to restore the most recent version from the c:\var\backup directory, enter the following command:

```
C:\Program Files\CSCOpx\bin\perl C:\Program Files\CSCOpx\bin\restorebackup.pl -d C:\var\backup
```

Tip
If you are restoring a database that contains RME data, you might be asked if you want to collect inventory data. Collecting this data can take a long time. You might want to respond No and then configure RME to schedule an inventory. In RME, select Devices > Inventory.

Step 3
Examine the log file, `NMSROOT\log\restorebackup.log`, to verify that the database was restored.

Step 4
Restart the system by entering:

```
net start crmdmgtd
```

Step 5
If you restore a database that was backed up prior to installing a Security Manager service pack, you must reapply the service pack after restoring the database.

Making Required Changes After Upgrade

Sometimes an application upgrade changes how particular types of information is handled in a way that requires that you make some manual changes. After upgrading to this version of the product, consider the following list of required changes and perform any that apply to your situation:
If you upgrade from any version earlier than 3.3.1, you must rediscover the inventory on any ASA 5580 device that includes a 4-port GigabitEthernet Fiber interface card (hardware type: i82571EB 4F). Inventory rediscovery overcomes a bug from previous releases that prevented changing speed nonnegotiate settings on the device. To rediscover inventory, right-click the device in Device view in the Security Manager client and select Discover Policies on Device, then select Live Device discovery and only the Inventory check box in the Policies to Discover group. Rediscovery replaces the Interfaces policy on the device.

If you upgrade from 3.3.1 or lower versions, and you managed Cisco ASR 1000 Series Aggregation Services Routers that used unsupported shared port adapters (SPA), you should rediscover policies on those devices so that Security Manager can discover the SPAs that were supported starting with version 4.0. Newly supported SPAs include all Ethernet (all speeds), Serial, ATM, and Packet over Sonet (POS) shared port adapters (SPA), but not services SPAs. Rediscovery is required if you configured ATM, PVC, or dialer related policies in the device CLI.

Migrating Security Manager to a New Computer or Operating System

You might need to move Security Manager to a new server. This move might be to a new physical computer, or you might want to perform a major upgrade to the operating system on the server (such as moving from Windows 2003 to Windows 2008).

When you are not changing the Security Manager version, but you are changing the physical hardware or the operating system, you need to go through a migration process. The migration process is essentially the same as the remote backup/restore upgrade process as described in Upgrading Server Applications, page 4-9; however, additional steps are required to migrate the data contained in the Event Manager data store. Use this procedure when you need to perform Security Manager server migration.

Note

Minor service pack updates to an operating system are not considered upgrades when it comes to Security Manager server-migration requirements. Server migration is required when you are moving between different major versions of the operating system, for example, as when the official name of the operating system changes.

Before You Begin

This procedure assumes that you want the target server (the server to which you are migrating Security Manager) to have the same database and event data store contents as the source computer. If you started using Security Manager on the target server, you cannot merge the database or event data store of the source and target systems: you must replace the target data with the source data. Any data that existed on the target system prior to the migration will become unusable after completing the migration. Do not attempt to copy the old target-system data into the newly-migrated folder.

Also note that the steps for copying and restoring the event data store are required only if you want to preserve this data. You can skip the steps if you want to start with a fresh empty event data store.

Step 1

Do the following on the source Security Manager server (the server from which you are migrating):

a. Determine the name of the event data store folder. Using the Security Manager client, select Tools > Security Manager Administration, and select Event Management from the table of contents. The folder is shown in the Event Data Store Location field; the default is NMSROOT\MDCEventing\database, where NMSROOT is the installation directory (usually C:\Program Files\CSCOpx).
b. Stop all processes by entering the following at the command line:
   
   \texttt{net stop crmdmgtd}

c. Make a copy of the $\text{NMSROOT}/\text{MDC}/\text{eventing}/\text{config}/\text{collector.properties}$ file and the event data store folder. Place the copy on a disk where you can access it from the target computer.

d. Back up the Security Manager database using the command line method as described in Backing Up the Server Database By Using the CLI, page 4-12.

**Step 2**

Prepare the new target computer. For example:

- If you are simply upgrading the operating system, but not moving to new hardware, perform the operating system upgrade and ensure that the operating system is functioning correctly. Then, install Security Manager.
- If you are moving to a new computer, ensure that it is functioning correctly and install Security Manager.

**Step 3**

Do the following on the target Security Manager server:

a. Stop all processes by entering the following at the command line:
   
   \texttt{net stop crmdmgtd}

d. Use the Security Manager client to log into the new server, then select Tools > Security Manager Administration, and select Event Management from the table of contents.

e. Ensure that the event data store folder exists and that it is empty (delete files if necessary). The folder must have the same name and location as the event data store had on the source server.

f. Select the correct Event Data Store Location (if the default is not already the correct folder), and deselect the Enable Event Management check box to stop the Event Manager service. Click Save to save your changes. You are prompted to verify that you want to stop the service; click Yes, and wait until you are notified that the service has stopped.

g. Copy the event data store backed up from the source computer to the new location on the target server.

h. Copy the backed up $\text{NMSROOT}/\text{MDC}/\text{eventing}/\text{config}/\text{collector.properties}$ file from the source computer to the target server, overwriting the file on the target server.

i. Using the Security Manager client, select Tools > Security Manager Administration, and select Event Management from the table of contents. Select the Enable Event Management check box and click Save. You are prompted to verify that you want to start the service; click Yes, and wait until you are notified that the service has started.

---

**Updating Security Manager, Performance Monitor, and RME Licenses**

Although you can specify permanent license files during installation, you can also add licenses after you install Security Manager, Performance Monitor, or RME. The other Cisco Security Management Suite applications do not require licenses.
The process for adding licenses is different for Security Manager compared to Performance Monitor and RME. The following procedure explains both processes. Keep in mind that the Performance Monitor/RME combined license is a separate file from the Security Manager license file.

For information about obtaining the licenses, see Effects of Licensing on Installation and Obtaining a License, page 1-6.

Before You Begin
You must copy the license file to the server before adding it to the application.

Procedure
To install licenses for Security Manager, Performance Monitor, or RME, follow these steps:

---

**Step 1** To install Security Manager licenses:

a. Log in to the server using the Security Manager client application (see Logging In to Security Manager Using the Security Manager Client, page 5-10).

b. Select Tools > Security Manager Administration and select Licensing from the table of contents.

c. Click CSM if the tab is not active.

d. Click Install a License to open the Install a License dialog box. Use this dialog box to select the license file and click OK. Repeat the process to add additional licenses.

**Step 2** To install Performance Monitor or RME licenses:

a. Log in to the Cisco Security Management Server desktop (see Logging In to Server Applications Using a Web Browser, page 5-10).

b. Click the Server Administration panel. CiscoWorks Common Services is opened on the Server > Admin tab.

(If you log in to the CiscoWorks home page, select Common Services > Server > Admin.)

c. Select Licensing. The License Information page displays the license name, license version, status of the license, and the expiration date of the license.

d. Click Update and enter the path to the new license file in the License field, or click Browse to locate the new file.

e. Click OK. The system verifies whether the license file is valid and updates the license. The updated licensing information appears in the License Information page.

---

Obtaining Service Packs and Point Patches

**Caution**
Do not download or open any file that claims to be a service pack or point patch for Security Manager unless you obtain it from Cisco. Third-party service packs and point patches are not supported.

After you install Security Manager or other applications, you might install a service pack or point patch from Cisco Systems to fix bugs, support new device types, or otherwise enhance the application.
Adding Applications to the Server’s Home Page

When you install Cisco Security Management Suite applications on the same server, the home page on that server displays links to the applications. However, if you install the applications on multiple servers, you need to register the applications on other servers for them to appear on a given server’s home page.

You need to do this only if you want the convenience of being able to connect to all related applications from a single home page; otherwise, you can use the applications by logging in directly to each server. For instructions on logging in to a server, which opens the home page, see Logging In to Server Applications Using a Web Browser, page 5-10.

Step 1 From the Cisco Security Manager Suite home page, click the Server Administration link. The Common Services Admin page appears.

Step 2 Select Server > HomePage Admin, and select Application Registration from the table of contents. The Application Registrations Status page appears.

Step 3 Click Register. The Choose Location for Registrations page appears.

Step 4 Select Register From Templates, then click Next.

Step 5 Select the application you want linked to the home page, for example, Monitoring, Analysis and Response System or RME, then click Next.

Step 6 Enter the server name, server display name, and port and protocol information for the device that is running the selected application, then click Next.

Step 7 Verify registration information, then click Finish. A launch point for the application now appears on the Cisco Security Manager Suite home page.

Uninstalling Server Applications

Use this procedure to uninstall server applications. Before uninstalling an application, consider performing a backup so that you can recover your data if you decide to re-install the application. For information on performing backups, see Backing Up the Database for Remote Upgrades, page 4-12.

Before You Begin
If any version of Windows Defender is installed, disable it before you uninstall a server application. Otherwise, the uninstallation application cannot run.
**Chapter 4 Installing and Updating Server Applications**

**Downgrading Server Applications**

You cannot downgrade Security Manager applications to earlier releases and preserve any configurations that you created in this release of the product. If you decide that you do not want to use this release of Security Manager, you can uninstall it and reinstall the desired older version of the product. (This

**Procedure**

To uninstall server applications, follow these steps:

---

**Step 1**

Select **Start > Programs > Cisco Security Manager > Uninstall Cisco Security Manager**. For servers where only Performance Monitor or RME is installed, you can also use **Start > Programs > Performance Monitor > Uninstall Performance Monitor** or **CiscoWorks > Uninstall CiscoWorks**.

**Step 2**

You are prompted with a list of installed applications. Select all applications that you want to uninstall. Do not select Common Services unless you intend to uninstall all Cisco Security Management Suite applications.

On Windows 2003 R2 Enterprise Server (Service Pack 2)—32 bit, the installation program asks you whether or not you want to uninstall Cisco Security Agent.

You cannot uninstall external Cisco Security Agent using this method. (External Cisco Security Agent is Cisco Security Agent that is not installed as part of the Cisco Security Manager installation.) If you want to uninstall Cisco Security Agent, select **Start > Programs > Cisco Security Agent > Uninstall Cisco Security Agent**. For more information, see Uninstalling Bundled Cisco Security Agent, page B-2.

**Step 3**

Click **Next** twice.

The uninstaller removes the applications that you selected.

---

**Note**

If the uninstallation causes an error, see Server Problems During Uninstallation, page A-8, and the “Troubleshooting and FAQs” chapter in Installing and Getting Started With CiscoWorks LAN Management Solution 3.1:


---

**Step 4**

Although no reboot is required, we recommend that you reboot the server after an uninstallation so that Registry entries and running processes on the server are in a suitable state for a future re-installation.

**Step 5**

Only if you uninstall all Cisco Security Management Suite applications, including Common Services:

- **a.** If **NMSROOT** still exists, delete it, move it, or rename it. **NMSROOT** is the path to the Security Manager installation directory. The default value of **NMSROOT** is **C:\Program Files\CSCOpx**. Other values, such as **E:\Program Files\CSCOpx**, are possible as well.

- **b.** If the **C:\CMFLOCK.TXT** file exists, delete it.

- **c.** Use a Registry editor to delete these Registry entries before you re-install the applications:
  - My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Resource Manager
  - My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\MDC

**Step 6**

If you disabled Windows Defender before uninstalling the applications, re-enable it now.
assumes that you have the required licenses and installation media for the older version.) You can then restore the desired database backup that you saved from your previous installation of the downgraded version, as described in Restoring the Server Database, page 4-13.

If you downgrade Security Manager, you must also downgrade Auto Update Server, Performance Monitor, and RME to a version supported by the Security Manager version that you reinstall.

After you restore the old database, keep in mind that it might contain device properties and policies that are no longer synchronized with the current state of the managed devices. For example, you might have upgraded the operating system on the device to one that is not directly supported by the older version of Security Manager, or you might have configured, and deployed, policies that do not exist in the older version. To ensure that the database is synchronized with the devices, consider rediscovering device policies for all managed devices. Be aware that some major changes (such as a major operating system release upgrade) require that you remove the device from the inventory and add it again. In some cases, you might need to revert an operating system upgrade (for example, ASA Software release 8.3 requires special handling and cannot be supported in downward compatibility mode, therefore, the Security Manager version you use must support it directly). See the “Managing the Device Inventory” chapter in the User Guide for Cisco Security Manager for more information.

Tip

If try to manage a device and operating system release combination that the older version of Security Manager cannot manage, you will see deployment errors.
Installing and Configuring the Client

There are two main client applications that you use with Security Manager applications:

- The Security Manager client. This is a client-server application that is installed on your workstation and that interacts with the database running on the Security Manager server, which normally resides on another computer. This client also uses your web browser for some functions.
- A web browser. You use your web browser to use Performance Monitor, AUS, RME, and for configuring the Security Manager server and other servers that use Common Services.

The following topics describe how to configure your web browser to run the clients and how to install the Security Manager client:

- Configuring Web Browser Clients, page 5-1
- Tips for Installing the Security Manager Client, page 5-5
- Installing the Security Manager Client, page 5-6
- Logging In to the Applications, page 5-9
- Uninstalling Security Manager Client, page 5-11

Configuring Web Browser Clients

You must ensure that your web browser is configured to allow certain types of content and not to block popup windows from the server running the applications. The web browser is used for displaying online help as well as functional application windows. The following sections explain the browser settings you must configure so that you can use your browser effectively as an application client:

- Configuring Internet Explorer Settings, page 5-2
- Configuring Firefox Settings, page 5-3
- Enabling and Configuring Exceptions in Third-party Tools, page 5-5
Chapter 5      Installing and Configuring the Client

Configuring Internet Explorer Settings

There are several settings that you need to configure in Internet Explorer for Security Manager and its applications to function correctly. Internet Explorer is used to display online help, activity reports, CS-MARS lookup information, and so forth. This procedure explains the settings you need to configure in Internet Explorer.

Procedure

Step 1  Turn off Pop-up Blocker for Security Manager by performing the following steps:
  a. Open Internet Explorer
  b. Go to Tools > Pop-up Blocker > Pop-up Blocker Settings
  c. In the Address of website to allow field, enter the IP address of your Security Manager server and then click Add.

 Caution  If you do not turn off Pop-up Blocker, you may not be able to discover devices in Security Manager.

 Tip  “Pop-up Blocker is a feature in Internet Explorer that lets you limit or block most pop-ups”

Step 2  In Internet Explorer, select Tools > Internet Options. All subsequent steps in this procedure are performed on the Internet Options dialog box.

Step 3  Allow active content by performing the following steps:
  a. Click the Advanced tab, scroll to the Security section, and select Allow active content to run in files on My Computer.
  b. Click Apply to save your changes.

Step 4  Confirm that the browser security settings enable you to save encrypted pages to disk. If you cannot save encrypted pages, you cannot download the client software installer.

On the Advanced tab, in the Security area, deselect Do not save encrypted Pages to Disk. If you needed to change the setting, click Apply to save your changes.

Step 5  Confirm that the size of the disk cache for temporary files is greater than the size of the client software installer that you expect to download. If the cache allocation is too small, you cannot download the installer. Change the cache size by performing the following steps:
  a. Click the General tab.
  b. Click Settings in the Temporary Internet Files group.
  c. If necessary, increase the amount of disk space to use for temporary Internet files, and click OK.
  d. Click Apply to save your changes.

Step 6  (Optional) Some interactions between CS-MARS and Security Manager require the opening of pages that have both secure and nonsecure content. By default, Internet Explorer asks you whether you want to display the nonsecure items. You can click Yes to this prompt and the software will function normally.
If desired, you can change the Internet Explorer settings so that you are not prompted and any page that has mixed content, that is, both secure and nonsecure content, are displayed automatically. Configure Internet Explorer to display mixed content pages by performing the following steps:

a. Click the Security tab.

b. Click Custom Level near the bottom of the dialog box.

c. Under the Miscellaneous heading, select the Enable radio button for the “Display mixed content” setting. (Ensure that you do not select Disable.)

d. Click Apply to save your changes.

Step 7 Click OK to close the Internet Options dialog box.

Configuring Firefox Settings

There are several settings that you need to configure in Firefox for Security Manager and its applications to function correctly. Firefox is used to display some features, such as online help, activity reports, CS-MARS lookup information, and so forth. This procedure explains the options you need to configure in Firefox.

- Editing the Preferences File, page 5-3
- Editing the Size of the Disk Cache, page 5-3
- Disabling the Popup Blocker or Creating a White List, page 5-4
- Enabling JavaScript, page 5-4
- Displaying Online Help on a New Tab in the Most Recent Window and Reusing Existing Windows on Subsequent Requests, page 5-4

Editing the Preferences File

Procedure

To edit the preferences file, do the following:

Step 1 From the \Mozilla Firefox\defaults\pref subdirectory, open firefox.js in a text editor, such as Notepad.

Step 2 Add the following:

```javascript
pref("dom.allow_scripts_to_close_windows", true);
```

Step 3 Save, and then close, the edited file.

Editing the Size of the Disk Cache

Confirm that the size of the disk cache for temporary files is greater than the size of the client software installer that you expect to download. If the cache allocation is too small, you cannot download the installer.

Procedure

To change the cache size, do the following:
Configuring Web Browser Clients

Chapter 5 Installing and Configuring the Client

Disabling the Popup Blocker or Creating a White List

Procedure
To disable popup blockers, do the following:

Step 1 Select Tools > Options, then click the Contents icon.
Step 2 Deselect the Block pop-up windows check box.

Alternatively, to create a white list of trustworthy sources from which to accept popups, select the Block pop-up windows check box, then click Exceptions and in the Allowed Sites - Popups dialog box do the following:

a. Enter http://<SERVER_NAME> (where SERVER_NAME is the IP address or DNS-routable name of your Security Manager server) in the Address of web site field, then click Allow.

b. Enter file:///C:/Documents%20and%20Settings/<USER_NAME>/Local%20Settings/Temp/ (where C: is the client system disk drive on which you installed Windows and USER_NAME is your Windows username on the client system), then click Allow.

c. Click Close.

Step 3 Click OK.

Enabling JavaScript

Procedure
To enable JavaScript, do the following:

Step 1 Select Tools > Options, then click the Contents icon.
Step 2 Select the Enable JavaScript check box.
Step 3 Click Advanced, and in the Advanced JavaScript Settings dialog box, select every check box in the Allow scripts to area.
Step 4 Click OK.

Displaying Online Help on a New Tab in the Most Recent Window and Reusing Existing Windows on Subsequent Requests

When you access online help the first time, two new browser windows might be opened: a blank page and a page with help contents. Also, existing browser windows might not be reused during subsequent attempts to access online help.

Procedure
To configure Firefox to display online help on a new tab in the most recently opened browser window and to reuse existing windows on later occasions, follow these steps:

**Step 1**
In the address bar, enter `about:config` and press **Enter**. The list of user preferences is displayed.

**Step 2**
Double-click `browser.link.open_external` and enter `3` in the resulting dialog box. This value denotes that links from an external application are opened in a new tab in the browser window that was last opened.

**Step 3**
Double-click `browser.link.open_newwindow` and set it to `1`. This value denotes that links are opened in the active tab or window.

**Step 4**
Double-click `browser.link.open_newwindow.restriction` and set it to `0`. This value causes all new windows to be opened as tabs.

**Step 5**
Close the about:config page.

---

**Note**
A blank page might be displayed when you open context-sensitive help, even after the browser status bar displays the status as Done. If this problem occurs, wait for a few minutes to allow the content to be downloaded and displayed.

---

**Enabling and Configuring Exceptions in Third-party Tools**

Some third-party popup blockers enable you to allow popups from a specific site or server without allowing popups universally. If your popup blocker does not allow you to configure exceptions to include in a white list, or if that option fails to meet your requirements, you must set your utility to allow all popups. The method for allowing popups from a trusted site varies according to the utility that you use. Please refer to the third-party product’s documentation for more information.

**Tips for Installing the Security Manager Client**

You use the Security Manager client to configure your devices. When you save changes in the client, they are saved to your workstation. You then must submit the changes to the database, which updates the database that resides on the server.

While using the client, there is constant back-and-forth communication between the client and the server. With that in mind, consider the following tips on installing the client to help improve client performance:

- Do not run the client on the same computer as the server as a normal day-to-day operation. If you install the client on the server, use it only for limited troubleshooting purposes.
- Install the client on workstations that are reasonably close to the server to avoid network latency problems. For example, if you have the server installed in the USA, a client running from a network in India might experience poor responsiveness due to the latency introduced. To alleviate this problem, you can employ a remote desktop or terminal server arrangement, where the clients are collocated in the same data center as the server.
- You can install only one copy of the client on a computer. There must be an exact version match between the client and server. Therefore, if you want to run two different versions of the Security Manager product, you must have two separate workstations for running the client.
Installing the Security Manager Client

The Security Manager client is a separate program that you install on your workstation. You use the client to log in to the Security Manager server and to configure security policies on your devices. The Security Manager client is the main application that you use with the product.

