Installation Guide for Cisco Security Manager 4.18

First Published: Published: August, 2018

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number:

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Installation Guide for Cisco Security Manager 4.18

© 2018 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface ix

Audience ix

Conventions x

Product Documentation x

Obtain Documentation and Submit a Service Request 3-xi

3-xi

CHAPTER 1 **Overview** 1-1

Introduction to Component Applications 1-1

Common Services 1-1

Security Manager 1-2

Auto Update Server 1-3

Introduction to Related Applications 1-3

Effect of Enabling Event Management 1-4

CHAPTER 2 **Licensing for Security Manager** 2-1

License Types 2-1

Base Licenses (Standard and Professional) 2-1

Standard-to-Professional Upgrade License 2-3

Incremental ("Add-on") Licenses 2-3

API License 2-3

Licensing and Deployment Scenarios 2-3

Active/Active 2-3

Active and Standby 2-3

License Types and Applicability 2-4

Licenses for Component Applications 2-4

Understanding Device Count for Purchasing License 2-4

Example for any Standalone Firewall Blade in Multi-context Mode 2-7

Example for Licenses Related to ASA Load Balancing Clusters 2-7

Determining Which License You Need 2-8

New Installation of Security Manager 4.18 2-8

Upgrade from Security Manager 4.x 2-8

90-day Evaluation License 2-8
Choosing the Right License when you are a New 4.x Customer 2-8
Choosing the Right License when you are an Existing 4.x Customer 2-9
Installing a License for Security Manager or Component Applications 2-9
Updating a License for Security Manager or Component Applications 2-10
Additional Documentation on Licensing 2-10
Getting Help with Licensing 2-10

CHAPTER 3 **Requirements and Dependencies** 3-1
Required Services and Ports 3-1
Windows Firewall Configuration Script 3-3
Server Requirements and Recommendations 3-4
Understanding Regional and Language Options and Related Settings 3-9
Using SAN Storage 3-10
Requirement for iSCSI Volumes 3-10
Client Requirements 3-11

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

CHAPTER 5 **Installing and Upgrading Server Applications** 5-1
Understanding the Required Server User Accounts 5-1
Using Remote Desktop Connection or VNC To Install Server Applications 5-2
Installing Security Manager Server, Common Services, and AUS 5-3
Upgrading Server Applications 5-6
Ensuring Security Manager Pending Data is Submitted and Approved 5-16
Restoring Changes that You Made to Property Files 5-17
Editing the csm.properties File After a Remote Upgrade 5-17
Backing Up the Database for Remote Upgrades 5-18
Backing Up the Server Database By Using the CLI 5-19
Restoring the Server Database 5-21
Making Required Changes After Upgrade 5-22
Migrating Security Manager to a New Computer or Operating System 5-22
Updating Security Manager 5-24
Obtaining Service Packs and Point Patches 5-25
Uninstalling Server Applications 5-25

Downgrading Server Applications 5-26

CHAPTER 6 **Installing and Configuring the Client 6-1**

Configuring Web Browser Clients 6-1
HTTP/HTTPS Proxy Exception 6-1
Configuring Browser Cookies 6-2
Configuring Internet Explorer Settings 6-2
Configuring Firefox Settings 6-3
Editing the Preferences File 6-3
Editing the Size of the Disk Cache 6-4
Disabling the Popup Blocker or Creating a White List 6-4
Enabling JavaScript 6-4
Displaying Online Help on a New Tab in the Most Recent Window and Reusing Existing Windows on Subsequent Requests 6-5
Enabling and Configuring Exceptions in Third-party Tools 6-5
Tips for Installing the Security Manager Client 6-5
Installing the Security Manager Client 6-6
Handling Security Settings That Prevent Installation 6-9
Configuring a Non-Default HTTP or HTTPS Port 6-9
Unable to Upgrade From a Previous Version of the Client 6-9
Patching a Client 6-10
Logging In to the Applications 6-10
Logging In to Security Manager Using the Security Manager Client 6-10
Logging In to Server Applications Using a Web Browser 6-12
Uninstalling Security Manager Client 6-12

CHAPTER 7 **Post-Installation Server Tasks 7-1**

Server Tasks To Complete Immediately 7-1
Verifying that Required Processes Are Running 7-2
Configuration of Heap Sizes for Security Manager Processes using MRF 7-2
Default Configuration 7-3
Configuration Commands 7-4
Configuring Heap Sizes for Processes 7-4
1. Save Existing Configuration 7-4
2. Read Existing Configuration 7-5
3. Modify Configuration 7-5
Summary of Configuring Heap Sizes for Processes 7-6
Typical scenarios in which the User Might Have to Reconfigure Heap Sizes 7-6
Scenario 1 7-6

Scenario 2 7-7
Scenario 3 7-7
Scenario 4 7-7
Best Practices for Ongoing Server Security 7-7
Verifying an Installation or an Upgrade 7-8
(Optional) Changing the Hostname of the Security Manager Server 7-8
Where To Go Next 7-9

CHAPTER 8 **Managing User Accounts** 8-1
Account Creation 8-1
Local Account 8-1
ACS Account 8-2
Non-ACS Account 8-2
User Permissions 8-3
Security Manager ACS Permissions 8-4
Understanding CiscoWorks Roles 8-6
CiscoWorks Common Services Default Roles 8-6
Selecting an Authorization Type and Assigning Roles to Users in Common Services 8-7
Understanding Cisco Secure ACS Roles 8-9
Cisco Secure ACS Default Roles 8-10
Customizing Cisco Secure ACS Roles 8-10
Default Associations Between Permissions and Roles in Security Manager 8-11
Integrating Security Manager with Cisco Secure ACS 8-12
ACS Integration Requirements 8-13
Procedural Overview for Initial Cisco Secure ACS Setup 8-14
Integration Procedures Performed in Cisco Secure ACS 8-15
Defining Users and User Groups in Cisco Secure ACS 8-15
Adding Managed Devices as AAA Clients in Cisco Secure ACS 8-17
Creating an Administration Control User in Cisco Secure ACS 8-20
Integration Procedures Performed in CiscoWorks 8-21
Creating a Local User in CiscoWorks 8-21
Defining the System Identity User 8-22
Configuring the AAA Setup Mode in CiscoWorks 8-23
Configuring an SMTP Server and System Administrator Email Address for ACS Status Notifications 8-24
Restarting the Daemon Manager 8-25
Assigning Roles to User Groups in Cisco Secure ACS 8-25
Assigning Roles to User Groups Without NDGs 8-25
Associating NDGs and Roles with User Groups 8-26

Troubleshooting Security Manager-ACS Interactions 8-28
Using Multiple Versions of Security Manager with Same ACS 8-28
Authentication Fails When in ACS Mode 8-29
System Administrator Granted Read-Only Access 8-29
ACS Changes Not Appearing in Security Manager 8-30
Devices Configured in ACS Not Appearing in Security Manager 8-30
Working in Security Manager after Cisco Secure ACS Becomes Unreachable 8-30
Restoring Access to Cisco Secure ACS 8-31
Authentication Problems with Multihomed Devices 8-31
Authentication Problems with Devices Behind a NAT Boundary 8-31
Local RBAC Using Common Services 4.2.2 8-31
Authentication Mode Setup 8-32
User Management 8-32
Group Management 8-33
Role Management 8-33

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-6
Server Problems During Uninstallation A-9
Troubleshooting the Security Manager Client A-11
Client Problems During Installation A-11
Client Problems After Installation A-14
Running a Server Self-Test A-17
Collecting Server Troubleshooting Information A-18
Viewing and Changing Server Process Status