You might have already installed the client on the Security Manager server when you installed the server software. However, using the client on the same system as the server is not recommended for normal day-to-day usage of the product. Instead, you should install the client on a separate workstation using the following procedure. For information on workstation system requirements and supported browser versions, see Client Requirements, page 2-7.

If you run into problems during installation, see the following topics:
- Handling Security Settings That Prevent Installation, page 5-7
- Unable to Upgrade From a Previous Version of the Client, page 5-8

Before You Begin
- Ensure that your browser is configured correctly. See Configuring Web Browser Clients, page 5-1.
- We recommend that you manually delete the Temp files on your client system before you download the client software installer. Deleting such files increases the chances that you have enough available space.
- If it is installed, the Cisco Security Agent needs to be disabled, either before or during the process of installing the client. If the client installer cannot disable the Cisco Security Agent during the installation process, the process aborts and you are prompted to manually disable it before restarting the client installation.
- If you already have the Security Manager client installed on the workstation, the installation program must first uninstall it before installing the updated client. The wizard will prompt you if this is necessary.

Procedure

Step 1
Log in to the client workstation using a user account that has Windows administrator privileges.

Step 2
In your web browser, open one of these URLs, where SecManServer is the name of the computer where Security Manager is installed. Click Yes on any Security Alert windows.
- If you are not using SSL, open http://SecManServer:1741
- If you are using SSL, open https://SecManServer:443

The Cisco Security Management Suite login screen is displayed. Verify on the page that JavaScript and cookies are enabled and that you are running a supported version of the web browser.

Step 3
Log in to the Cisco Security Management Suite server with your username and password. When you initially install the server, you can log in using the username admin and the password defined during product installation.

Step 4
You are prompted to either open or run the file or to save it to disk. You can choose either option. If you choose to save it to disk, run the program after downloading it (double-click the file or select the Run option if your browser prompts you).

Tip If you get any security warnings about the application, such as “a problem was detected” or “the publisher cannot be verified” or that an unidentified application wants access to your computer, ensure that you allow the access. You might need to click more than one button, and the button names vary based on the application prompting you (such as Allow, Yes, Apply, and so forth).

Step 5 Follow the installation wizard instructions. During installation, you are asked for the following information:

- Server name—The DNS name or IP address of the server on which the Security Manager server software is installed. Normally, this is the server from which you downloaded the client installer.

- Protocol—HTTPS or HTTP. Select the protocol the Security Manager server is configured to use. Typically, the server is configured to use HTTPS. Ask your system administrator if you are not sure which to select. Also, if you know that the server is configured to use a non-default port, configure the port after installation using the information in Configuring a Non-Default HTTP or HTTPS Port, page 5-8.

- Shortcuts—Whether to create shortcuts for just yourself, for all user accounts that log in to this workstation, or for no users. This determines who will see Cisco Security Manager Client in the Start menu. You can start the client from Start > Programs > Cisco Security Manager Client > Cisco Security Manager Client or from the icon on the desktop.

- Installation location—The folder in which you want to install the client. Accept the default unless you have a compelling reason to install it elsewhere. The default location is C:\Program Files\Cisco Systems.

Step 6 After you click Finish to complete the installation, if you disabled an antivirus application temporarily, re-enable it.

If the Cisco Security Agent was stopped by the client installer, it is restarted at the end of the installation. However, if you manually disabled the Cisco Security Agent on your system, you must enable it after client installation is complete.

Handling Security Settings That Prevent Installation

There are many different ways you can configure security settings on your workstation, and many different products that you can install, that might prevent you from installing the Security Manager client. If you run into problems during installation, first ensure that your Windows user account has the administrative privileges required for installing software, then consider the following tips:

- (Windows 2003 or Windows XP) Internet Explorer Enhanced Security default settings might stop you from downloading the installation utility from your server. In this case, the following message appears:

  Internet Explorer cannot download CSMClientSetup.exe from <server>. Internet Explorer was not able to open this Internet site. The requested site is either unavailable or cannot be found. Please try again later.
Installing the Security Manager Client

To work around this problem, select Start > Settings > Control Panel > Add or Remove Programs, then click Add/Remove Windows Components. From the Windows Component Wizard window, deselect the Internet Explorer Enhanced Security Configuration check box, click Next, and then click Finish.

- (Windows Vista) The system displays the User Account Control popup window to indicate that an unidentified program wants access to your computer. This occurs because of a limitation in the InstallAnywhere software. This one-time popup displays only when installing the client software. Select Allow to continue.

- (Windows XP SP2 and Vista) Increased security features might cause the following message to be displayed:

  Security Warning Message. The publisher could not be verified. Are you sure you want to run this software?

  When you see this message, click Yes to continue.

- (Windows Vista) When you download the client software from your server, a File Download - Security Warning dialog box appears and asks, “Do you want to run or save this file?” Click Save to continue.

Configuring a Non-Default HTTP or HTTPS Port

The Security Manager server uses these default ports: HTTPS is 443; HTTP is 1741. If your organization installed the Security Manager server to use a different port, you need to configure the client to use the non-standard port. Otherwise, the client cannot connect to the server.

To configure different ports for your client, edit the C:\Program Files\Cisco Systems\Cisco Security Manager Client\jars\client.info file using a text editor such as Notepad. Add the following settings and specify the custom port number in place of <port number>:

- HTTPS_PORT=<port number>
- HTTP_PORT=<port number>

These settings are used the next time you start the client.

Unable to Upgrade From a Previous Version of the Client

When you attempt to install the Security Manager client when you already have an older client installed, or when you used to have a client installed on the workstation, the client installer first uninstalls the previous version before installing the new one. If you receive the error message “Could not find main class. Program will exit,” the installer cannot install the client.

Procedure

This problem occurs because of the presence of old registry entries in your system. To correct this problem, do the following:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Start the Registry Editor by selecting Start &gt; Run and entering regedit.</th>
</tr>
</thead>
</table>
| Step 2 | Remove the following registry key:  
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\f427e21299b0dd254754c0d2778feec4-837992615 |
**Step 3**  
Delete the previous installation directory, usually C:\Program Files\Cisco Systems\Cisco Security Manager Client.

**Step 4**  
Rename the following folder:  
C:\Program Files\Common Files\InstallShield\Universal\common\Gen1

**Step 5**  
Select Start > Control Panel > Add or Remove Programs. If the Cisco Security Manager Client is still listed, click Remove. If you receive the message, “Program already removed; do you want to remove it from the list?”, click Yes.

If you still cannot re-install the Security Manager client, rename the C:\Program Files\Common Files\InstallShield directory, then try again. Also see Client Problems During Installation, page A-9.

---

**Patching a Client**

After you apply a service pack or a point patch to your Security Manager server, the Security Manager client prompts you to apply an update when you log in to the server. The version number of the client software must be the same as the version number of the server software.

When you are prompted to download and apply a required software update, your web browser is used to download the update. You are prompted to either open or run the file, or to save it to disk. You can choose either option. If you choose to save it to disk, run the program after downloading it (double-click the file or select the Run option if your browser prompts you).

Installation of the patch is similar to installation of the client, and you must allow (or click Yes) to any security alerts from Cisco Security Agent or other security software you have installed to allow the installer to run.

When prompted for installation location, ensure that you select the folder in which you installed the client, and select Yes to All if you are asked if you want to overwrite files.

**Tip**  
If you get an error message that says that the URL cannot be retrieved or that the connection timed out, you need to uninstall the Security Manager client, then install a fresh copy (which will already have the patch applied). For more information, see Uninstalling Security Manager Client, page 5-11 and Installing the Security Manager Client, page 5-6.

---

**Logging In to the Applications**

After you have installed the server applications, configured your web browser, and installed the Security Manager client, you can log in to the applications:

- Logging In to Security Manager Using the Security Manager Client, page 5-10
- Logging In to Server Applications Using a Web Browser, page 5-10
Logging In to Security Manager Using the Security Manager Client

Use the Security Manager client to perform most Security Manager tasks.

Tip
You must log into the workstation using a Windows user account that has Administrator privileges to fully use the Security Manager client. If you try to operate the client with lesser privileges, you might find that some features do not work correctly.

Procedure

Step 1
Select Start > Programs > Cisco Security Manager Client > Cisco Security Manager Client to start the client.

Step 2
In the Security Manager login window, enter or select the DNS name or IP address of the server to which you want to log in, and enter your Security Manager username and password. If the server uses HTTPS for connections, ensure that the check box is selected; otherwise, deselect it. Click Login.

The client logs in to the server and opens the client interface. If the server prompts you to download and install a client software update, see Patching a Client, page 5-9.

Tip
The client closes if it is idle for 120 minutes. To change the idle timeout, select Tools > Security Manager Administration, select Customize Desktop from the table of contents, and enter the desired timeout period. You can also disable the feature so that the client does not close automatically.

Step 3
To exit Security Manager, select File > Exit.

Logging In to Server Applications Using a Web Browser

Only the Security Manager server uses a regular Windows application client for hosting the client application. All other applications, including the server administration features of Security Manager (through the Common Services application), CiscoWorks, Auto Update Server, Performance Monitor, and RME, are hosted in your web browser.

Logging in to these applications is identical. If you install more than one application on a single server, you log in to all installed applications at the same time. This is because the login is controlled by CiscoWorks, and all these applications are hosted under the CiscoWorks umbrella.

Procedure

Step 1
In your web browser, open one of these URLs, where server is the name of the computer where you installed any of the server applications. Click Yes on any Security Alert windows.

- If you are not using SSL, open http://server:1741.
- If you are using SSL, open https://server:443.

The Cisco Security Management Suite login screen is displayed. Verify on the page that JavaScript and cookies are enabled and that you are running a supported version of the web browser. For information on configuring the browser to run the applications, see Configuring Web Browser Clients, page 5-1.
Chapter 5      Installing and Configuring the Client

Step 2 Log in to the Cisco Security Management Suite server with your username and password. When you initially install the server, you can log in using the username admin and the password defined during product installation.

Step 3 On the Cisco Security Management Suite home page, you can access the features installed on the server. The home page can contain different items based on what you installed.

- Click the panel for the application that you want to run, such as Auto Update Server, Performance Monitor, or Resource Manager Essentials.
- Click the Server Administration panel to open the CiscoWorks Common Services Server menu. You can click this link to get to any place within Common Services. CiscoWorks Common Services is the foundation software that manages the server. Use it to configure and manage back-end server features such as server maintenance and troubleshooting, local user definition, and so on.
- Click the CiscoWorks link (in the upper right of the page) to open the CiscoWorks home page on the server.
- Click the Cisco Security Manager Client Installer to install the Security Manager client. The client is the main interface for using the Security Manager server.

Step 4 To exit the application, click Logout in the upper right corner of the screen. If you have both the home page and the Security Manager client open at the same time, exiting the browser connection does not exit the Security Manager client.

Uninstalling Security Manager Client

If you want to uninstall the Security Manager client, select Start > Programs > Cisco Security Manager Client > Uninstall Cisco Security Manager Client and follow the uninstallation wizard prompts.

If you are uninstalling the client from the Security Manager server, you can also uninstall the client using the server uninstaller.
Post-Installation Server Tasks

The following topics are tasks to complete after you install Security Manager or its related applications on a server.

- Server Tasks To Complete Immediately, page 6-1
- Verifying that Required Processes Are Running, page 6-2
- Verifying an Installation or an Upgrade, page 6-3
- Where To Go Next, page 6-4

Server Tasks To Complete Immediately

Make sure that you complete the following tasks immediately after installation.

<table>
<thead>
<tr>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Re-enable or re-install antivirus scanners and similar products.</strong> If you uninstalled or temporarily disabled any server security software, such as an antivirus tool or Cisco Security Agent, re-install or restart that software now, then restart your server if required.</td>
</tr>
<tr>
<td><strong>Note</strong> If you see that your antivirus software is reducing the efficiency or responsiveness of a Security Manager server, see your antivirus software documentation for recommended settings.</td>
</tr>
<tr>
<td>2. <strong>Re-enable the services and server processes that you disabled for installation.</strong> Do not re-enable IIS.</td>
</tr>
<tr>
<td>3. <strong>Re-enable any mission-critical applications that you disabled for installation, including those that use any Sybase technology or software code.</strong></td>
</tr>
<tr>
<td>4. <strong>On the server, add a self-signed certificate to the list of trusted certificates.</strong> To learn how, see your browser documentation.</td>
</tr>
<tr>
<td>5. <strong>Check for updates on Cisco.com for Security Manager and its related applications.</strong> If you learn that updates are available, install the ones that are relevant to your organization and network.</td>
</tr>
</tbody>
</table>
Verifying that Required Processes Are Running

You can run the `pdshow` command from a Windows command prompt window to verify that all required processes are running correctly for the Cisco server applications that you choose to install. Process requirements differ among the applications.

Tip
To learn more about `pdshow`, see the Common Services documentation.

Use Table 6-1 to understand which applications require which processes.

<table>
<thead>
<tr>
<th>This application:</th>
<th>Requires these Daemon Manager processes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Services</td>
<td>Apache</td>
</tr>
<tr>
<td></td>
<td>CmfDbEngine</td>
</tr>
<tr>
<td></td>
<td>CmfDbMonitor</td>
</tr>
<tr>
<td></td>
<td>CMFOGSServer</td>
</tr>
<tr>
<td></td>
<td>CSRegistryServer</td>
</tr>
<tr>
<td></td>
<td>DCRServer</td>
</tr>
<tr>
<td></td>
<td>diskWatcher</td>
</tr>
<tr>
<td></td>
<td>EDS</td>
</tr>
<tr>
<td></td>
<td>EDS-GCF</td>
</tr>
<tr>
<td></td>
<td>ESS</td>
</tr>
<tr>
<td></td>
<td>EssMonitor</td>
</tr>
<tr>
<td></td>
<td>jxm</td>
</tr>
<tr>
<td></td>
<td>LicenseServer</td>
</tr>
<tr>
<td></td>
<td>Proxy</td>
</tr>
<tr>
<td></td>
<td>Tomcat</td>
</tr>
<tr>
<td></td>
<td>TomcatMonitor</td>
</tr>
<tr>
<td></td>
<td>NameServer</td>
</tr>
<tr>
<td></td>
<td>NameServerMonitor</td>
</tr>
<tr>
<td>Cisco Security Manager</td>
<td>AthenaOGSServer</td>
</tr>
<tr>
<td></td>
<td>VmsBackendServer</td>
</tr>
<tr>
<td></td>
<td>VmsDbEngine</td>
</tr>
<tr>
<td></td>
<td>VmsDbMonitor</td>
</tr>
<tr>
<td></td>
<td>VmsEventServer</td>
</tr>
<tr>
<td>Auto Update Server</td>
<td>AusDbEngine</td>
</tr>
<tr>
<td></td>
<td>AusDbMonitor</td>
</tr>
<tr>
<td>Resource Manager Essentials</td>
<td>ChangeAudit</td>
</tr>
<tr>
<td></td>
<td>ConfigMgmtServer</td>
</tr>
<tr>
<td></td>
<td>CTMTrmServer</td>
</tr>
<tr>
<td></td>
<td>EssentialsDM</td>
</tr>
<tr>
<td></td>
<td>ICServer</td>
</tr>
<tr>
<td></td>
<td>RMEDbEngine</td>
</tr>
<tr>
<td></td>
<td>RMEOGSServer</td>
</tr>
<tr>
<td></td>
<td>SyslogAnalyzer</td>
</tr>
<tr>
<td></td>
<td>SyslogCollector</td>
</tr>
</tbody>
</table>

Tip
To verify that the Windows service called “Cisco Security Agent” is running on your server, select Start > Settings > Control Panel > Administrative Tools > Services.
Best Practices for Ongoing Server Security

The least secure component of a system defines how secure the system is. The steps in the following checklist can help you to secure a server and its OS after you install Security Manager:

1. **Monitor server security regularly.** Log and review system activity. Use security tools such as the Microsoft Security Configuration Tool Set (MSCTS) and Fport to periodically review the security configuration of your server. Review the log file for the standalone version of Cisco Security Agent that is installed sometimes on a Security Manager server.

   **Tip** You can obtain MSCTS from the Microsoft web site and Fport from the Foundstone/McAfee web site.

2. **Limit physical access to your server.** If your server contains removable media drives, set the server to boot from the hard drive first. Your data can be compromised if someone boots your server from a removable media drive. You can typically set the boot order in the system BIOS. Make sure you protect the BIOS with a strong password.

3. **Do not install remote access or administration tools on the server.** These tools provide a point of entry to your server and are a security risk.

4. **Set a virus scanning application to run automatically and continuously on the server.** Virus scanning software can prevent trojan horse applications from infecting your server. Update the virus signatures regularly.

5. **Back up your server database frequently.** Store all backups in a secure location with restricted access.

Verifying an Installation or an Upgrade

You can use Common Services to verify that you installed or upgraded Security Manager successfully. If you are trying to verify the installation because the Security Manager interface does not appear or is not displayed correctly, see Server Problems After Installation, page A-5.

**Step 1** Use a browser on the client system to log in to the Security Manager server using either of the following:

- For HTTP service—http://<server_name>:1741
- For SSL service—https://<server_name>:443

To learn which browsers and browser versions are supported, see Client Requirements, page 2-7.

**Step 2** From the Cisco Security Management Suite page, click the **Server Administration** panel to open Common Services at the **Server > Admin** page.

**Step 3** To display the Process Management page, click **Processes**.

The resulting list names all the server processes and describes the operational status of each process. The following processes must be running normally:

- vmsDbEngine
- vmsDbMonitor
- EDS
To learn whether an installed application might require other processes, such as RmeOrb and RmeGatekeeper for RME, read the documentation for that application on Cisco.com. For product documentation URLs, see the following:

- Common Services Documentation, page xi.
- Resource Manager Essentials Documentation, page xii.

## Where To Go Next

<table>
<thead>
<tr>
<th>If you want to:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand the basics</td>
<td>See the interactive <em>JumpStart</em> guide that opens when you start Security Manager.</td>
</tr>
<tr>
<td>Get up and running with the product quickly</td>
<td>See the “Getting Started with Security Manager” topic in the online help, or see Chapter 1 of <em>User Guide for Cisco Security Manager</em>.</td>
</tr>
<tr>
<td>Complete the product configuration</td>
<td>See the “Completing the Initial Security Manager Configuration” topic in the online help, or see Chapter 1 of <em>User Guide for Cisco Security Manager</em>.</td>
</tr>
</tbody>
</table>
| Manage user authentication and authorization | See the following topics:  
  - Setting Up User Permissions, page 7-1  
  - Integrating Security Manager with Cisco Secure ACS, page 7-8 |
Managing User Accounts

To use Security Manager, users must log in to the product and create individual accounts for each user. Either you can create accounts that are unique to Security Manager, which are defined on the Security Manager server and are called local accounts, or you can use your enterprise ACS server to authenticate users. The following topics describe how to create and manage user accounts, and how to integrate the product with your ACS system:

- Setting Up User Permissions, page 7-1
- Integrating Security Manager with Cisco Secure ACS, page 7-8
- Troubleshooting Security Manager-ACS Interactions, page 7-23

In some cases, you may want to use a CiscoWorks login module other than the CiscoWorks Local login module or the ACS module. That approach is called using a non-ACS login module, and it is supported by CiscoWorks. For example, you can use LDAP (Lightweight Directory Access Protocol). For information on this approach, see “Setting the Login Module to Non-ACS” in the User Guide for CiscoWorks Common Services 3.3 at the following URL:


See also the more general section “Setting up the AAA Mode” in the User Guide for CiscoWorks Common Services 3.3 at the following URL:


Setting Up User Permissions

Cisco Security Manager authenticates your username and password before you can log in. After they are authenticated, Security Manager establishes your role within the application. This role defines your permissions (also called privileges), which are the set of tasks or operations that you are authorized to perform. If you are not authorized for certain tasks or devices, the related menu items, items in tables of contents, and buttons are hidden or disabled. In addition, a message tells you that you do not have permission to view the selected information or perform the selected operation.

Authentication and authorization for Security Manager is managed either by the CiscoWorks server or the Cisco Secure Access Control Server (ACS). By default, CiscoWorks manages authentication and authorization, but you can change to Cisco Secure ACS by using the AAA Mode Setup page in CiscoWorks Common Services. For more information about ACS integration, see Integrating Security Manager with Cisco Secure ACS, page 7-8.
The major advantages of using Cisco Secure ACS are the ability to create highly granular user roles with specialized permissions sets (for example, allowing the user to configure certain policy types but not others) and the ability to restrict users to certain devices by configuring network device groups (NDGs). These granular privileges are not available for CiscoWorks local users.

To view the complete Security Manager permissions tree, log in to Cisco Secure ACS, then click **Shared Profile Components** on the navigation bar. For more information, see Customizing Cisco Secure ACS Roles, page 7-6.

The following topics describe user permissions:

- Security Manager ACS Permissions, page 7-2
- Understanding CiscoWorks Roles, page 7-4
- Understanding Cisco Secure ACS Roles, page 7-5
- Default Associations Between Permissions and Roles in Security Manager, page 7-7

**Security Manager ACS Permissions**

Cisco Security Manager provides default ACS roles and permissions. You can customize the default roles or create additional roles to suit your needs. However, when defining new roles or customizing default roles, make sure that the permissions you select are logical within the context of the Security Manager application. For example, if you assign modify permissions without view permissions, you lock the user out of the application.

Security Manager classifies permissions into the following categories. For an explanation of individual permissions, see the online help integrated with Cisco Secure ACS (for information on viewing the permissions, see Customizing Cisco Secure ACS Roles, page 7-6).

- **View**—Allows you to view the current settings. These are the main view permissions:
  - **View > Policies**. Allows you to view the various types of policies. The folder contains permissions for various policy classes, such as firewall and NAT.
  - **View > Objects**. Allows you to view the various types of policy objects. The folder contains permissions for each type of policy object.
  - **View > Admin**. Allows you to view Security Manager administrative settings.
  - **View > CLI**. Allows you to view the CLI commands configured on a device and preview the commands that are about to be deployed.
  - **View > Config Archive**. Allows you to view the list of configurations contained in the configuration archive. You cannot view the device configuration or any CLI commands.
  - **View > Devices**. Allows you to view devices in Device view and all related information, including their device settings, properties, assignments, and so on. You can limit device permissions to particular sets of devices by configuring network device groups (NDGs).
  - **View > Device Managers**. Allows you to launch read-only versions of the device managers for individual devices, such as the Cisco Router and Security Device Manager (SDM) for Cisco IOS routers.
  - **View > Topology**. Allows you to view maps configured in Map view.
- **Modify**—Allows you to change the current settings.
– Modify > Policies. Allows you to modify the various types of policies. The folder contains permissions for various policy classes.

– Modify > Objects. Allows you to modify the various types of policy objects. The folder contains permissions for each type of policy object.

– Modify > Admin. Allows you to modify Security Manager administrative settings.

– Modify > Config Archive. Allows you to modify the device configuration in the Configuration Archive. In addition, it allows you to add configurations to the archive and customize the Configuration Archive tool.

– Modify > Devices. Allows you to add and delete devices, as well as modify device properties and attributes. To discover the policies on the device being added, you must also enable the Import permission. In addition, if you enable the Modify > Devices permission, make sure that you also enable the Assign > Policies > Interfaces permission. You can limit device permissions to particular sets of devices by configuring network device groups (NDGs).

– Modify > Hierarchy. Allows you to modify device groups.

– Modify > Topology. Allows you to modify maps in Map view.

• Assign—Allows you to assign the various types of policies to devices and VPNs. The folder contains permissions for various policy classes.

• Approve—Allows you to approve policy changes and deployment jobs.

• Control—Allows you to issue commands to devices, such as ping. This permission is used for connectivity diagnostics.

• Deploy—Allows you to deploy configuration changes to the devices in your network and perform rollback to return to a previously deployed configuration.

• Import—Allows you to import the configurations that are already deployed on devices into Security Manager. You must also have view device and modify device privileges.

• Submit—Allows you to submit your configuration changes for approval.

Tips
• When you select modify, assign, approve, import, control or deploy permissions, you must also select the corresponding view permissions; otherwise, Security Manager will not function properly.

• When you select modify policy permissions, you must also select the corresponding assign and view policy permissions.

• When you permit a policy that uses policy objects as part of its definition, you must also grant view permissions to these object types. For example, if you select the permission for modifying routing policies, you must also select the permissions for viewing network objects and interface roles, which are the object types required by routing policies.

• The same holds true when permitting an object that uses other objects as part of its definition. For example, if you select the permission for modifying user groups, you must also select the permissions for viewing network objects, ACL objects, and AAA server groups.

• You can limit device permissions to particular sets of devices by configuring network device groups (NDGs). NDGs have the following effects on policy permissions:
  – To view a policy, you must have permissions for at least one device to which the policy is assigned.
  – To modify a policy, you must have permissions for all the devices to which the policy is assigned.
Setting Up User Permissions

- To view, modify, or assign a VPN policy, you must have permissions for all the devices in the VPN topology.
- To assign a policy to a device, you need permissions only for that device, regardless of whether you have permissions for any other devices to which the policy is assigned. (VPN policies are an exception, as noted above.) However, if a user assigns a policy to a device for which you do not have permissions, you cannot modify that policy.

Understanding CiscoWorks Roles

When users are created in CiscoWorks Common Services, they are assigned one or more roles. The permissions associated with each role determine the operations that each user is authorized to perform in Security Manager.

The following topics describe CiscoWorks roles:

- CiscoWorks Common Services Default Roles, page 7-4
- Assigning Roles to Users in CiscoWorks Common Services, page 7-5

CiscoWorks Common Services Default Roles

CiscoWorks Common Services contains the following default roles for Security Manager:

- **Help Desk**—Help desk users can view (but not modify) devices, policies, objects, and topology maps.
- **Approver**—In addition to view permissions, approvers can approve or reject deployment jobs. They cannot perform deployment.
- **Network Operator**—In addition to view permissions, network operators can view CLI commands and Security Manager administrative settings. Network operators can also modify the configuration archive and issue commands (such as ping) to devices.
- **Network Administrator**—Network administrators have complete view and modify permissions, except for modifying administrative settings. They can discover devices and the policies configured on these devices, assign policies to devices, and issue commands to devices. Network administrators cannot approve activities or deployment jobs; however, they can deploy jobs that were approved by others.

**Note**

Cisco Secure ACS features a default role called Network Administrator that contains a different set of permissions. For more information, see Understanding Cisco Secure ACS Roles, page 7-5.

- **System Administrator**—System administrators have complete access to all Security Manager permissions, including modification, policy assignment, activity and job approval, discovery, deployment, and issuing commands to devices.

For details about which Security Manager permissions are associated with each CiscoWorks role, see Default Associations Between Permissions and Roles in Security Manager, page 7-7.

**Tips**

- Additional roles, such as Export Data, might be displayed in Common Services if additional applications are installed on the server. The Export Data role is for third-party developers and is not used by Security Manager.
Although you cannot change the definition of CiscoWorks roles, you can define which roles are assigned to each user. For more information, see Assigning Roles to Users in CiscoWorks Common Services, page 7-5.

To generate a permissions table in CiscoWorks, select Server > Reports > Permission Report and click Generate Report.

Assigning Roles to Users in CiscoWorks Common Services

When you define a user in CiscoWorks Common Services, you must select the roles that the user should have. By changing the role definition for a user, you change the types of operations this user is authorized to perform in Security Manager. For example, if you assign the Help Desk role, the user is limited to view operations and cannot modify any data. However, if you assign the Network Operator role, the user is also able to modify the configuration archive. You can assign multiple roles to each user.

Tip
You must restart Security Manager after making changes to user permissions.

Related Topics
- Security Manager ACS Permissions, page 7-2
- Default Associations Between Permissions and Roles in Security Manager, page 7-7
- Understanding CiscoWorks Roles, page 7-4

Step 1
In Common Services, select Server > Security, then select Single-Server Trust Management > Local User Setup from the table of contents.

Tip
To reach the Local User Setup page from within Security Manager, select Tools > Security Manager Administration > Server Security, then click Local User Setup.

Step 2
Do one of the following:
- To create a user, click Add and enter the username, password, and email address.
- To change the roles of an existing user, check the check box next to the user and click Edit.

Step 3
On the User Information page, select the roles to assign to this user. For more information about each role, see CiscoWorks Common Services Default Roles, page 7-4.

Step 4
Click OK to save your changes.

Step 5
Restart Security Manager.

Understanding Cisco Secure ACS Roles

Cisco Secure ACS provides greater flexibility for managing Security Manager permissions than does CiscoWorks because it supports application-specific roles that you can configure. Each role is made up of a set of permissions that determine the level of authorization to Security Manager tasks. In Cisco Secure ACS, you assign a role to each user group (and optionally, to individual users as well), which enables each user in that group to perform the operations authorized by the permissions defined for that role.
In addition, you can assign these roles to Cisco Secure ACS device groups, allowing permissions to be differentiated on different sets of devices.

**Note**

Cisco Secure ACS device groups are independent of Security Manager device groups.

The following topics describe Cisco Secure ACS roles:

- Cisco Secure ACS Default Roles, page 7-6
- Customizing Cisco Secure ACS Roles, page 7-6

### Cisco Secure ACS Default Roles

Cisco Secure ACS includes the same roles as CiscoWorks (see Understanding CiscoWorks Roles, page 7-4), plus these additional roles:

- **Security Approver**—Security approvers can view (but not modify) devices, policies, objects, maps, CLI commands, and administrative settings. In addition, security approvers can approve or reject the configuration changes contained in an activity. They cannot approve or reject the deployment job, nor can they perform deployment.

- **Security Administrator**—In addition to having view permissions, security administrators can modify devices, device groups, policies, objects, and topology maps. They can also assign policies to devices and VPN topologies, and perform discovery to import new devices into the system.

- **Network Administrator**—In addition to view permissions, network administrators can modify the configuration archive, perform deployment, and issue commands to devices.

**Note**

The permissions contained in the Cisco Secure ACS network administrator role are different from those contained in the CiscoWorks network administrator role. For more information, see Understanding CiscoWorks Roles, page 7-4.

Unlike CiscoWorks, Cisco Secure ACS enables you to customize the permissions associated with each Security Manager role. For more information about modifying the default roles, see Customizing Cisco Secure ACS Roles, page 7-6.

For details about which Security Manager permissions are associated with each Cisco Secure ACS role, see Default Associations Between Permissions and Roles in Security Manager, page 7-7.

**Related Topics**

- Integrating Security Manager with Cisco Secure ACS, page 7-8
- Setting Up User Permissions, page 7-1

### Customizing Cisco Secure ACS Roles

Cisco Secure ACS enables you to modify the permissions associated with each Security Manager role. You can also customize Cisco Secure ACS by creating specialized user roles with permissions that are targeted to particular Security Manager tasks.

**Note**

You must restart Security Manager after making changes to user permissions.
Setting Up User Permissions

Related Topics

- Security Manager ACS Permissions, page 7-2
- Default Associations Between Permissions and Roles in Security Manager, page 7-7

Step 1
In Cisco Secure ACS, click **Shared Profile Components** on the navigation bar.

Step 2
Click **Cisco Security Manager** on the Shared Components page. The roles that are configured for Security Manager are displayed.

Step 3
Do one of the following:
- To create a role, click **Add**. Enter a name for the role and, optionally, a description.
- To modify an existing role, click the role.

Step 4
Check and uncheck the check boxes in the permissions tree to define the permissions for this role.

Checking the check box for a branch of the tree selects all permissions in that branch. For example, selecting the **Assign** checkbox selects all the assign permissions.

Descriptions of the individual permissions are included in the window. For additional information, see Security Manager ACS Permissions, page 7-2.

**Tip**
When you select modify, approve, assign, import, control or deploy permissions, you must also select the corresponding view permissions; otherwise, Security Manager does not function properly.

Step 5
Click **Submit** to save your changes.

Step 6
Restart Security Manager.

Default Associations Between Permissions and Roles in Security Manager

Table 7-1 shows how Security Manager permissions are associated with CiscoWorks Common Services roles and the default roles in Cisco Secure ACS. For information about the specific permissions, see Security Manager ACS Permissions, page 7-2.

**Table 7-1 Default Permission to Role Associations in Security Manager**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>View Device</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>View Policy</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>View Objects</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>View Topology</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>View CLI</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
Integrating Security Manager with Cisco Secure ACS

This section describes how to integrate your Cisco Secure ACS with Cisco Security Manager.

Cisco Secure ACS provides command authorization for users who are using management applications, such as Security Manager, to configure managed network devices. Support for command authorization is provided by unique command authorization set types (called roles in Security Manager) that contain a set of permissions. These permissions (also called privileges) determine the actions that users with particular roles can perform within Security Manager.

Cisco Secure ACS uses TACACS+ to communicate with management applications. For Security Manager to communicate with Cisco Secure ACS, you must configure the CiscoWorks server in Cisco Secure ACS as a AAA client that uses TACACS+. In addition, you must provide the CiscoWorks server with the administrator name and password that you use to log in to the Cisco Secure ACS. Fulfilling these requirements ensures the validity of communications between Security Manager and Cisco Secure ACS.

### Table 7-1 Default Permission to Role Associations in Security Manager (continued)

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Admin</td>
<td>Yes</td>
</tr>
<tr>
<td>View Config Archive</td>
<td>Yes</td>
</tr>
<tr>
<td>View Device Managers</td>
<td>Yes</td>
</tr>
<tr>
<td>Modify Permissions</td>
<td>Modify Device</td>
</tr>
<tr>
<td></td>
<td>Modify Hierarchy</td>
</tr>
<tr>
<td></td>
<td>Modify Policy</td>
</tr>
<tr>
<td></td>
<td>Modify Image</td>
</tr>
<tr>
<td></td>
<td>Modify Objects</td>
</tr>
<tr>
<td></td>
<td>Modify Topology</td>
</tr>
<tr>
<td></td>
<td>Modify Admin</td>
</tr>
<tr>
<td></td>
<td>Modify Config Archive</td>
</tr>
<tr>
<td>Additional Permissions</td>
<td>Assign Policy</td>
</tr>
<tr>
<td></td>
<td>Approve Policy</td>
</tr>
<tr>
<td></td>
<td>Approve CLI</td>
</tr>
<tr>
<td></td>
<td>Discover (Import)</td>
</tr>
<tr>
<td></td>
<td>Deploy</td>
</tr>
<tr>
<td></td>
<td>Control</td>
</tr>
<tr>
<td></td>
<td>Submit</td>
</tr>
</tbody>
</table>
Note

For an understanding of TACACS+ security advantages, see User Guide for Cisco Secure Access Control Server.

When Security Manager initially communicates with Cisco Secure ACS, it dictates to Cisco ACS the creation of default roles, which appear in the Shared Profile Components section of the Cisco Secure ACS HTML interface. It also dictates a custom service to be authorized by TACACS+. This custom service appears on the TACACS+ (Cisco IOS) page in the Interface Configuration section of the HTML interface. You can then modify the permissions included in each Security Manager role and apply these roles to users and user groups.

The following topics describe how to use Cisco Secure ACS with Security Manager:

- ACS Integration Requirements, page 7-9
- Procedural Overview for Initial Cisco Secure ACS Setup, page 7-10
- Integration Procedures Performed in Cisco Secure ACS, page 7-11
- Integration Procedures Performed in CiscoWorks, page 7-17
- Restarting the Daemon Manager, page 7-20
- Assigning Roles to User Groups in Cisco Secure ACS, page 7-21

ACS Integration Requirements

To use Cisco Secure ACS, make sure that the following steps are completed:

- You defined roles that include the permissions required to perform necessary functions in Security Manager.
- The Network Access Restriction (NAR) includes the device group (or the devices) that you want to administer, if you apply a NAR to the profile.
- Managed device names are spelled and capitalized identically in Cisco Secure ACS and in Security Manager. This restriction applies to the display names, not the hostnames defined on the devices. ACS naming restrictions can be more limiting than those for Security Manager, so you should define the device in ACS first.
- There are additional device display name requirements that you must meet for PIX/ASA security contexts, FWSMs, and IPS devices. These are described in Adding Devices as AAA Clients Without NDGs, page 7-13.

Tips

- We highly recommend that you create a fault-tolerant infrastructure that utilizes multiple Cisco Secure ACS servers. Having multiple servers helps to ensure your ability to continue work in Security Manager even if connectivity is lost to one of the ACS servers.
- You can integrate only one version of Security Manager with a Cisco Secure ACS. Therefore, if your organization is using two different versions of Security Manager at the same time, you must perform integration with two different Cisco Secure ACS servers. You can, however, upgrade to a new version of Security Manager without having to use a different ACS.
- Even when Cisco Secure ACS authentication is used, CiscoWorks Common Services software uses local authorization for CiscoWorks Common Services-specific utilities, such as Compact Database and Database Checkpoint. To use these utilities, you must be defined locally and be assigned the appropriate permissions.
Procedural Overview for Initial Cisco Secure ACS Setup

The following procedure summarizes the overall tasks you need to perform to use Cisco Secure ACS with Security Manager. The procedure contains references to more specific procedures used to perform each step.

Related Topics
- ACS Integration Requirements, page 7-9
- Integrating Security Manager with Cisco Secure ACS, page 7-8

Step 1  Plan your administrative authentication and authorization model.
You should decide on your administrative model before using Security Manager. This includes defining the administrative roles and accounts that you plan to use.

Tip  When defining the roles and permissions of potential administrators, you should also consider whether to enable Workflow. This selection affects how you can restrict access.

For more information, see the following:
- Understanding Cisco Secure ACS Roles, page 7-5
- User Guide for Cisco Security Manager
- User Guide for Cisco Secure Access Control Server

Step 2  Install Cisco Secure ACS, Cisco Security Manager, and CiscoWorks Common Services.
Install Cisco Secure ACS. Install CiscoWorks Common Services and Cisco Security Manager on a different server. Do not run Cisco Secure ACS and Security Manager on the same server.

For more information, see the following:
- Release Notes for Cisco Security Manager (for information on the supported versions of Cisco Secure ACS)
- Installing Security Manager Server, Common Services, and AUS, page 4-3
- Installation Guide for Cisco Secure ACS for Windows Server

Step 3  Perform integration procedures in Cisco Secure ACS.
Define Security Manager users as ACS users and assign them to user groups based on their planned role, add all your managed devices (as well as the CiscoWorks/Security Manager server) as AAA clients, and create an administration control user.

For more information, see Integration Procedures Performed in Cisco Secure ACS, page 7-11.

Step 4  Perform integration procedures in CiscoWorks Common Services.
Configure a local user that matches the system identity user defined in Cisco Secure ACS, define that same user for the system identity setup, configure ACS as the AAA setup mode, and configure an SMTP server and system administrator email address.
Step 5  **Restart the Daemon Manager.**

You must restart the Security Manager server Daemon Manager for the AAA settings you configured to take effect.

For more information, see **Restarting the Daemon Manager**, page 7-20.

Step 6  **Assign roles to user groups in Cisco Secure ACS.**

Assign roles to each user group configured in Cisco Secure ACS. The procedure you should use depends on whether you have configured network device groups (NDGs).

For more information, see **Assigning Roles to User Groups in Cisco Secure ACS**, page 7-21.

---

**Integration Procedures Performed in Cisco Secure ACS**

The following topics describe the procedures to perform in Cisco Secure ACS when integrating it with Cisco Security Manager. Perform the tasks in the listed order. For more information about the procedures described in these sections, see *User Guide for Cisco Secure Access Control Server*.

1. **Defining Users and User Groups in Cisco Secure ACS**, page 7-11
2. **Adding Managed Devices as AAA Clients in Cisco Secure ACS**, page 7-13
3. **Creating an Administration Control User in Cisco Secure ACS**, page 7-16

**Defining Users and User Groups in Cisco Secure ACS**

All users of Security Manager must be defined in Cisco Secure ACS and assigned a role appropriate to their job function. The easiest way to do this is to divide the users into different groups based on each default role available in ACS, for example, assigning all the system administrators to one group, all the network operators to another group, and so on. For more information about the default roles in ACS, see *Cisco Secure ACS Default Roles*, page 7-6.

You must create an additional user that is assigned the system administrator role with full permissions to devices. The credentials established for this user are later used on the System Identity Setup page in CiscoWorks. See **Defining the System Identity User**, page 7-18.

Please note that at this stage you are merely assigning users to different groups. The actual assignment of roles to these groups is performed later, after CiscoWorks, Security Manager, and any other applications have been registered to Cisco Secure ACS.

---

**Tip**

This procedure explains how to create user accounts during the initial Cisco Secure ACS integration. After you complete the integration, when you create a user account, you can assign it to the appropriate group as you create the account.

**Related Topics**

- **ACS Integration Requirements**, page 7-9
- **Procedural Overview for Initial Cisco Secure ACS Setup**, page 7-10
- **Assigning Roles to User Groups in Cisco Secure ACS**, page 7-21
Chapter 7      Managing User Accounts

Integrating Security Manager with Cisco Secure ACS

Step 1  Log in to Cisco Secure ACS.

Step 2  Configure a user with full permissions using the following procedure. For more information about the options available when configuring users and user groups, see User Guide for Cisco Secure Access Control Server.

a. Click User Setup on the navigation bar.

b. On the User Setup page, enter a name for the new user and click Add/Edit.

c. Select an authentication method from the Password Authentication list under User Setup.

d. Enter and confirm the password for the new user.

e. Select Group 1 as the group to which the user should be assigned.

f. Click Submit to create the user account.

Tip  Do not create a user named admin. The admin user is the fall-back user in Security Manager. If the ACS system stops working for some reason, you can still log in to CiscoWorks Common Services on the Security Manager server using the admin account to change the AAA mode to CiscoWorks local authentication and continue using the product.

c. Select Group 1 as the group to which the user should be assigned.

Step 3  Repeat this process for each Security Manager user. We recommend dividing the users into groups based on the role each user will be assigned:

- Group 1—System Administrators
- Group 2—Security Administrators
- Group 3—Security Approvers
- Group 4—Network Administrators
- Group 5—Approvers
- Group 6—Network Operators
- Group 7—Help Desk

For more information about the default permissions associated with each role, see Default Associations Between Permissions and Roles in Security Manager, page 7-7. For more information about customizing user roles, see Customizing Cisco Secure ACS Roles, page 7-6.

Note  At this stage, the groups themselves are collections of users without any role definitions. You assign roles to each group after you complete the integration process. See Assigning Roles to User Groups in Cisco Secure ACS, page 7-21.

Step 4  Create an additional user that you will use as the system identity user in CiscoWorks Common Services. Assign this user to the system administrators group and grant all privileges to devices. The credentials established for this user are later used on the System Identity Setup page in CiscoWorks. See Defining the System Identity User, page 7-18.

Step 5  Continue with Adding Managed Devices as AAA Clients in Cisco Secure ACS, page 7-13.
Adding Managed Devices as AAA Clients in Cisco Secure ACS

Before you can begin importing devices into Security Manager, you must first configure each device as a AAA client in your Cisco Secure ACS. In addition, you must configure the CiscoWorks/Security Manager server as a AAA client.

If Security Manager is managing security contexts configured on firewall devices, including security contexts configured on FWSMs for Catalyst 6500/7600 devices, each context must be added individually to Cisco Secure ACS. Likewise, all virtual sensors defined on IPS devices must also be added.

The method for adding managed devices depends on whether you want to restrict users to managing a particular set of devices by creating network device groups (NDGs). Proceed as follows:

- If you want users to have access to all devices, add the devices as described in Adding Devices as AAA Clients Without NDGs, page 7-13.
- If you want users to have access only to certain NDGs, add the devices as described in Configuring Network Device Groups for Use in Security Manager, page 7-14.

Adding Devices as AAA Clients Without NDGs

This procedure describes how to add devices as AAA clients of a Cisco Secure ACS. For complete information about all available options, see User Guide for Cisco Secure Access Control Server.

Tip

Remember to add the CiscoWorks/Security Manager server as a AAA client.

Related Topics

- ACS Integration Requirements, page 7-9
- Procedural Overview for Initial Cisco Secure ACS Setup, page 7-10

Step 1

Click Network Configuration on the Cisco Secure ACS navigation bar.

Step 2

Click Add Entry beneath the AAA Clients table.

Step 3

Enter the AAA client hostname (up to 32 characters) on the Add AAA Client page. The hostname of the AAA client must match the display name you plan to use for the device in Security Manager.

For example, if you intend to append a domain name to the device name in Security Manager, the AAA client hostname in ACS must be <device_name>.<domain_name>.

When naming the CiscoWorks server, we recommend using the fully qualified hostname. Be sure to spell the hostname correctly. (The hostname is not case sensitive.)

Additional naming conventions include:

- PIX or ASA security context, or FWSM security context when discovered through the FWSM: <parent_display_name>_context_name>
- FWSM blade: <chassis_name>_FW_<slot_number>
- FWSM security context when discovered through the chassis: <chassis_name>_FW_<slot_number>_context_name
- IPS sensor: <IPSParentName>_virtualSensorName

Step 4

Enter the IP address of the network device in the AAA Client IP Address field. If the device does not have an IP address (for example, a virtual sensor or a virtual context), enter the word dynamic instead of an address.
Integrating Security Manager with Cisco Secure ACS

**Note**
If you are adding a multi-homed device (a device with multiple NICs), enter the IP address of each NIC. Press Enter between each address. In addition, you must modify the gatekeeper.cfg file on the Security Manager server.

**Step 5** Enter the shared secret in the Key field.
**Step 6** Select TACACS+ (Cisco IOS) from the Authenticate Using list.
**Step 7** Click Submit to save your changes. The device you added is displayed in the AAA Clients table.
**Step 8** Repeat the process to add additional devices.
**Step 9** To save the devices you have added, click Submit + Restart.
**Step 10** Continue with Creating an Administration Control User in Cisco Secure ACS, page 7-16.

Configuring Network Device Groups for Use in Security Manager

Cisco Secure ACS enables you to configure network device groups (NDGs) that contain specific devices to be managed. For example, you can create NDGs for each geographic region or NDGs that match your organizational structure. When used with Security Manager, NDGs enable you to provide users with different levels of permissions, depending on the devices they need to manage. For example, by using NDGs you can assign User A system administrator permissions to the devices located in Europe and Help Desk permissions to the devices located in Asia. You can then assign the opposite permissions to User B.

NDGs are not assigned directly to users. Rather, NDGs are assigned to the roles that you define for each user group. Each NDG can be assigned to a single role only, but each role can include multiple NDGs. These definitions are saved as part of the configuration for the selected user group.

**Tips**
- Each device can be a member of only one NDG.
- NDGs are not related to the device groups that you can configure in Security Manager.
- For complete details about managing NDGs, see *User Guide for Cisco Secure Access Control Server*.

The following topics outline the basic information and steps for configuring NDGs:
- NDGs and User Permissions, page 7-14
- Activating the NDG Feature, page 7-15
- Creating NDGs, page 7-15
- Associating NDGs and Roles with User Groups, page 7-22

**NDGs and User Permissions**

Because NDGs limit users to particular sets of devices, they affect policy permissions, as follows:
- To view a policy, you must have permissions for at least one device to which the policy is assigned.
- To modify a policy, you must have permissions for all the devices to which the policy is assigned.
- To view, modify, or assign a VPN policy, you must have permissions for all the devices in the VPN topology.
To assign a policy to a device, you need permissions only for that device, regardless of whether you have permissions for any other devices to which the policy is assigned. (VPN policies are an exception, as noted above.) However, if a user assigns a policy to a device for which you do not have permissions, you cannot modify that policy.

**Note**

To modify an object, a user does not need modify permissions for all the devices that are using the object. However, a user must have modify permissions for a particular device in order to modify a device-level object override defined on that device.

**Related Topics**

- Configuring Network Device Groups for Use in Security Manager, page 7-14
- Setting Up User Permissions, page 7-1

**Activating the NDG Feature**

You must activate the NDG feature before you can create NDGs and populate them with devices.

**Related Topics**

- Creating NDGs, page 7-15
- Associating NDGs and Roles with User Groups, page 7-22
- NDGs and User Permissions, page 7-14
- Configuring Network Device Groups for Use in Security Manager, page 7-14

**Step 1**

Click **Interface Configuration** on the Cisco Secure ACS navigation bar.

**Step 2**

Click **Advanced Options**.

**Step 3**

Scroll down, then check the **Network Device Groups** check box.

**Step 4**

Click **Submit**.

**Step 5**

Continue with *Creating NDGs, page 7-15*.

**Creating NDGs**

This procedure describes how to create NDGs and populate them with devices. Each device can belong to only one NDG.

**Tip**

We highly recommend creating a special NDG that contains the CiscoWorks/Security Manager servers.

**Before You Begin**

Activate the NDG feature as described in *Activating the NDG Feature, page 7-15*.

**Related Topics**

- Associating NDGs and Roles with User Groups, page 7-22
- NDGs and User Permissions, page 7-14
- Configuring Network Device Groups for Use in Security Manager, page 7-14
Chapter 7  Managing User Accounts

Integrating Security Manager with Cisco Secure ACS

Step 1  Click **Network Configuration** on the navigation bar.

All devices are initially placed under Not Assigned, which holds all devices that were not placed in an NDG. Please note that Not Assigned is *not* an NDG.

Step 2  Create NDGs:

a.  Click **Add Entry**.

b.  Enter a name for the NDG on the New Network Device Group page. The maximum length is 24 characters. Spaces are permitted.

c.  (Optional) Enter a key to be used by all devices in the NDG. If you define a key for the NDG, it overrides any keys defined for the individual devices in the NDG.

d.  Click **Submit** to save the NDG.

e.  Repeat the process to create more NDGs.

Step 3  Populate the NDGs with devices. Keep in mind that each device can be a member of only one NDG.

a.  Click the name of the NDG in the Network Device Groups area.

b.  Click **Add Entry** in the AAA Clients area.

c.  Define the particulars of the device to add to the NDG, then click **Submit**. For more information, see **Adding Devices as AAA Clients Without NDGs**, page 7-13.

d.  Repeat the process to add the remaining devices to NDGs. The only device you should consider leaving in the Not Assigned category is the default AAA server.

e.  After you configure the last device, click **Submit + Restart**.

Step 4  Continue with **Creating an Administration Control User in Cisco Secure ACS**, page 7-16.

---

**Tip**

You can associate roles with each NDG only after completing the integration procedures in Cisco Secure ACS and CiscoWorks Common Services. See **Associating NDGs and Roles with User Groups**, page 7-22.

---

**Creating an Administration Control User in Cisco Secure ACS**

Use the Administration Control page in Cisco Secure ACS to define the administrator account that is used when defining the AAA setup mode in CiscoWorks Common Services. Security Manager uses this account to access the ACS server and register the application, to query device group membership and group setup, and to perform other basic interactions with ACS. For more information, see **Configuring the AAA Setup Mode in CiscoWorks**, page 7-18.

**Related Topics**

-  **ACS Integration Requirements**, page 7-9
-  **Procedural Overview for Initial Cisco Secure ACS Setup**, page 7-10

---

Step 1  Click **Administration Control** on the Cisco Secure ACS navigation bar.

Step 2  Click **Add Administrator**.

Step 3  On the Add Administrator page, enter a name and password for the administrator.
Step 4 Select the following administrator privileges:
- Under Users and Group Setup
  - Read access to users in group
  - Read access of these groups
- Under Shared Profile Components
  - Create Device Command Set Type
- Network Configuration

Step 5 Click Submit to create the administrator. For more information about the options available when configuring an administrator, see *User Guide for Cisco Secure Access Control Server*.

---

**Integration Procedures Performed in CiscoWorks**

After you complete the integration tasks in Cisco Secure ACS (described in *Integration Procedures Performed in Cisco Secure ACS, page 7-11*), you must complete some tasks in CiscoWorks Common Services. Common Services performs the actual registration of any installed applications, such as Cisco Security Manager and Auto Update Server, into Cisco Secure ACS.

The following topics describe the procedures to perform in CiscoWorks Common Services when integrating it with Cisco Security Manager:
- Creating a Local User in CiscoWorks, page 7-17
- Defining the System Identity User, page 7-18
- Configuring the AAA Setup Mode in CiscoWorks, page 7-18
- Configuring an SMTP Server and System Administrator Email Address for ACS Status Notifications, page 7-20

**Creating a Local User in CiscoWorks**

Use the Local User Setup page in CiscoWorks Common Services to create a local user account that duplicates the system identity user you previously created in Cisco Secure ACS (as described in *Defining Users and User Groups in Cisco Secure ACS, page 7-11*). This local user account is later used for the system identity setup. For more information, see *Defining the System Identity User, page 7-18*.

Related Topics
- ACS Integration Requirements, page 7-9
- Procedural Overview for Initial Cisco Secure ACS Setup, page 7-10

---

Step 1 Log in to CiscoWorks using the admin user account.

Step 2 Select Server > Security from Common Services, then select Local User Setup from the TOC.

Tip To get to this page from the Security Manager client, select Tools > Security Manager Administration > Server Security and click Local User Setup.

Step 3 Click Add.
Step 4 Enter the same name and password that you entered when creating the system identity user in Cisco Secure ACS. See Defining Users and User Groups in Cisco Secure ACS, page 7-11.

Step 5 Check all check boxes under Roles.

Step 6 Click OK to create the user.

---

**Defining the System Identity User**

Use the System Identity Setup page in CiscoWorks Common Services to create a trust user (called the System Identity user) that enables communication between servers that are part of the same domain and application processes that are located on the same server. Applications use the System Identity user to authenticate processes on local or remote CiscoWorks servers. This is especially useful when the applications must synchronize before any users have logged in.

In addition, the System Identity user is often used to perform a subtask when the primary task has already been authorized for the logged in user.

The System Identity user you configure here must also be defined as a local user in CiscoWorks (assigned to all roles) and as a user with all privileges to devices in ACS. If you do not select a user with the required privileges, you might not be able to view all the devices and policies configured in Security Manager. Make sure that you performed the following procedures before continuing:

- Defining Users and User Groups in Cisco Secure ACS, page 7-11
- Creating a Local User in CiscoWorks, page 7-17

**Related Topics**

- ACS Integration Requirements, page 7-9
- Procedural Overview for Initial Cisco Secure ACS Setup, page 7-10

---

**Configuring the AAA Setup Mode in CiscoWorks**

Use the AAA Setup Mode page in CiscoWorks Common Services to define your Cisco Secure ACS as the AAA server, including the required port and shared secret key. In addition, you can define up to two backup servers.
This procedure performs the actual registration of CiscoWorks and Security Manager (and optionally, Auto Update Server) into Cisco Secure ACS.

**Tip**
The AAA setup configured here is not retained if you uninstall CiscoWorks Common Services or Cisco Security Manager. In addition, this configuration cannot be backed up and restored after re-installation. Therefore, if you upgrade to a new version of either application, you must reconfigure the AAA setup mode and reregister Security Manager with ACS. This process is not required for incremental updates. If you install additional applications, such as AUS, on top of CiscoWorks, you must reregister the new applications and Cisco Security Manager.

### Related Topics
- ACS Integration Requirements, page 7-9
- Procedural Overview for Initial Cisco Secure ACS Setup, page 7-10

**Step 1**
In Common Services, select **Server > Security**, then select **AAA Mode Setup** from the TOC.

**Tip**
To get to this page from the Security Manager client, select **Tools > Security Manager Administration > Server Security** and click **AAA Mode Setup**.

**Step 2**
Select **TACACS+** under Available Login Modules.

**Step 3**
Select **ACS** as the AAA type.

**Step 4**
Enter the IP addresses of up to three Cisco Secure ACS servers in the Server Details area. The secondary and tertiary servers act as backups in case the primary server fails. All servers must be running the same version of Cisco Secure ACS.

**Note**
If all the configured TACACS+ servers fail to respond, you must log in using the **admin** CiscoWorks Local account, then change the AAA mode back to Non-ACS/CiscoWorks Local. After the TACACS+ servers are restored to service, you must change the AAA mode back to ACS.

**Step 5**
In the Login area, enter the name of the administrator that you defined on the Administration Control page of Cisco Secure ACS. For more information, see Creating an Administration Control User in Cisco Secure ACS, page 7-16.

**Step 6**
Enter and verify the password for this administrator.

**Step 7**
Enter and verify the shared secret key that you entered when you added the Security Manager server as a AAA client of Cisco Secure ACS. See Adding Devices as AAA Clients Without NDGs, page 7-13.

**Step 8**
Check the **Register all installed applications with ACS** check box to register Security Manager and any other installed applications with Cisco Secure ACS.

**Step 9**
Click **Apply** to save your settings. A progress bar displays the progress of the registration. A message is displayed when registration is complete.

**Step 10**
Restart the Cisco Security Manager Daemon Manager service. See Restarting the Daemon Manager, page 7-20.
Step 11  Log back in to Cisco Secure ACS to assign roles to each user group. See Assigning Roles to User Groups in Cisco Secure ACS, page 7-21.

Configuring an SMTP Server and System Administrator Email Address for ACS Status Notifications

If all the ACS servers become unavailable, users cannot perform tasks in Security Manager. Users who are logged in can be abruptly logged out of the system (without an opportunity to save changes) if they try to perform a task that requires ACS authorization.

If you configure Common Services settings to identify an SMTP server and a system administrator, Security Manager sends an email message to the administrator if all ACS servers become unavailable. This can alert you to a problem that needs immediate attention. The administrator might also receive email messages from Common Services for non-ACS-related events.

Tip  Security Manager can send email notifications for several other types of events such as deployment job completion, activity approval, or ACL rule expiration. The SMTP server you configure here is also used for these notifications, although the sender email address is set in Security Manager. For more information about configuring these other email addresses, see the User Guide for Cisco Security Manager for this version of the product, or the client online help.

Step 1  In Common Services, click Server > Admin, and select System Preferences from the table of contents.
Step 2  On the System Preferences page, enter the hostname or IP address of an SMTP server that Security Manager can use. The SMTP server cannot require user authentication for sending email messages.
Step 3  Enter an email address that CiscoWorks can use for sending emails. This does not have to be the same email address that you configure for Security Manager to use when sending notifications.
If the ACS server becomes unavailable, a message is sent to (and from) this account.
Step 4  Click Apply to save your changes.

Restarting the Daemon Manager

This procedure describes how to restart the Daemon Manager of the Security Manager server. You must do this so the AAA settings that you configured take effect. You can then log back in to CiscoWorks using the credentials defined in Cisco Secure ACS.

Related Topics
- Procedural Overview for Initial Cisco Secure ACS Setup, page 7-10
- ACS Integration Requirements, page 7-9

Step 1  Log in to the machine on which the Security Manager server is installed.
Step 2  Select Start > Programs > Administrative Tools > Services to open the Services window.
Step 3  From the list of services displayed in the right pane, select Cisco Security Manager Daemon Manager.
Step 4  Click the Restart Service button on the toolbar.
Assigning Roles to User Groups in Cisco Secure ACS

After you have registered CiscoWorks, Security Manager and other installed applications to Cisco Secure ACS, you can assign roles to each of the user groups that you previously configured in Cisco Secure ACS. These roles determine the actions that the users in each group are permitted to perform in Security Manager.

The procedure for assigning roles to user groups depends on whether NDGs are being used:

- Assigning Roles to User Groups Without NDGs, page 7-21
- Associating NDGs and Roles with User Groups, page 7-22

Assigning Roles to User Groups Without NDGs

This procedure describes how to assign the default roles to user groups when NDGs have not been defined. For more information, see Cisco Secure ACS Default Roles, page 7-6.

Before You Begin

- Create a user group for each default role. See Defining Users and User Groups in Cisco Secure ACS, page 7-11.
- Complete the procedures described in these topics:
  - Integration Procedures Performed in Cisco Secure ACS, page 7-11
  - Integration Procedures Performed in CiscoWorks, page 7-17

Related Topics

- Understanding CiscoWorks Roles, page 7-4
- Understanding Cisco Secure ACS Roles, page 7-5

Step 1 Log in to Cisco Secure ACS.
Step 2 Click Group Setup on the navigation bar.
Step 3 Select the user group for system administrators from the list (see Defining Users and User Groups in Cisco Secure ACS, page 7-11), then click Edit Settings.

Tip You can rename the groups with a more meaningful name to make it easier to identify the correct groups. Select a group and click Rename Group to change the name.

Step 4 Assign the system administrator role to this group:
   a. Scroll down to the CiscoWorks area under TACACS+ Settings.
   b. Select the first Assign option, then select System Administrator from the list of CiscoWorks roles.
   c. Scroll down to the Cisco Security Manager Shared Services area.
   d. Select the first Assign option, then select System Administrator from the list of Cisco Secure ACS roles.
Step 5
Repeat the process for the remaining roles, assigning each role to the appropriate user group.

When selecting the Security Approver or Security Administrator roles in Cisco Secure ACS, we recommend selecting Network Administrator as the closest equivalent CiscoWorks role.

For more information about customizing the default roles in ACS, see Customizing Cisco Secure ACS Roles, page 7-6.

Associating NDGs and Roles with User Groups

When you associate NDGs with roles for use in Security Manager, you must create definitions in two places on the Group Setup page:

- CiscoWorks area
- Cisco Security Manager area

The definitions in each area should match as closely as possible. When associating custom roles or ACS roles that do not exist in CiscoWorks Common Services, try to define as close an equivalent as possible based on the permissions assigned to that role.

You must create associations for each user group that will be used with Security Manager. For example, if you have a user group containing support personnel for the Western region, you can select that user group, then associate the NDG containing the devices in that region with the Help Desk role.

Before You Begin
Activate the NDG feature and create NDGs. See Configuring Network Device Groups for Use in Security Manager, page 7-14.

Related Topics
- ACS Integration Requirements, page 7-9
- Procedural Overview for Initial Cisco Secure ACS Setup, page 7-10

Step 1
Click Group Setup on the navigation bar.

Step 2
Select a user group from the Group list, then click Edit Settings.

Tip
You can rename the groups with a more meaningful name to make it easier to identify the correct groups. Select a group and click Rename Group to change the name.

Step 3
Map NDGs and roles for use in CiscoWorks:

a. On the Group Setup page, scroll down to the CiscoWorks area under TACACS+ Settings.

b. Select Assign a Ciscoworks on a per Network Device Group Basis.

c. Select an NDG from the Device Group list.

d. Select the role to which this NDG should be associated from the second list.

e. Click Add Association. The association appears in the Device Group box.

f. Repeat the process to create additional associations.

g. To remove an association, select it from the Device Group, then click Remove Association.
Step 4
Map NDGs and roles for use in Cisco Security Manager; you should create associations that match as closely as possible the associations defined in the previous step:

a. On the Group Setup page, scroll down to the Cisco Security Manager area under TACACS+ Settings.
b. Select Assign a Cisco Security Manager on a per Network Device Group Basis.
c. Select an NDG from the Device Group list.
d. Select the role to which this NDG should be associated from the second list.
e. Click Add Association. The association appears in the Device Group box.
f. Repeat the process to create additional associations.

Note When you are selecting the Security Approver or Security Administrator roles in Cisco Secure ACS, we recommend selecting Network Administrator as the closest equivalent CiscoWorks role.

Note CiscoWorks Common Services has a default role called “Network Administrator.” Cisco Secure ACS has a default role called “Network Admin.” These roles are not identical; they differ for a few of the permissions in Cisco Security Manager.

Step 5
Click Submit to save your settings.

Step 6
Repeat the process to define NDGs for the remaining user groups.

Step 7
To save the associations that you have created, click Submit + Restart.

For more information about customizing the default roles in ACS, see Customizing Cisco Secure ACS Roles, page 7-6.

Troubleshooting Security Manager-ACS Interactions

This following topics describe how to troubleshoot common problems that could occur because of how Security Manager and Cisco Secure ACS interact:

- Using Multiple Versions of Security Manager with Same ACS, page 7-23
- Authentication Fails When in ACS Mode, page 7-24
- System Administrator Granted Read-Only Access, page 7-24
- ACS Changes Not Appearing in Security Manager, page 7-25
- Devices Configured in ACS Not Appearing in Security Manager, page 7-25
- Working in Security Manager after Cisco Secure ACS Becomes Unreachable, page 7-25
- Restoring Access to Cisco Secure ACS, page 7-26
- Authentication Problems with Multihomed Devices, page 7-26
- Authentication Problems with Devices Behind a NAT Boundary, page 7-26
Using Multiple Versions of Security Manager with Same ACS

You cannot use the same Cisco Secure ACS with two different versions of Security Manager. For example, if you have integrated Security Manager 3.3.1 with a Cisco Secure ACS and another part of your organization plans to use Security Manager 4.0.1 without upgrading the existing installation, you must integrate Security Manager 4.0.1 with a different ACS than the one used for Security Manager 3.3.1.

If you upgrade an existing Security Manager installation, you can continue to use the same Cisco Secure ACS. The permission settings are updated as required.

Authentication Fails When in ACS Mode

If authentication keeps failing when you log in to Security Manager or CiscoWorks Common Services, even though you used Common Services to configure Cisco Secure ACS as the AAA server for authentication, do the following:

- Ensure that there is connectivity between the ACS servers and the server running Common Services and Security Manager.
- Ensure that the user credentials (username and password) you are using are defined in ACS and are assigned to the appropriate user group.
- Ensure that the Common Services server is defined as a AAA client on the Network Configuration page of ACS. Verify that the shared secret keys defined in Common Services (AAA Mode Setup page) and ACS (Network Configuration) match.
- Ensure that the IP address of each ACS server is correctly defined on the AAA Mode Setup page in Common Services.
- Ensure that the correct account is defined on the Administration Control page of ACS.
- Go to the AAA Mode Setup page in Common Services and verify that Common Services and Security Manager (as well as any other installed applications, such as AUS) are registered with Cisco Secure ACS.
- Go to Administration Control > Access Setup in ACS and ensure that the ACS is configured for HTTPS communication.
- If you receive “key mismatch” errors in the ACS log, verify whether the Security Manager server is defined as a member of a network device group (NDG). If it is, be aware that if you defined a key for the NDG, that key takes precedence over the keys defined for the individual devices in the NDG, including the Security Manager server. Ensure that the key defined for the NDG matches the secret key of the Security Manager server.

System Administrator Granted Read-Only Access

If you have read-only access to all policy pages of Security Manager even after logging in as a System Administrator with full permissions, do the following in Cisco Secure ACS:

- (When using network device groups (NDGs)) Click Group Setup on the Cisco Secure ACS navigation bar, then verify that the System Administrator user role is associated with all necessary correct NDGs for both CiscoWorks and Cisco Security Manager, especially the NDG containing the Common Services/Security Manager server.
• Click **Network Configuration** on the navigation bar, then do the following:
  - Verify that the Common Services/Security Manager server is not assigned to the Not Assigned (default) group.
  - Verify that the Common Services/Security Manager server is configured to use TACACS+ not RADIUS. TACACS+ is the only security protocol supported between the two servers.

  **Note**
  You can configure the network devices (routers, switches, firewalls, and so on) managed by Security Manager for either TACACS+ or RADIUS.

### ACS Changes Not Appearing in Security Manager

When you are using Security Manager with Cisco Secure ACS 4.x, information from ACS is cached when you log in to Security Manager or CiscoWorks Common Services on the Security Manager server. If you make changes in the Cisco Secure ACS Network Configuration and Group Setup while logged in to Security Manager, the changes might not appear immediately or be immediately effective in Security Manager. You must log out of Security Manager and Common Services and close their windows, then log in again, to refresh the information from ACS.

If you need to make changes in ACS, it is best practice to first log out of and close Security Manager windows, make your changes, and then log back in to the product.

  **Note**
  Although Cisco Secure ACS 3.3 is not supported, if you are using that version of ACS, you must open Windows Services and restart the Cisco Security Manager Daemon Manager service to get the ACS changes to appear in Security Manager.

### Devices Configured in ACS Not Appearing in Security Manager

If the devices that you configured on the Cisco Secure ACS are not appearing in Security Manager, it is probably a problem with the device display name.

The device display names defined in Security Manager must match the names you configure in ACS when you add the devices as AAA clients. This is particularly important when you use domain names. If you intend to append a domain name to the device name in Security Manager, the AAA client hostname in ACS must be `<device_name>.<domain_name>`, for example, pixfirewall.cisco.com.

### Working in Security Manager after Cisco Secure ACS Becomes Unreachable

Security Manager sessions are affected if the Cisco Secure ACS cannot be reached. Therefore, you should consider creating a fault-tolerant infrastructure that utilizes multiple Cisco Secure ACS servers. Having multiple servers helps to ensure your ability to continue work in Security Manager even if connectivity is lost to one of the ACS servers.

If your setup includes only a single Cisco Secure ACS and you wish to continue working in Security Manager in the event the ACS becomes unreachable, you can switch to performing local AAA authentication on the Security Manager server.
Procedure
To change the AAA mode, follow these steps:

---

**Step 1**  
Log in to Common Services using the admin CiscoWorks local account.

**Step 2**  
Select Server > Security > AAA Mode Setup, then change the AAA mode back to Non-ACS/CiscoWorks Local. This enables you to perform authentication and authorization using the local Common Services database and its built-in roles. Bear in mind that you must create local users in the AAA database to make use of local authentication.

**Step 3**  
Click Change.

---

Restoring Access to Cisco Secure ACS

If you cannot access Security Manager because the Cisco Secure ACS is down, do the following:

- Open up Windows Services on the ACS server and check whether the CSTacacs and CSRadius services are up and running. Restart these services if required.
- Perform the following procedure in CiscoWorks Common Services:

**Step 1**  
Log in to Common Services as the admin user.

**Step 2**  
Open a DOS window and run NMSROOT\bin\perl ResetLoginModule.pl.

**Step 3**  
Exit Common Services, then log in a second time as the admin user.

**Step 4**  
Go to Server > Security > AAA Mode Setup, then change the AAA mode to Non-ACS > CW Local mode.

**Step 5**  
Open Windows Services and restart the Cisco Security Manager Daemon Manager service.

---

Authentication Problems with Multihomed Devices

If you cannot configure a multihomed device (a device with multiple network interface cards (NICs)) that was added to the Cisco Secure ACS, even though your user role includes Modify Device permissions, there might be a problem with the way you entered the IP addresses for the device.

When you define a multihomed device as a AAA client of the Cisco Secure ACS, make sure to define the IP address of each NIC. Press Enter between each entry. For more information, see Adding Devices as AAA Clients Without NDGs, page 7-13.

---

Authentication Problems with Devices Behind a NAT Boundary

If you cannot configure a device with a pre-NAT or post-NAT IP address that was added to the Cisco Secure ACS, even though your user role includes Modify Device permissions, there might be a problem with the IP addresses that you configured.
When a device is behind a NAT boundary, make sure to define all IP addresses, including pre-NAT and post-NAT, for the device in the AAA client configuration settings in Cisco Secure ACS. For more information on how to add AAA client settings to ACS, see *User Guide for Cisco Secure Access Control Server*.
Troubleshooting

CiscoWorks Common Services provides Security Manager with its framework for installation, uninstallation, and re-installation on servers. If the installation or uninstallation of Security Manager server software causes an error, see “Troubleshooting and FAQs” in the Common Services online help or read it on Cisco.com:

The following topics help you to troubleshoot problems that might occur when you install, uninstall, or re-install Security Manager-related software applications on a client system or on a server, including the standalone version of Cisco Security Agent.

- Startup Requirements for Cisco Security Manager Services, page A-1
- Comprehensive List of Required TCP and UDP Ports, page A-2
- Troubleshooting the Security Manager Server, page A-4
- Troubleshooting the Security Manager Client, page A-9
- Troubleshooting Bundled Cisco Security Agent, page A-15
- Running a Server Self-Test, page A-17
- Collecting Server Troubleshooting Information, page A-17
- Viewing and Changing Server Process Status, page A-18
- Reviewing the Server Installation Log File, page A-19

Startup Requirements for Cisco Security Manager Services

Cisco Security Manager services must be started in a specific order for Security Manager to function correctly. The initialization of these services is controlled by the Cisco Security Manager Daemon Manager service. You should not change the service startup type for any of the Cisco Security Manager services. You should also not stop or start any of the Cisco Security Manager services manually. If you need to restart a specific service, you should restart the Cisco Security Manager Daemon Manager which ensures that all the related services are stopped and started in the correct order.
Comprehensive List of Required TCP and UDP Ports

The Cisco Security Management Suite applications need to communicate with clients and other applications. Other server applications might be installed on separate computers. For successful communication, certain TCP and UDP ports need to be open and available for transmitting traffic. Normally, you need to open only those ports described in Required Services and Ports, page 2-1. However, if you find that the applications are not able to communicate, the following table describes additional ports that you might need to open. The list is in port number order.

<table>
<thead>
<tr>
<th>Table A-1 Required Services and Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service</strong></td>
</tr>
<tr>
<td>Ping</td>
</tr>
<tr>
<td>FTP</td>
</tr>
<tr>
<td>SSH</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Telnet</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>SMTP</td>
</tr>
<tr>
<td>TACACS+ (for ACS)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>TFTP</td>
</tr>
<tr>
<td>HTTP</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>SNMP (polling)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>SNMP (traps)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>HTTPS (SSL)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Syslog</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### Table A-1 Required Services and Ports (continued)

<table>
<thead>
<tr>
<th>Service</th>
<th>Used For, or Used By</th>
<th>Port Number/Range of Ports</th>
<th>Protocol</th>
<th>Inbound</th>
<th>Outbound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Copy Protocol</td>
<td>Common Services</td>
<td>514 TCP X X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>Common Services</td>
<td>1741 TCP X —</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Manager</td>
<td>TCP X —</td>
<td>TCP X —</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUS</td>
<td>TCP X —</td>
<td>TCP X —</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance Monitor</td>
<td>TCP X —</td>
<td>TCP X —</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RADIUS</td>
<td>Security Manager (to external AAA server)</td>
<td>1645, 1646, 1812(new), 389, 636 (SSL), 88 TCP X —</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td></td>
<td>TCP X —</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kerberos</td>
<td></td>
<td>TCP X —</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control Server HTTP/HTTPS</td>
<td>Security Manager</td>
<td>2002 TCP — X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPO port for CiscoWorks gatekeeper</td>
<td>Common Services</td>
<td>8088 TCP X X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tomcat shutdown</td>
<td>Common Services</td>
<td>9007 TCP X —</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tomcat Ajp13 connector</td>
<td>Common Services</td>
<td>9009 TCP X —</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>Security Manager</td>
<td>10033 TCP X —</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>License Server</td>
<td>Common Services</td>
<td>40401 TCP X —</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Daemon Manager</td>
<td>Common Services</td>
<td>42340 TCP X X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Osagent</td>
<td>Common Services</td>
<td>42342 UDP X X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>Common Services</td>
<td>43441 TCP X —</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sybase</td>
<td>Auto Update Server</td>
<td>43451 TCP X X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance Monitor</td>
<td>43453 TCP X X</td>
<td>TCP X X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCR and OGS</td>
<td>Common Services</td>
<td>40050–40070 TCP X —</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Services</td>
<td>Software Service</td>
<td>42350/44350 UDP X X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software Listening</td>
<td>42351/44351 TCP X X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software HTTP</td>
<td>42352/44352 TCP X X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software Routing</td>
<td>42353/44353 TCP X X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport Mechanism (CSTM)</td>
<td>Common Services</td>
<td>50000–50020 TCP X —</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. To share and exchange information with a Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance, Security Manager uses HTTPS over port 443 by default. You can choose whether to use a different port for this purpose.

2. During the installation or upgrade of Security Manager, the Common Services syslog service port is changed from 514 to 49514. Later, if Security Manager is uninstalled, the port is not reverted to 514.
Troubleshooting the Security Manager Server

This section answers questions that you might have about:

- Server Problems During Installation, page A-4
- Server Problems After Installation, page A-5
- Server Problems During Uninstallation, page A-8

Server Problems During Installation

Q. When I install the server software, what does this installation error message mean?

A. Server software installation error messages and explanations appear in Table A-2 on page A-4, where they are sorted alphabetically by their first word.

<table>
<thead>
<tr>
<th>Table A-2 Installation Error Messages (Server)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Message</strong></td>
</tr>
</tbody>
</table>
| License file failed. ERROR: The file with the name c:\progra-1\CSCOpx\setup does not exist | An earlier attempt to uninstall a Common Services-dependent application failed. | 1. Shut down the server, then restart it.  
2. Use a Registry editor to delete this entry: $HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\ResourceManager\CurrentVersion.  
3. In the directory where you installed Security Manager, create a subdirectory named setup.  
4. Delete CMFLOCK.TXT if it exists.  
5. Re-install Security Manager. |
| Corrupt License file. Please enter a valid License file. | Your license file is corrupted or the contents of the license file are invalid. | See Getting Help with Licensing, page 1-7. |
| Corrupt License file entered for 5 tries. Install will proceed in EVAL mode. Press OK to proceed. | You entered the pathname to an invalid license file for five consecutive attempts. After five failed attempts, installation continues in evaluation mode. | Click OK to close the license error dialog box, and installation proceeds to the next screen of the wizard. |
| One instance of CiscoWorks Installation is already running. If you are sure that no other instances are running, remove the file C:\CMFLOCK.TXT. This installation will now abort. | An earlier attempt to install a Common Services-dependant application failed. | Delete the C:\CMFLOCK.TXT file, then try again. |
| Severe Failed on call to FileInsertLine. | Your server does not meet the requirement for hard drive space. | See Server Requirements, page 2-3. |
Troubleshooting the Security Manager Server

Appendix A  Troubleshooting

Table A-2  Installation Error Messages (Server) (continued)

<table>
<thead>
<tr>
<th>Message</th>
<th>Reason for Message</th>
<th>User Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporary directory used by installation has reached _istmp9x. If _istmp99 is reached, no more setups can be run on this computer, they fail with error -112.</td>
<td>Temporary files that are supposed to be deleted automatically during software installations have not been deleted on your server.</td>
<td>Search the temporary directory on your server for subdirectories with names that include the “_istmp” string. Delete all such subdirectories.</td>
</tr>
<tr>
<td>Windows cannot find ‘C:\Documents and Settings\Administrator\WINWS\System32\cmd.exe’. Make sure you typed the name correctly, and then try again. To search for a file, click the Start button, and then click Search.</td>
<td>You left Terminal Services enabled during installation, even though we do not support this. See Readiness Checklist for Installation, page 3-4.</td>
<td>1. Disable Terminal Services. To learn how to do this, see the “Terminal Server Support for Windows 2000 and Windows 2003 Server” topic in Installing and Getting Started With CiscoWorks LAN Management Solution 3.1, at <a href="http://www.cisco.com/en/US/docs/net_mgmt/cisco_works_lan_management_solution/3.1/install/guide/IGSG31.html">http://www.cisco.com/en/US/docs/net_mgmt/cisco_works_lan_management_solution/3.1/install/guide/IGSG31.html</a> 2. Try again to install Security Manager.</td>
</tr>
<tr>
<td>Setup has detected that unInstallShield is in use. Close unInstallShield and restart setup. Error 432.</td>
<td>The installation program checks the Windows account permissions during installation. If the Windows account that you are installing CiscoWorks Common Services under does not have local administrator privileges, InstallShield displays this error message.</td>
<td>1. Verify that you have appropriate permissions to write to %WINDIR%. Installation or uninstallation has to be done by a member of local administrators group. 2. Click OK to close the error message, log out of Windows, and log back in to Windows using an account that has local administrator privileges.</td>
</tr>
</tbody>
</table>

Q. What should I do if the server installer suspends operation (hangs)?
A. Reboot and try again.

Q. Can I install both Cisco Security Manager and Cisco Secure Access Control Server on one system?
A. We recommend that you do not. We do not support the coexistence of Security Manager on the same server with Cisco Secure ACS for Windows.

Q. Why does the Security Manager database backup fail?
A. If network management applications, such as Tivoli, were used to install Cygwin on the same system where a Security Manager server was installed, backup of the Security Manager database fails. Uninstall Cygwin.

Server Problems After Installation

Q. The Security Manager interface does not appear, or is not displayed correctly, or certain interface elements are missing. What happened?
A. There are several possible explanations. Investigate the scenarios in this list to understand and work around simple problems that might affect the interface:
• Some required services are not running on your server. Restart the server daemon manager, wait for all services to start completely, then restart Security Manager Client and try again to connect.

• Your server does not have enough free disk space. Confirm that the Security Manager partition on your server has at least 500 MB free.

• Your base license file is corrupted. See Getting Help with Licensing, page 1-7.

• Your server uses the wrong Windows language. Only English, on US-English versions of Windows, and Japanese, on Japanese versions of Windows, are supported. (See Server Requirements, page 2-3.) Any other language can corrupt the installed version of Security Manager, and missing GUI elements are one possible symptom. If you are using an unsupported language, you must select a supported language, then uninstall and re-install Security Manager. See Uninstalling Server Applications, page 4-18.

• Problems occurred when you installed Cisco Security Agent. You can check its installation log to learn whether problems interfered with the installation. See Troubleshooting Bundled Cisco Security Agent, page A-15.

• You ran the Security Manager installation utility over a network connection, but we do not support this use case (see Installing Security Manager Server, Common Services, and AUS, page 4-3). You must uninstall and re-install the server software. See Uninstalling Server Applications, page 4-18.

• Your client system does not meet the minimum requirements. See Client Requirements, page 2-7.

• You tried to use HTTP, but the required protocol is HTTPS.

• Buttons are the only missing element. You opened the Display Properties control panel on the client system, then changed one or more settings under the Appearance tab while you were simultaneously using Security Manager Client. To work around this problem, exit Security Manager Client, then restart it.

• The wrong graphics card driver software is installed on your client system. See Client Requirements, page 2-7.

**Problem**  When trying to open web interface to Security Manager using a web browser, a message indicates that I do not have permission to access /cwhp/LiaisonServlet on the Security Manager server. What does this mean?

**Solution**  The following table describes common causes and suggested workarounds for this problem.

<table>
<thead>
<tr>
<th>Table A-3 Causes and Workarounds for LiaisonServlet Error</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Cause</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-virus application</td>
<td>Uninstall the anti-virus application.</td>
</tr>
<tr>
<td>installed on server</td>
<td></td>
</tr>
<tr>
<td>IIS installed on server</td>
<td>IIS is not compatible with Security Manager and must be uninstalled.</td>
</tr>
</tbody>
</table>

OL-23410-01
Q. Security Manager sees only the local volumes, not the mapped drives, when I use it to browse directories on my server. Why?
A. Microsoft includes this feature by design in Windows to enhance server security. You must place any files you need to select in Security Manager on the server, such as license files.

Q. Why is Security Manager missing from the Start menu in my Japanese version of Windows?
A. You might have configured the regional and language option settings on the server to use English. We do not support English as the language in any Japanese version of Windows (see Server Requirements, page 2-3). Use the Control Panel to reset the language to Japanese.

Q. My server SSL certificate is no longer valid. Also, the DCRServer process does not start. What happened?
A. You reset the server date or time so that it is outside the range in which your SSL certificate is valid. See Readiness Checklist for Installation, page 3-4. To work around this problem, reset the server date/time settings.

Q. I was not prompted for the protocol to be used for communication between the server and client. Which protocol is used by default? Do I need to configure this setting manually using any other mode?
A. HTTPS is used as the communication protocol between the server and client, by default, when you install the client during the server installation. Because the communication is secure with the default protocol, you might not need to modify this setting manually.

An option to select HTTP as the protocol is available only when you run the client installer to install Security Manager client separately outside of the server installer. However, we recommend that you do not use HTTP as the communication protocol between the server and client. The client must use whatever protocol the server is configured to use.

Q. I am using a VMware setup, and system performance is unacceptably slow, for example, system backup takes two hours.
A. Ensure that you allocate two or more CPUs to the VM running Security Manager. Systems allocating one CPU have been found to have unacceptable performance for some system activities.

---

### Table A-3 Causes and Workarounds for LiaisonServlet Error (continued)

<table>
<thead>
<tr>
<th>Cause</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services required by Security Manager do not start in proper order</td>
<td>The only service that should be set to Automatic is the Cisco Security Manager Daemon Manager. All other CiscoWorks services should be set to Manual. Please note that it may take the Daemon Manager a few minutes to start up the other Ciscoworks services. These services must start up in the proper order; manually starting up the services can cause errors.</td>
</tr>
</tbody>
</table>
| casuser password | The casuser login is equivalent to a Windows administrator and provides access to all Common Services and Security Manager tasks. Reset the casuser password as follows:  
1. Open a command line on the server.  
2. Type `C:\Program Files\CSCOpx\setup\support\resetCasuser.exe`, then press Enter.  
3. Choose option 1 (Randomly generate casuser password). |
Server Problems During Uninstallation

Q. What does this uninstallation error message mean?

A. Uninstallation error messages and explanations appear in Table A-4 on page A-8, where they are sorted alphabetically by their first word. For additional information about uninstallation error messages, see the Common Services 3.2 documentation on Cisco.com.

Table A-4 Uninstallation Error Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Reason for Message</th>
<th>User Action</th>
</tr>
</thead>
</table>
| C:\NMSROOT\MDC\msfc-backend refers to a location that is unavailable. It could be on a hard drive on this computer, or on a network. Check to make sure that the disk is properly inserted, or that you are connected to the Internet or your network, and then try again. If it still cannot be located, the information might have been moved to a different location. | The message might be benign, and clicking OK to dismiss it might be all that is required. Otherwise, the message might appear on servers where either or both of the following conditions apply: - Simple file sharing is enabled in Windows. - Offline file synchronization is enabled in Windows. | If you dismiss the message and the uninstallation fails, try either or both of these possible workarounds, then try again to uninstall:  
**Simple File Sharing**  
1. Select Start > Settings > Control Panel > Folder Options.  
2. Click the View tab.  
3. Scroll to the bottom of the Advanced Settings pane.  
4. Uncheck the Use simple file sharing (Recommended) check box, then click OK.  
**Offline File Synchronization**  
1. Select Start > Settings > Control Panel > Folder Options.  
2. Click the Offline Files tab.  
3. Uncheck the Enable Offline Files check box, then click OK. |
| C:\temp\<subdirectory>\setup.exe - Access is denied. The process cannot access the file because it is being used by another process. | Uninstallation failed. | Reboot the server, then complete the procedure described in Uninstalling Server Applications, page 4-18. |
| | | |
| 0 file(s) copied.  
1 file(s) copied. | | |

T
Troubleshooting the Security Manager Client

This section answers questions that you might have about:

- Client Problems During Installation, page A-9
- Client Problems After Installation, page A-12

Client Problems During Installation

**Q.** When I install the client software, what does this installation error message mean?

**A.** Client software installation error messages and explanations appear in Table A-5, where they are sorted alphabetically by their first word.

---

**Table A-4 Uninstallation Error Messages (continued)**

<table>
<thead>
<tr>
<th>Message</th>
<th>Reason for Message</th>
<th>User Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Management Instrumentation (WMI) is running.</td>
<td>Either your organization uses WMI or someone enabled the WMI service accidentally on your server.</td>
<td>Click Yes.</td>
</tr>
</tbody>
</table>

The setup program has detected Windows Management Instrumentation (WMI) services running. This will lock some Cisco Security Manager processes and may abort uninstallation abruptly. To avoid this, uninstallation will stop and start the WMI services. Do you want to proceed? Click Yes to proceed with this uninstallation. Click No to exit uninstallation.

**Q.** What should I do if the uninstaller hangs?

**A.** Reboot, then try again.

**Q.** What should I do if the uninstaller displays a message to say that the `crmdmgtd` service is not responding and asks “Do you want to keep waiting?”

**A.** The uninstallation script includes an instruction to stop the crmdmgtd service, which did not respond to that instruction before the script timed out. Click Yes. In most cases, the crmdmgtd service then stops as expected.
Table A-5  Installation Error Messages (Client)

<table>
<thead>
<tr>
<th>Message</th>
<th>Reason for Message</th>
<th>User Action</th>
</tr>
</thead>
</table>
| Could not install engine jar | Previous software installations and un installations caused InstallShield to run incorrectly. | 1. Navigate to: C:\Program Files\Common Files\InstallShield\Universal\common\Gen1.  
2. Rename the Gen1 folder, then try again to install Security Manager Client.  
If Gen1 is not present, rename common instead. |
| Error - Cannot Connect to Server | Most likely, the server is misconfigured for HTTPS traffic. | 1. From a browser, log in to the Cisco Security Management Suite desktop at https://<server>/CSCOnm/servlet/login/login.jsp.  
2. Click Server Administration.  
3. In the Admin window, select Server > Security.  
4. From the TOC, select Single Server Management > Browser-Server Security Mode Setup, then confirm that the Enable radio button is selected.  
If the radio button is not selected, select it now, then click Apply.  
5. When prompted, restart the Cisco Security Manager Daemon Manager.  
6. Wait 5 minutes, then try again to use Security Manager Client.  
If you still cannot connect, consider the other possible problems that the error message describes. |
| Error - Cisco Security Agent Running | Cisco Security Agent needs to be stopped during the client installation. | • Click Yes to disable the Cisco Security Agent.  
• Click No to cancel the operation and stop the Cisco Security Agent manually.  
• Click Help to access online help for Security Manager client. |

The client cannot connect to the server. This can be caused by one of the following reasons:  
The server name is incorrect.  
The protocol (http, https) is incorrect.  
The server is not running.  
Network access issues. Please confirm that the server name and protocol are correct.  
The server is running and you are not experiencing network connectivity issues by loading the CS Manager home page in your browser.
What should I do if the client installer suspends operation (hangs)?

**A.** Try the following. Any one of them might solve the problem:

1. Navigate to C:\Program Files\Common Files\InstallShield\Universal\common\Gen1.
2. Rename the Gen1 folder, then try again to install Security Manager Client.
   If Gen1 is not present, rename common instead.

Errors occurred during the installation.

- null

- Only a Windows user whose login account has administrative privileges can install Security Manager Client.

Log in as a Windows administrator, then try again to install Security Manager Client.

Internet Explorer cannot download CSMClientSetup.exe from <server>. Internet Explorer was not able to open this Internet site. The requested site is either unavailable or cannot be found. Please try again later.

If the OS on your client system is Windows 2003, its Internet Explorer Enhanced Security default settings might stop you from downloading the client software installation utility from your server.

1. Select Start > Control Panel > Add or Remove Programs.
2. Click Add/Remove Windows Components.
3. When the Windows Component Wizard window opens, uncheck the Internet Explorer Enhanced Security Configuration check box, click Next, then click Finish.

Unable to Get Data

A database failure prevented successful completion of this operation.

You tried to use the client to connect to the server before the server database was completely up and running.

Wait a few minutes, then try again to log in. If the problem persists, verify that all required services are running.
If antivirus software is installed on your client system, disable it, then try again to run the installer.

Reboot the client system, then try again to run the installer.

Use a browser on the client system to log in to the Security Manager server at http://<server_name>:1741. If you see an error message that says “Forbidden” or “Internal Server Error,” the required Tomcat service is not running. Unless you rebooted your server recently and Tomcat has not had enough time yet to start running, you might have to review server logs or take other steps to investigate why Tomcat is not running.

Q. The installer says that a previous version of the client is installed and that it will be uninstalled. However, I do not have a previous version of the client installed. Is this a problem?

A. During installation or re-installation of the client, the installer might detect a previously installed client, even if no such client exists, and display an incorrect message that it will be uninstalled. This message is displayed because of the presence of certain old registry entries in your system. Although client installation proceeds normally when this message appears, use the Registry Editor to delete the following key to prevent this message from being displayed during subsequent installations: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Cisco Security Manager Client. (To open the Registry Editor, select Start > Run and enter regedit.) Also, rename the C:\Program Files\Zero G Registry\com.zerog.registry.xml file (any name will do).

Client Problems After Installation

Q. Why does the interface not look right?

A. An older video (graphics) card might fail to display the Security Manager GUI correctly until you upgrade its driver software. To test whether this problem might affect your client system, right-click My Computer, select Properties, select Hardware, click Device Manager, then expand the Display adapters entry. Double-click the entry for your adapter to learn what driver version it uses. You can then do one of the following:

- If your client system uses an ATI MOBILITY FireGL video card, you might have to obtain a video driver other than the driver that came with your card. The driver that you use must be one that allows you to configure Direct 3D settings manually. Any driver lacking that capability might stop your client system from displaying elements in the Security Manager GUI.

- For any video card, go to the web sites of the PC manufacturer and the card manufacturer to check for incompatibilities with the display of modern Java2 graphics libraries. In most cases where a known incompatibility exists, at least one of the two manufacturers provides a method for obtaining and installing a compatible driver.

Q. Why is the Security Manager Client missing from the Start menu in my Japanese version of Windows?

A. You might have configured the regional and language option settings to use English on the client system. We do not support English as the language in any Japanese version of Windows. Use the Control Panel to reset the language to Japanese.

Q. Why is the Security Manager Client missing from the Start menu for some or all the users on a workstation on which it is installed?

A. When you install the client, you select whether shortcuts will be created for just the user installing the product, for all users, or for no users. If you want to change your election after installation, you can do so manually by copying the Cisco Security Manager Client folder from Documents and
Troubleshooting the Security Manager Client

**Settings</user>\Start Menu\Programs\Cisco Security Manager to Documents and Settings\All Users\Start Menu\Programs\Cisco Security Manager. If you elected to not create shortcuts, you need to manually create the shortcut in the indicated All Users folder.

**Q.** What can I do if my connections from a client system to the server seem unusually slow, or if I see DNS errors when I try to log in?

**A.** You might have to create an entry for your Security Manager server in the *hosts* file on your client system. Such an entry can help you to establish connections to your server if it is not registered with the DNS server for your network. To create this helpful entry on your client system, use Notepad or any other plain text editor to open C:\WINDOWS\system32\drivers\etc\hosts. (The host file itself contains detailed instructions for how to add an entry.)

**Q.** What is wrong with my authentication setup if my login credentials are accepted without any error message when I try to log in with Security Manager Client, but the Security Manager desktop is blank and unusable? (Furthermore, does the same problem explain why, in my web browser, Common Services on my Security Manager server accepts my login credentials but then fails to load the Cisco Security Management Suite desktop?)

**A.** You did not finish all the required steps for Cisco Secure ACS to provide login authentication services for Security Manager and Common Services. Although you entered login credentials in ACS, you did not define the Security Manager server as a AAA client. You must do so, or you cannot log in. See the ACS documentation for detailed instructions.

**Q.** What should I do if I cannot use Security Manager Client to log in to the server and a message says...?

<table>
<thead>
<tr>
<th>... repeatedly that the server is checking its license.</th>
<th>Verify that your server meets the minimum hardware and software requirements. See <em>Server Requirements</em>, page 2-3.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Synchronizing with DCR.</strong></td>
<td>There are two possible explanations:</td>
</tr>
</tbody>
</table>

- You started Security Manager Client shortly after your server restarted. If so, allow a few more minutes for the server to become fully available, then try again to use Security Manager Client.

- Your CiscoWorks administrative password contains special characters, such as ampersands (&). As a result, the Security Manager installation failed to create a comUser.dat file in the NMSROOT\lib\classpath subdirectory on your server, where NMSROOT is the directory in which you installed Common Services (the default is C:\Program Files\CSCOpx):

  a. Either contact Cisco TAC for assistance in replacing comUser.dat or re-install Security Manager.

  b. Create a Common Services password that does not use special characters.
### Troubleshooting the Security Manager Client

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Q.</strong> Why is the Activity Report not displayed when I use Internet Explorer as my default browser?</td>
<td><strong>A.</strong> This problem occurs because of invalid registry key values or inaccuracies with the location of some of the dll files associated with Internet Explorer. For information on how to work around this problem, refer to the Microsoft Knowledge Base article 281679, which is available at this URL: <a href="http://support.microsoft.com/kb/281679/EN-US">http://support.microsoft.com/kb/281679/EN-US</a>.</td>
</tr>
<tr>
<td><strong>Q.</strong> How can I clear the server list from the Server Name field in the Login window?</td>
<td><strong>A.</strong> Edit csmserver.txt to remove unwanted entries. The file is in the directory in which you installed the Security Manager client. The default location is C:\Program Files\Cisco Systems\Cisco Security Manager Client.</td>
</tr>
<tr>
<td><strong>Q.</strong> The Security Manager client did not load because of a version mismatch. What does this mean?</td>
<td><strong>A.</strong> The Security Manager server version does not match the client version. To fix this, download and install the most recent client installer from the server.</td>
</tr>
<tr>
<td><strong>Q.</strong> Where are the client log files located?</td>
<td><strong>A.</strong> The client log files are located in C:\Program Files\Cisco Systems\Cisco Security Manager Client\logs. Each GUI session has its own log file.</td>
</tr>
<tr>
<td><strong>Q.</strong> How do I know if Security Manager is running in HTTPS mode?</td>
<td><strong>A.</strong> Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• After you log in to the server using a browser, look at the URL in the address field. If the URL starts with https, Security Manager is running in HTTPS mode.</td>
</tr>
<tr>
<td></td>
<td>• Go to Common Services &gt; Server &gt; Security &gt; Single Server Management &gt; Browser-Server Security Mode Setup. If you see Current Setting: Enabled, Security Manager is running in HTTPS mode. If the setting is Disabled, use HTTP.</td>
</tr>
<tr>
<td></td>
<td>• When logging in using the client, first try HTTPS mode (check the HTTPS checkbox). If you get the message “Login URL access is forbidden; Please make sure your protocol (HTTP, HTTPS) is correct,” the server is probably running in HTTP mode. Uncheck the HTTPS checkbox and try again.</td>
</tr>
</tbody>
</table>

---

Error - Unable to Check License on Server.

An attempt to check the license file on the Security Manager server has failed.

Please confirm that the server is running. If the server is running, please contact the Cisco Technical Assistance Center.

At least one of the following services did not start correctly. On the server, select **Start > Programs > Administrative Tools > Services**, right-click each service named below, then select **Restart** from the shortcut menu:

- Cisco Security Manager Daemon Manager
- Cisco Security Manager database engine
- Cisco Security Manager Tomcat Servlet Engine
- Cisco Security Manager VisiBroker Smart Agent
- Cisco Security Manager Web Engine

Wait 5 minutes, then try again to start Security Manager Client.
Q. How can I enable the Client Debug log level?

A. In the file client.info, which is located by default in C:\Program Files\Cisco Systems\Cisco Security Manager Client\jars, modify the DEBUG_LEVEL parameters to include DEBUG_LEVEL=ALL and then restart the Security Manager client.

Q. When working with a dual-screen setup, certain windows and popup messages always appear on the primary screen, even when the Security Manager client is running on the secondary screen. For example, with the client running on the secondary screen, windows such as the Policy Object Manager always open in the primary screen. Can I fix this?

A. This is a known issue with the way dual-screen support is implemented in certain operating systems. We recommend running the Security Manager client on the primary screen. You should launch the client after configuring the dual-screen setup.

If a window opens on the other screen, you can move it by pressing Alt+spacebar, followed by M; you can then use the arrow keys to move the window.

Q. I cannot install or uninstall any software on a client system. Why?

A. If you run an installation and an uninstallation simultaneously on the client system, even if they are for different applications, you corrupt the client system InstallShield database engine and are prevented from installing or uninstalling any software. For more information, log in to your Cisco.com account, then use Bug Toolkit to view CSCsd21722 and CSCsc91430.

Troubleshooting Bundled Cisco Security Agent

This section answers questions that you might ask about troubleshooting the standalone version of Cisco Security Agent that is installed in most cases when you install Security Manager server software.

Q. Under what circumstances might the standalone agent block network access to and from my server?

A. In broad terms, there are only two possibilities: Either malicious software is running on your server and the agent blocked it, or legitimate software on the server tried to do something that the agent misinterpreted as malicious. Both these problems can occur only if you previously set the agent security level to high and, in so doing, enabled an agent policy that is intended to detect and block the actions of untrusted rootkits. (The default setting is medium.)

We recommend that you investigate both possibilities to determine which of them is true in your case. Reading this log file should help you to identify the application whose actions the agent deemed suspicious: C:\Program Files\Cisco Systems\CSAgent\log\csalog.txt.

If your investigation shows that malicious software is running on the server, we recommend that you identify and eliminate whatever exploited vulnerabilities allowed the dangerous installation to occur. We further recommend that you wipe the server hard drive, then use the checklists and procedures in this guide to re-install everything.

If you discover that benign (harmless) software—such as a trustworthy antivirus tool or a known device driver that loads dynamically after a system restart—triggered the agent, you can do any of the following:

- Reset the agent security level to medium, then restart the server.
Troubleshooting Bundled Cisco Security Agent

Note

If you later set the agent security level again to high, the agent again considers the trusted and re-installed software to be untrustworthy and again blocks all network traffic.

- Uninstall the trusted software.
- Uninstall the agent. We recommend that you do never do this. See Uninstalling Bundled Cisco Security Agent, page B-2.
- Ask Cisco TAC to give you a revised agent. See Obtaining Documentation and Submitting a Service Request, page xii.

Another explanation is possible if the standalone agent blocks network access from your server. The Cisco Security Agent baseline policy for Windows users will not allow you to use Windows File Explorer to access any web page through HTTP.

Q. Why is Cisco Security Agent missing from the Start menu in my Japanese version of Windows?

A. You might have configured the regional and language option settings on the server to use English. We do not support English as the language in any Japanese version of Windows (see Server Requirements, page 2-3). Use the Control Panel to reset the language to Japanese.

Q. How can I verify that any Windows services that my standalone Cisco Security Agent might require are actually running on my server?

A. The standalone agent requires only one Windows service. Select Start > Settings > Control Panel > Administrative Tools > Services. You should see a running service called “Cisco Security Agent.”

Q. The red pennant icon for Cisco Security Agent changed in my Windows system tray. The icon now has a red circle partially superimposed over it. What does it mean?

A. Something has disabled the agent (for example, you turned it off) or it is broken. Restarting your server might cause the standalone agent to reset itself, or you can check whether a message in the log tells you exactly what happened. See C:\Program Files\CiscoSystems\CSAgent\log\csalog.txt.

Q. The agent has blocked a valid operation. What can I do?

A. You can choose any of these possible workarounds:

- Right-click the agent icon in the Windows system tray, then select the off option to disable the agent temporarily. When you complete the task, re-enable the agent.
- Uninstall the agent, even though we recommend that you do not uninstall it. See Uninstalling Bundled Cisco Security Agent, page B-2.
- Select Start > Programs > Cisco Systems > Cisco Security Agent > Cisco Security Agent Diagnostics to run the diagnostic utility.

If none of the workarounds is sufficient, you can open a case with Cisco TAC (see Obtaining Documentation and Submitting a Service Request, page xii).

Q. After I disable Cisco Security Agent so I can upgrade to a newer version of Security Manager, Cisco Security Agent is re-enabled, causing the upgrade to fail. What must I do?
Run a Server Self-Test

To run a self-test that confirms whether your Security Manager server is operating correctly:

**Step 1**
From a system on which Security Manager Client is connected to your Security Manager server, select Tools > Security Manager Administration.

**Step 2**
In the Administration window, click Server Security, then click any button. A new browser opens, displaying one of the security settings pages in the Common Services GUI, corresponding to the button you clicked.

**Step 3**
From the Common Services page, select Admin under the Server tab.

**Step 4**
In the Admin page TOC, click Selftest.

**Step 5**
Click Create.

**Step 6**
Click the SelfTest Information at <MM-DD-YYYY HH:MM:SS> link, where:
- MM-DD-YYYY is the current month, day, and year.
- HH:MM:SS is a timestamp that specifies the hour, minute, and second when you clicked Selftest.

**Step 7**
Read the entries in the Server Info page.

Collecting Server Troubleshooting Information

If you are experiencing problems with Security Manager, and you cannot resolve the problem after trying all the recommendations listed in the error message and reviewing this guide for a possible solution, use the Security Manager Diagnostics utility to collect server information.

The Security Manager Diagnostics utility collects server diagnostic information in a ZIP file, CSMDiagnostics.zip. You overwrite the file with new information each time you run Security Manager Diagnostics, unless you rename the file. The information in your CSMDiagnostics.zip file can help a Cisco technical support engineer to troubleshoot any problems that you might have with Security Manager or its related applications on your server.

**Tip**
Security Manager also includes an advanced debugging option that collects information about the configuration changes that have been made with the application. To activate this option, select Tools > Security Manager Administration > Debug Options, then check the Capture Discovery/Deployment Debugging Snapshots to File check box. Bear in mind that although the additional information saved to the diagnostics file may aid the troubleshooting effort, the file may contain sensitive information, such as passwords. You should change debugging levels only if the Cisco Technical Assistance Center (TAC) asks you to change them.
You can run Security Manager Diagnostics in either of two ways.

### From a Security Manager client system:

1. After you establish a Security Manager Client session to your server, click **Tools > Security Manager Diagnostics**, then click **OK**.
   
   The CSMDiagnostics.zip file is saved on your server in the $NMSROOT$/MDC/etc directory, where $NMSROOT$ is the directory in which you installed Common Services ($C:\Program Files\CSCOpx$, for example).

2. Click **Close**.

   **Note**: We recommend that you rename this file so it does not get overwritten each time you run this utility.

### From a Security Manager server:

1. Open a Windows command window, for example, by selecting **Start > Run**, then enter command.

2. Enter `C:\Program Files\CSCOpx\MDC\bin\CSMDiagnostics`. Alternatively, to save the ZIP file in a different location than $NMSROOT$/MDC/etc, enter `CSMDiagnostics drive:\path`. For example, `CSMDiagnostics D:\temp`.

### Viewing and Changing Server Process Status

To verify that the server processes for Security Manager are running correctly:

**Step 1**

From the CiscoWorks home page, select **Common Services > Server > Admin**.

**Step 2**

In the Admin page TOC, click **Processes**.

The Process Management table lists all server processes. Entries in the ProcessState column indicate whether a process is running normally.

**Step 3**

If a required process is not running, restart it. See **Restarting All Processes on Your Server**, page A-18.

**Note**: Only users with local administrator privileges can start and stop the server processes.

### Restarting All Processes on Your Server

**Note**: You must stop all processes, then restart them all, or this method does not work.

**Step 1**

At the command prompt, enter `net stop crmdmgtd` to stop all processes.

**Step 2**

Enter `net start crmdmgtd` to restart all processes.
Tip

Alternatively, you can select Start > Settings > Control Panel > Administrative Tools > Services, then restart Cisco Security Manager Daemon Manager.

Reviewing the Server Installation Log File

If responses from the server differ from the responses that you expect, you can review error and warning messages in the server installation log file.

Use a text editor to open C:\Ciscoworks_install_NNN.log, where NNN is a timestamp in the format YYYYMMDD_HHMMSS.

In most cases, the log file to review is the one that has either the highest number appended to its filename or has the most recent creation date.

For example, you might see log file error and warning entries that say:

ERROR: Cannot Open C:\PROGRA~1\CSCOpx/lib/classpath/ssl.properties at C:\PROGRA~1\CSCOpx\MDC\Apache\ConfigSSL.pl line 259.
INFO: Enabling SSL....
WARNING: Unable to enable SSL. Please try later....

Note

In the event of a severe problem, you can send the log file to Cisco TAC. See Obtaining Documentation and Submitting a Service Request, page xii.
Bundled Cisco Security Agent: Overview

Cisco Security Agent provides host-based intrusion prevention. Regarding Security Manager, there are two versions of Cisco Security Agent—external and bundled:

- **External Cisco Security Agent**—Cisco Security Agent that is not installed as part of the Cisco Security Manager installation.
- **Bundled Cisco Security Agent**—Cisco Security Agent that is installed as part of the Cisco Security Manager installation. Bundled Cisco Security Agent is sometimes referred to as a “customized, standalone agent” because it is customized for Security Manager and because Management Center for Cisco Security Agents is not installed; thus, it is standalone.

This appendix describes the bundled version of Cisco Security Agent that is frequently installed on a Security Manager server.

- General user documentation for Cisco Security Agent is on Cisco.com at: [http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html](http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html). However, the bundled agent on your server is customized for Security Manager. Because you cannot configure the bundled agent and because Management Center for Cisco Security Agents is not installed, some information in the documentation for Management Center for Cisco Security Agents does not apply.
- To understand and work around problems that you might have with the standalone agent, see Troubleshooting Bundled Cisco Security Agent, page A-15.

This appendix contains the following major sections:

- **The Basics**, page B-1
- **Understanding and Managing Security Level Settings**, page B-2
- **Uninstalling Bundled Cisco Security Agent**, page B-2
- **Cleaning Up an Unclean Agent**, page B-3

### The Basics

If your target server is not protected by external Cisco Security Agent when you start to install Security Manager, Security Manager under certain conditions installs bundled Cisco Security Agent, with predefined policies that you cannot change. See Cisco Security Agent, page 1-3.

Caution: Cisco Security Manager may not work as expected if external Cisco Security Agent (Cisco Security Agent that is not installed as part of the Cisco Security Manager installation) is installed on the server machine.
After installation, bundled Cisco Security Agent controls system operations with policies that allow or deny specific system actions. The agent checks whether an action is allowed or denied before any system resources are accessed and acted upon. The agent never interferes with your daily operations unless it detects what it considers to be a forbidden or unexpected system operation. Nonetheless, its rules are meant to protect your server from rootkits or similarly malicious software and are therefore very strict.


**Note**

If you think that Cisco Security Agent has blocked a valid operation, you can contact Cisco TAC. See [Obtaining Documentation and Submitting a Service Request, page xii](#).

### Agent Log Files

Three log files for the standalone agent are stored in the C:\Program Files\Cisco Systems\CSAgent\log subdirectory:

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSAgent-Install.log</td>
<td>installation log file</td>
</tr>
<tr>
<td>csalog.txt</td>
<td>general log file</td>
</tr>
<tr>
<td>securitylog.txt</td>
<td>security events log file</td>
</tr>
</tbody>
</table>

### Understanding and Managing Security Level Settings

You can right-click the agent icon in the server system tray to change the security level setting at any time. The security level setting determines whether the agent imposes high, medium, or low-security restrictions on your server, or if it imposes no restrictions. The default is medium. Every level that you might select provides a distinct balance between security and convenience.

If you set the agent security level to high, it prevents your server from accepting inbound connections on any UDP or TCP ports except the specific ports that Security Manager and Common Services use. In addition, if the level is high and if the agent detects an untrusted rootkit, all connections (inbound and outbound) are blocked.

### Uninstalling Bundled Cisco Security Agent

You can uninstall bundled Cisco Security Agent, in the process removing all restrictions that the agent imposes, but your server will be significantly more vulnerable and exposed to attack than it is when the agent is installed. We do not recommend that you uninstall Cisco Security Agent.

As a temporary alternative, you can right-click the agent icon in your server system tray, then select a lower security level setting or select the option that temporarily disables the standalone agent.

Another alternative is to reset bundled Cisco Security Agent, clearing its rootkit detection status. To reset the agent, select **Start > Programs > Cisco Systems > Cisco Security Agent > Reset Cisco Security Agent**.

To uninstall bundled Cisco Security Agent, select **Start > Programs > Cisco Security Agent > Uninstall Cisco Security Agent**. Uninstallation in this way requires a system restart.
Cleaning Up an Unclean Agent

You might find that while upgrading Security Manager, Cisco Security Agent remains active, even after you try to uninstall it.

If you cannot uninstall Cisco Security Agent, try to stop the Cisco Security Agent service:

- If you can stop the Cisco Security Agent service, follow the Procedure for Typical Cleanup, page B-3.
- If you can not stop the Cisco Security Agent service, follow the Procedure for Atypical Cleanup, page B-3.

Procedure for Typical Cleanup

If you cannot uninstall Cisco Security Agent, but you can stop the Cisco Security Agent service, follow these steps to uninstall Cisco Security Agent using a typical cleanup:

**Step 1** Remove Cisco Security Agent from Add/Remove programs.

If you try to remove the CSagent from Add/Remove Programs, and an error states the CSAgent cannot be removed, you should first delete the CSAgent entries in regedit before removing Cisco Security Agent from Add/Remove programs. See Procedure for Atypical Cleanup, page B-3.

**Step 2** Delete the Cisco Security Agent from Start > All Programs.

**Step 3** Manually remove the CSAgent folder from C:\Program Files\Cisco Systems.

**Step 4** Search the registry and delete all entries for the strings “CSAgent” and “Cisco Security Agent.” To access the registry, select Start > Run. Enter regedit in the Open field, then click Open.

**Step 5** Restart the server.

Procedure for Atypical Cleanup

If you cannot uninstall Cisco Security Agent, and you can not stop the Cisco Security Agent service, follow these steps to uninstall Cisco Security Agent using an a typical cleanup:

**Step 1** Search the registry and delete all entries for the strings “CSAgent” and “Cisco Security Agent.” To access the registry, select Start > Run. Enter regedit in the Open field, then click Open.

**Step 2** Delete the Cisco Security Agent from Start > All Programs.

**Step 3** Remove Cisco Security Agent from Add/Remove programs.

**Step 4** Manually remove the CSAgent folder from C:\Program Files\Cisco Systems.

**Step 5** Restart the server.

Manually Removing the CSAgent Version 5.2.0.282

If you cannot uninstall the CSAgent with Add/Remove programs, or if the Agent uninstall failed, do the following to remove the Agent manually:
Appendix B  Bundled Cisco Security Agent: Overview

Cleaning Up an Unclean Agent

**Step 1**
Boot up in SAFEMODE with networking for Windows machines (usually F8).

**Note**
If you are removing the agent from a system without IIS or Apache, go to Step 4.

**Step 2**
Run the following from a CMD shell in the ..\csagent\bin:

- **For IIS**
  csa_datafilter -u iis
- **For Apache 1.3**
  csa_datafilter -u apache13 <.conf file with full path name> <modules dir. path>
- **For Apache 2.0**
  csa_datafilter -u apache20 <.conf file with full path name> <modules dir. path>

**Step 3**
If the above scripts do not work, remove the filters manually as follows:

**For Apache 1.3**

a. Go to where Apache is installed (normally Program Files\apache).
b. Open apache\conf\httpd.conf using notepad.
c. Search for "csafilter".
d. Delete the the two lines that begin with:
   "loadmodule csafilter. . ."
   "addmodule mod_csafilter . . ."
e. Go to apache\modules and delete the following:
   mod_csafilter*.so

**For Apache 2**

Follow the steps noted for Apache 1_3, with the exception that no reference is made to "addmodule mod_csafilter. . ."

**For IIS**

a. Right-click My Computer, then select Manage.
b. Go to Services and Applications.
c. Right-click Internet Information Services, then select Properties.
d. Under Master Properties, select www service.
e. Edit and click the ISAPI Filters tab.
f. Highlight the csafilter, then select Remove.
g. Click OK.

**Step 4**
Net stop CSAgent in case some CSA agent services were started.

**Step 5**
Make sure the CSA agent icon (red pennant) does not appear in the system tray.

**Note**
If the Agent icon is shown, exit, right-click the red pennant, then click Exit Agent Panel.
Appendix B  Bundled Cisco Security Agent: Overview

Cleaning Up an Unclean Agent

Step 6  Delete the Program Files\Cisco (Systems)\CSAgent folder.

Step 7  Delete the following directory:
        Program Files\InstallShield Installation Information\{DE49974667B9-11D4-97CE-0050DA10E5AE}

Step 8  Delete the following driver files, which, depending on your operating system, might be located at
         Windows (or WINNT)\system32\drivers:
         – csacentr.sys
         – csafile.sys
         – csanet.sys
         – csareg.sys
         – csatdi.sys

Step 9  Delete all references to csagent in the Start Menu\Programs directory.

Step 10 Delete WINDOWS\system32\csauser.dll, which, depending on your operating system, might be located at
         WINNT\system32\.

        Note  Do not delete the entire key; remove only CSAUSER.DLL. Any other DLLs that are referenced
         in the AppInit_DLLs registry key are required by other programs and deleting them can cause
         system instability.

If you cannot delete this file, you must modify the registry key that loads this DLL, then reboot before you
         can delete it. To do this, follow these steps:
         a.  Open the registry editor by selecting Start > Run > regedit.
         b.  Go to HKLM > SOFTWARE > Microsoft > Windows NT > CurrentVersion > Windows.
         c.  Modify the AppInit_DLLs registry key and change the reference from csauser.dll to xyz.

        Note  It is possible that even after modifying the reference to xyz and rebooting the server, the
         csauser.dll file is still not deleted. If this occurs, skip the following substep and proceed with
         the next step.

         d.  Restart.

        Note  After removing csauser.dll from the AppInit_DLLs registry key, you must reboot before
         Windows allows you to delete the csauser.dll file.

Step 11 Delete WINNT or WINDOWS\system32\csafilter.dll, csa_uninstall.bat, csarule.dll (if they exist).

Step 12 Delete the reference to Cisco Security Agent in Start > Programs > Startup.

Step 13 Delete the following registry keys:
     •  HKLM > system > controlset001 > control > session manager > knowndlls > csasuser.dll
     •  HKLM > system > controlset002 > control > session manager > knowndlls > csasuser.dll
     •  HKLM > system > controlset003 > control > session manager > knowndlls > csasuser.dll (WinNT)
     •  HKLM > System > Currentcontrolset > Services > csacenter, csafile, csanet, csareg, csATDI,
         csagent, csafilter, csahook
Appendix B  Bundled Cisco Security Agent: Overview

Cleaning Up an Unclean Agent

- HKEY_Local_Machine > Software > Cisco > CSAgent
- HKEY_Local_Machine > Software > Cisco > CSAgentinstalled
- HKEY_Local_Machine > Software > Microsoft > windows > currentversion > uninstall > {DE499746-67B9-11D4-97CE-0050DA10E5AE}

Step 14  W2K, WINXP, W2K3

a. Remove references to any Cisco Security Agent* resource in the Windows Device Manager. (Go to Start > Control Panel > System > Hardware > Device Manager.) Make sure you select "show hidden devices" (View > Show hidden devices) and expand the non-plug and play devices section.

b. Right click each Cisco Security Agent* resource and uninstall it.

Note  Do not reboot until all the "Cisco Security Agent*" resources are uninstalled.

c. Restart. You must restart for the changes to take effect.

Step 15  For WINNT

a. Remove references to any "Cisco Security Agent*" resource in the Windows Device Manager.

b. Right-click each "Cisco Security Agent*" resource and uninstall it.

Note  Do not reboot until all the "Cisco Security Agent*" resources are uninstalled.

c. Restart. You must restart for the changes to take effect.

Step 16  Reboot the server and verify that all CSA resources are deleted in Windows Device Manager. (See Step 14.)

Step 17  Delete WINNT or WINDOWS\system32\csauser.dll after you reboot.

Step 18  Search the registry and delete all entries for the strings "CSAgent" and "Cisco Security Agent." To access the registry, select Start > Run. Enter regedit in the Open field, then click Open.

Some entries cannot be deleted.

Step 19  Verify that CSAgent is not listed in Control Panel > Add/Remove Programs.
Open Source License Notices for Cisco Security Manager

Notices

The following notices pertain to this software license:

- OpenSSL/Open SSL Project, page C-2
- Axis, page C-3
- Castor, page C-6
- cglib, page C-9
- Velocity, page C-12
- Apache Commons, page C-15
- ODMG, page C-18
- log4j, page C-19
- jdt-compiler-3.1.1.jar, page C-21
- jta-1.1.jar, page C-25
- slf4j-api-1.5.2.jar, page C-27
OpenSSL/OpenSSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).
Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

   The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Axis

Apache Axis is an implementation of the SOAP ("Simple Object Access Protocol") submission to W3C.

From the draft W3C specification:
“SOAP is a lightweight protocol for exchanging structured information in a decentralized, distributed environment. It is an XML-based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses.”

[http://ws.apache.org/axis/]

License

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.
"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."
"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
(b) You must cause any modified files to carry prominent notices stating that You changed the files; and
(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[ ]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

[http://www.apache.org/licenses/LICENSE-2.0]

Castor

Castor is an Open Source data binding framework for Java[tm]. It's the shortest path between Java objects, XML documents and relational tables. Castor provides Java-to-XML binding, Java-to-SQL persistence, and more.

[http://castor.codehaus.org/]
Appendix C
Open Source License Notices for Cisco Security Manager

License

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.
"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.
"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.
"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.
"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.
"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.
"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.
"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).
"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.
"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."
"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.
3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
(b) You must cause any modified files to carry prominent notices stating that You changed the files; and
(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
(d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
Appendix C      Open Source License Notices for Cisco Security Manager

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!)
The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

[cglib]
cglib is a powerful, high performance and quality Code Generation Library, It is used to extend JAVA classes and implements interfaces at runtime.

[http://cglib.sourceforge.net/]

License

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION
1. Definitions.
"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution

incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
(b) You must cause any modified files to carry prominent notices stating that You changed the files; and
(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at
http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

[http://www.apache.org/licenses/LICENSE-2.0]

Velocity

Velocity is a project of the Apache Software Foundation, charged with the creation and maintenance of open-source software related to the Apache Velocity Engine.

[http://velocity.apache.org/]

Velocity is a Java-based template engine. It permits anyone to use a simple yet powerful template language to reference objects defined in Java code.

When Velocity is used for web development, web designers can work in parallel with Java programmers to develop websites according to the Model-View-Controller (MVC) model, meaning that web page designers can focus solely on creating a site that looks good, and programmers can focus solely on writing top-notch code.

[http://velocity.apache.org/engine/releases/velocity-1.6.2/]

License

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION
1. Definitions.
"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution
incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

[http://www.apache.org/licenses/LICENSE-2.0]

Apache Commons

The Commons is an Apache project focused on all aspects of reusable Java components.

[http://commons.apache.org/]

Components

The following components of Apache Commons pertain to this software license:

- Beanutils
- CLI
- Collections
- DbUtils
- Digester
- Lang
- Logging

License

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s)
with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any
entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution
incorporated within the Work constitutes direct or contributory patent infringement, then any patent
licenses granted to You under this License for that Work shall terminate as of the date such litigation is
filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in
any medium, with or without modifications, and in Source or Object form, provided that You meet the
following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
(b) You must cause any modified files to carry prominent notices stating that You changed the files; and
(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent,
trademark, and attribution notices from the Source form of the Work, excluding those notices that do not
pertain to any part of the Derivative Works; and
(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that
You distribute must include a readable copy of the attribution notices contained within such NOTICE
file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the
following places: within a NOTICE text file distributed as part of the Derivative Works; within the
Source form or documentation, if provided along with the Derivative Works; or, within a display
generated by the Derivative Works, if and wherever such third-party notices normally appear. The
contents of the NOTICE file are for informational purposes only and do not modify the License. You
may add Your own attribution notices within Derivative Works that You distribute, alongside or as an
addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot
be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or
different license terms and conditions for use, reproduction, or distribution of Your modifications, or for
any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work
otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally
submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of
this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall
supersede or modify the terms of any separate license agreement you may have executed with Licensor
regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service
marks, or product names of the Licensor, except as required for reasonable and customary use in
describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides
the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT
WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without
limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or
FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the
appropriateness of using or redistributing the Work and assume any risks associated with Your exercise
of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence),
contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts)
or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect,
special, incidental, or consequential damages of any character arising as a result of this License or out
of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work
stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if
such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at
http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

[http://www.apache.org/licenses/LICENSE-2.0]

ODMG

ODMG is a standard API for Object Persistence specified by the ODMG consortium (www.odmg.org).
[http://db.apache.org/ojb/docu/faq.html#relatedTo]

Availability


License

License Agreement
Redistribution of this software is permitted provided that the following conditions are met:
1. Redistributions of source or binary code formats must retain the above copyright notice.
2. Redistribution in any product and all advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes copyrighted software developed by E. Wray Johnson for use and distribution by the Object Data Management Group (http://www.odmg.org)/." [http://www.odbms.org/ODMG/OG/wrayjohnson.aspx]
log4j

log4j is open-source logging software for java related to the logging of application behavior.

[http://logging.apache.org/]

License

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."
"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

jdt-compiler-3.1.1.jar

jdt-compiler-3.1.1.jar is included in JDT Core, which is the Java infrastructure of the Java IDE. [http://www.eclipse.org/jdt/core/index.php]

Core is in turn a component of the Eclipse Java development tools (JDT) project. The JDT project provides the tool plug-ins that implement a Java IDE supporting the development of any Java application, including Eclipse plug-ins. [http://www.eclipse.org/jdt/index.php]
License

Eclipse Public License - v 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS ECLIPSE PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program; where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS
A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must:

a) promptly notify the Commercial Contributor in writing of such claim, and

b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A
PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient’s rights granted under Section 2(b) shall terminate as of the date such litigation is filed. All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient’s rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. The Eclipse Foundation is the initial Agreement Steward. The Eclipse Foundation may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

jta-1.1.jar

jta-1.1.jar is included in Java Transaction API (JTA), which specifies standard Java interfaces between a transaction manager and the parties involved in a distributed transaction system: the resource manager, the application server, and the transactional applications.


License

SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THIS SPECIFICATION TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS AGREEMENT. PLEASE READ THE TERMS AND CONDITIONS OF THIS AGREEMENT CAREFULLY. BY DOWNLOADING THIS SPECIFICATION, YOU ACCEPT THE TERMS AND CONDITIONS OF THE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY IT, SELECT THE "DECLINE" BUTTON AT THE BOTTOM OF THIS PAGE.


Version: 1.1
Status: Maintenance Release
Release: 14 February 2007
Copyright 2007 SUN MICROSYSTEMS, INC.
4150 Network Circle, Santa Clara, California 95054, U.S.A
All rights reserved.

LIMITED LICENSE GRANTS

1. License for Evaluation Purposes. Sun hereby grants you a fully-paid, non-exclusive, non-transferable, worldwide, limited license (without the right to sublicense), under Sun's applicable intellectual property rights to view, download, use and reproduce the Specification only for the purpose of internal evaluation. This includes (i) developing applications intended to run on an implementation of the Specification, provided that such applications do not themselves implement any portion(s) of the Specification, and (ii) discussing the Specification with any third party; and (iii) excerpting brief portions of the Specification in oral or written communications which discuss the Specification provided that such excerpts do not in the aggregate constitute a significant portion of the Specification.

2. License for the Distribution of Compliant Implementations. Sun also grants you a perpetual, non-exclusive, non-transferable, worldwide, fully paid-up, royalty free, limited license (without the right to sublicense) under any applicable copyrights or, subject to the provisions of subsection 4 below, patent rights it may have covering the Specification to create and/or distribute an Independent Implementation of the Specification that: (a) fully implements the Specification including all its required interfaces and functionality; (b) does not modify, subset, superset or otherwise extend the Licensor Name Space, or include any public or protected packages, classes, Java interfaces, fields or methods within the Licensor Name Space other than those required/authorized by the Specification or Specifications being implemented; and (c) passes the Technology Compatibility Kit (including satisfying the requirements of the applicable TCK Users Guide) for such Specification ("Compliant Implementation"). In addition, the foregoing license is expressly conditioned on your not acting outside its scope. No license is granted hereunder for any other purpose (including, for example, modifying the Specification, other than to the extent of your fair use rights, or distributing the Specification to third parties). Also, no right, title, or
interest in or to any trademarks, service marks, or trade names of Sun or Sun's licensors is granted hereunder. Java, and Java-related logos, marks and names are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

3. Pass-through Conditions. You need not include imitations (a)-(c) from the previous paragraph or any other particular "pass through" requirements in any license You grant concerning the use of your Independent Implementation or products derived from it. However, except with respect to Independent Implementations (and products derived from them) that satisfy limitations (a)-(c) from the previous paragraph, You may neither: (a) grant or otherwise pass through to your licensees any licenses under Sun's applicable intellectual property rights; nor (b) authorize your licensees to make any claims concerning their implementation's compliance with the Specification in question.


a. With respect to any patent claims covered by the license granted under subparagraph 2 above that would be infringed by all technically feasible implementations of the Specification, such license is conditioned upon your offering on fair, reasonable and non-discriminatory terms, to any party seeking it from You, a perpetual, non-exclusive, non-transferable, worldwide license under Your patent rights which are or would be infringed by all technically feasible implementations of the Specification to develop, distribute and use a Compliant Implementation.

b. With respect to any patent claims owned by Sun and covered by the license granted under subparagraph 2, whether or not their infringement can be avoided in a technically feasible manner when implementing the Specification, such license shall terminate with respect to such claims if You initiate a claim against Sun that it has, in the course of performing its responsibilities as the Specification Lead, induced any other entity to infringe Your patent rights.

c. Also with respect to any patent claims owned by Sun and covered by the license granted under subparagraph 2 above, where the infringement of such claims can be avoided in a technically feasible manner when implementing the Specification such license, with respect to such claims, shall terminate if You initiate a claim against Sun that its making, having made, using, offering to sell, selling or importing a Compliant Implementation infringes Your patent rights.

5. Definitions. For the purposes of this Agreement: "Independent Implementation" shall mean an implementation of the Specification that neither derives from any of Sun's source code or binary code materials nor, except with an appropriate and separate license from Sun, includes any of Sun's source code or binary code materials; "Licensor Name Space" shall mean the public class or interface declarations whose names begin with "java", "javax", "com.sun" or their equivalents in any subsequent naming convention adopted by Sun through the Java Community Process, or any recognized successors or replacements thereof; and "Technology Compatibility Kit" or "TCK" shall mean the test suite and accompanying TCK User's Guide provided by Sun which corresponds to the Specification and that was available either (i) from Sun's 120 days before the first release of Your Independent Implementation that allows its use for commercial purposes, or (ii) more recently than 120 days from such release but against which You elect to test Your implementation of the Specification.

This Agreement will terminate immediately without notice from Sun if you breach the Agreement or act outside the scope of the licenses granted above.

DISCLAIMER OF WARRANTIES

THE SPECIFICATION IS PROVIDED "AS IS". SUN MAKES NO REPRESENTATIONS OR WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT (INCLUDING AS A CONSEQUENCE OF ANY PRACTICE OR IMPLEMENTATION OF THE SPECIFICATION), OR THAT THE CONTENTS OF THE SPECIFICATION ARE SUITABLE FOR ANY PURPOSE. This document does not represent any commitment to release or implement any portion of the Specification in any product. In addition, the Specification could include technical inaccuracies or typographical errors.
LIMITATION OF LIABILITY

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION, LOST REVENUE, PROFITS OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED IN ANY WAY TO YOUR HAVING, IMPLEMENTING OR OTHERWISE USING USING THE SPECIFICATION, EVEN IF SUN AND/OR ITS LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. You will indemnify, hold harmless, and defend Sun and its licensors from any claims arising or resulting from: (i) your use of the Specification; (ii) the use or distribution of your Java application, applet and/or implementation; and/or (iii) any claims that later versions or releases of any Specification furnished to you are incompatible with the Specification provided to you under this license.

RESTRICTED RIGHTS LEGEND

U.S. Government: If this Specification is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in the Software and accompanying documentation shall be only as set forth in this license; this is in accordance with 48 C.F.R. 227.7201 through 227.7202-4 (for Department of Defense (DoD) acquisitions) and with 48 C.F.R. 2.101 and 12.212 (for non-DoD acquisitions).

REPORT

If you provide Sun with any comments or suggestions concerning the Specification ("Feedback"), you hereby: (i) agree that such Feedback is provided on a non-proprietary and non-confidential basis, and (ii) grant Sun a perpetual, non-exclusive, worldwide, fully paid-up, irrevocable license, with the right to sublicense through multiple levels of sublicensees, to incorporate, disclose, and use without limitation the Feedback for any purpose.

GENERAL TERMS

Any action related to this Agreement will be governed by California law and controlling U.S. federal law. The U.N. Convention for the International Sale of Goods and the choice of law rules of any jurisdiction will not apply.

The Specification is subject to U.S. export control laws and may be subject to export or import regulations in other countries. Licensee agrees to comply strictly with all such laws and regulations and acknowledges that it has the responsibility to obtain such licenses to export, re-export or import as may be required after delivery to Licensee. This Agreement is the parties' entire agreement relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, conditions, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification to this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

Rev. April, 2006

[https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/CDS-CDS_Developer-Site/en_US/-/USD/View License-Start]

slf4j-api-1.5.2.jar

slf4j-api-1.5.2.jar is included in the Simple Logging Facade for Java (SLF4J), which serves as a simple facade or abstraction for various logging frameworks, e.g., java.util.logging, log4j, and logback.

[http://www.slf4j.org/]
License

Licensing terms for SLF4J

SLF4J source code and binaries are distributed under the MIT license.

Copyright (c) 2004-2008 QOS.ch
All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

These terms are identical to those of the MIT License, also called the X License or the X11 License, which is a simple, permissive non-copyleft free software license. It is deemed compatible with virtually all types of licenses, commercial or otherwise. In particular, the Free Software Foundation has declared it compatible with GNU GPL. It is also known to be approved by the Apache Software Foundation as compatible with Apache Software License.

[http://www.slf4j.org/license.html]
INDEX

A

Access Control Server (ACS)
activating NDG feature 7-15
adding devices as AAA clients without NDGs 7-13
adding managed devices 7-13
adding managed devices and configuring NDGs 7-22
adding multihomed devices 7-26
adding users 7-11
assigning roles to user groups 7-21
assigning roles to user groups with NDGs 7-22
assigning roles to user groups without NDGs 7-21
associating user roles and permissions 7-7
authentication fails 7-24
changes not appearing in Security Manager 7-25
configuring CiscoWorks AAA mode 7-18
configuring network device groups 7-14
configuring SMTP and e-mail for notifications 7-20
creating administration control user 7-16
creating local users in CiscoWorks 7-17
creating network device groups 7-15
customizing user roles 7-6
default roles 7-6
defining system identity user 7-11
devices not appearing in Security Manager 7-25
integrating with Security Manager 7-8
integration checklist 7-10
integration requirements 7-9
performing integration 7-11
performing integration in CiscoWorks 7-17
read-only access for system administrators 7-24
registering Security Manager 7-19
reinstalling server applications 4-4
restarting Daemon Manager 7-20
restoring access 7-26
troubleshooting 7-23
understanding user permissions 7-1
user permissions 7-2
using multiple versions of Security Manager 7-23
working after ACS becomes unreachable 7-25
accounts, user
managing 7-1
required 4-1
antivirus utilities, requirement to disable 3-4
applications
downgrading server 4-19
installing and configuring client 5-1
installing and upgrading server 4-1
logging into 5-9
required changes after upgrading server 4-14
uninstalling server 4-18
upgrading server 4-9
approve permissions 7-3
approver role 7-4
assign permissions 7-3
authorization, changes in ACS for devices 7-25
Auto Update Server (AUS)
installing 4-3
licensing 1-7
logging into 5-10
overview 1-2
required user accounts 4-1
server requirements 2-3
uninstalling 4-18
upgrading 4-9
### B

**backup**
- committing pending data before performing: 4-11
- Cygwin limitations: A-5
- database: 4-12

**backup/restore upgrade path, definition of**: 4-9

**back up database**: 4-12

**bootstrapping devices**: 6-4

**browsers**
- configuring required settings: 5-1
- configuring required settings for Firefox: 5-3
- configuring required settings for Internet Explorer: 5-2
- logging into applications: 5-10
- supported: 2-6, 2-8

**Bundled Cisco Security Agent, definition of**: 1-3, B-1

### C

**certificates**
- requirement to create: 6-1
- troubleshooting: 3-4

**Cisco Security Agent (CSA)**
- cleaning an unclean agent: B-3
- importing policies into full version: 3-2
- installation, conditions for: 1-3
- installing: 4-3
- logs: B-2
- manually removing: B-4
- overview: 1-3
- policies for Bundled Cisco Security Agent: B-1
- security levels: B-2
- troubleshooting: A-15
- uninstalling: B-2
- upgrading: 4-9

**Cisco Security Management Suite**
- adding applications to home page: 4-18

**CiscoWorks Common Services**
- assigning roles to users: 7-5
- associating user roles and permissions: 7-7
- available user roles: 7-4
- configuring AAA mode: 7-18
- creating administration control user in ACS: 7-16
- creating local user for Cisco Secure ACS: 7-17
- defining system identity user: 7-18
- installing: 4-3
- licensing: 1-7
- logging into: 5-10
- overview: 1-1
- performing integration for Cisco Secure ACS: 7-17
- registering Security Manager with Cisco Secure ACS: 7-19
- required version: 1-1
- understanding user permissions: 7-1
- uninstalling: 4-18
- upgrading: 4-9

**client**
- clearing server list in Login window: A-14
- log files: A-14
- operating systems: 2-7
- requirements: 2-7
- troubleshooting after installation: A-12
- troubleshooting installation: A-9

**Compatibility View in Internet Explorer 8**: 2-6, 2-8

**control permissions**: 7-3

**Cygwin problems during database backup**: A-5

### D

**Daemon Manager**
- restarting after Cisco Secure ACS integration: 7-20

**database**
- backing up: 4-12
- committing pending data before upgrade: 4-11
- restoring: 4-13
- date and time settings: 2-1, 3-4
- deploy permissions: 7-3
devices
  bootstrapping 6-4
  changes to ACS authorization not appearing in Security Manager 7-25
directory encryption, restriction against 2-4
documentation
  Common Services  i-xi
  Resource Manager Essentials (RME)  i-xii
  Security Manager, AUS, Performance Monitor  i-xi
domain controllers (primary or backup), unsupported use 2-4
dual-screen setups  A-15

E
  e-mail address, Security Manager administrator 7-20
  encrypted directories, restriction against 2-4
  error messages
    client installation  A-9
    server installation  A-4
    server uninstallation  A-8
External Cisco Security Agent, definition of 1-3, B-1

F
  Firefox
    cache size requirement 5-3
    configuring required settings 5-3
    disabling popup blocker 5-4
    displaying help in new tab 5-4
    editing the preferences file 5-3
    enabling Javascript 5-4
    supported versions 2-6, 2-8
  for more information 6-4

H
  help desk user role 7-4
  home page, adding applications to 4-18

HTTP, configuring non-default port 5-8
HTTPS
  configuring non-default port 5-8
  determining mode  A-14

I
  import permissions 7-3
  indirect upgrade path, definition of 4-9
installation
  Performance Monitor 4-5
  RME 4-7
  Security Manager, AUS, Common Services 4-3
  Security Manager client 5-6
  security settings that prevent client troubleshooting 5-7
  troubleshooting client  A-9
  troubleshooting server  A-4
  using remote desktop or VNC 4-2
  verifying 6-3
  Internet Explorer
    cache size requirement 5-2
    configuring required settings 5-2
    security settings 5-2
    supported versions 2-6, 2-8
  Internet Explorer 8 Compatibility View 2-6, 2-8
  Internet Information Server (IIS), requirement to uninstall 3-3

J
  Java requirements 2-8

L
  language support 2-7
  LAN Management Solution (LMS), unsupported use 3-3
  LiaisonServlet error, troubleshooting  A-6
  licenses
    effect of upgrade 1-6
Index

how handled during product upgrade 4-9
obtaining 1-6
overview 1-5
Product Authorization Key (PAK) 1-6
Security Manager kit part numbers 1-6
Software License Claim Certificate 1-6
understanding 1-5
updating 4-16
local upgrade path, definition of 4-9
log files A-19

M

memory (RAM)
  client requirements 2-7
modify permissions 7-2

N

Network Access Restriction (NAR) 7-9
network administrator role
  Cisco Secure ACS 7-6
  CiscoWorks 7-4
network device groups (NDGs)
  activating NDG feature 7-15
  associating with roles and user groups 7-22
  configuring 7-14
  creating 7-15
  effect on user permissions 7-14
network operator role 7-4

O

operating systems
  client 2-7
overview 1-1

P

pdshow command 6-2
pending data, committing 4-11
performance
  client recommendations 2-7
  server best practices 3-1
  server recommendations 2-3
Performance Monitor
  installing 4-5
  licensing 1-7
  logging into 5-10
  overview 1-3
  required user accounts 4-1
  server requirements 2-3
uninstalling 4-18
updating licenses 4-16
upgrading 4-9
permanent license, upgrading from evaluation license 1-6
permissions
  assigning roles in CiscoWorks 7-5
  associating with user roles 7-7
  categories 7-2
  customizing for ACS 7-6
  impact of NDGs 7-14
  understanding 7-1
point patches
  applying to a client 5-9
  obtaining 4-17
popup blocker
  disabling 5-5
  disabling for Firefox 5-4
ports
  comprehensive list of required TCP/UDP A-2
  configuring non-default HTTP/HTTPS 5-8
  list of typically required 2-1
processes
  restarting server A-18
  troubleshooting A-18
verifying 6-2
product registration 1-6
property files 4-11

R
remote desktop, using for installation 4-2
remote upgrade path, definition of 4-9
requirements
  client 2-7
    data and time settings 2-1, 3-4
  general server 2-1
  server 2-3
  unsupported server configurations 2-4
Resource Manager Essentials (RME)
  documentation i-xii
  installing 4-7
  licensing 1-7
  logging into 5-10
  required user accounts 4-1
  server requirements 2-3
  uninstalling 4-18
  updating licenses 4-16
  upgrading 4-9
restorebackup.pl command 4-13
restore database 4-13
roles
  Cisco Secure ACS users 7-5
  CiscoWorks users 7-4

S
Security 1-2
security
  server best practices 3-1
  security administrator role 7-6
  security approver role 7-6
Security Manager
  committing pending data before upgrade 4-11
  component applications 1-1
  downgrading server 4-1
  getting started with 6-4
  installing 4-3
  licenses
    effect on upgrade 1-6
    obtaining 1-6
    overview 1-5
    understanding 1-5
  logging in using browser 5-10
  logging in using client 5-10
  overview 1-2
  related applications 1-4
  required changes after upgrade 4-14
  required user accounts 4-1
  restarting Daemon Manager 7-20
  server requirements 2-3
  service startup requirements A-1
  troubleshooting interaction with ACS 7-23
  uninstalling server 4-18
  updating licenses 4-16
  upgrading server 4-9
Security Manager client
  clearing server list in Login window A-14
  configuring non-default HTTP/HTTPS port 5-8
  determining HTTPS mode A-14
  handling security settings that prevent installation 5-7
  installing 5-6
  locating client logs A-14
  logging into 5-10
  patching 5-9
  resolving version mismatch A-14
  running in dual-screen mode A-15
  unable to upgrade 5-8
  uninstalling 5-11
server
  best practices for security 6-3
Index

date and time settings 2-1, 3-4
general requirements 2-1
performance, best practices for enhancing 3-1
post installation tasks 6-1
preparation checklists 3-1
readiness checklist 3-4
requirements 2-3
security, best practices for enhancing 3-1
troubleshooting post-installation problems A-5
unsupported configurations 2-4
verifying processes 6-2
service packs
applying to a client 5-9
obtaining 4-17
services, minimum required for Windows 3-3
service startup requirements A-1
SMTP, configuring for ACS notifications 7-20
SSL certificate invalidation 3-4
submit permissions 7-3
Sybase, requirement to disable 3-4
system administrator role 7-4
system identity user 7-11, 7-18

T

TACACS+
selecting as CiscoWorks AAA mode 7-18
using ACS as 7-8
TCP
comprehensive list of required ports A-2
list of typically required ports 2-1
Terminal Services, unsupported configuration 2-4
troubleshooting
ACS configurations 7-23
antivirus scanners 3-2
Cisco Security Agent
blocking a valid operation A-16
blocking network access A-15
icon appearance changed in system tray A-16
client after installation A-12
client installation A-9
client installer says old version is installed when it is not A-12
collecting server troubleshooting information A-17
Cygwin prevents backup A-5
dual-screen setups A-15
error messages
client installation A-9
server installation A-4
server uninstallation A-8
host-based intrusion software 3-2
incorrect interface appearance A-5
installation does not run A-15
installation hangs A-5, A-11
invalid SSL certificate 3-4
java.security.cert errors 3-4
LiaisonServlet error A-6
mapped drives A-7
missing drives A-5
overview A-1
restarting server processes A-18
reviewing installation log files A-19
security settings that prevent installation 5-7
security software conflicts 3-2
server installation A-4
server problems after installation A-5
server processes A-18
server self-test A-17
server uninstall A-8
unable to upgrade client 5-8
uninstallation does not run A-15
uninstallation hangs A-9

T

typographical conventions in this document i-x

U

UDP

comprehensive list of required ports A-2
Index

Installation Guide for Cisco Security Manager 4.0.1

list of typically required ports 2-1
uninstallation
   recommendation to restart servers 4-19
   Security Manager client 5-11
   server applications 4-18
   troubleshooting server A-8
upgrade, verifying 6-3
user accounts
   admin 4-1
   casuser 4-1
   creating 4-1
   managing 7-1
System Identity 4-2
user permissions
   assigning roles in CiscoWorks 7-5
   associating with user roles 7-7
   categories 7-2
   customizing for ACS 7-6
   impact of NDGs 7-14
   understanding 7-1
user roles
   associating with user permissions 7-7
   available CiscoWorks user roles 7-4
   Cisco Secure ACS 7-5
   CiscoWorks 7-4
   default ACS roles 7-6

V
version mismatch, resolving A-14
view permissions 7-2
VMware 4-5
VMWare supported versions 2-6
VNC, using for installation 4-2

W
web browsers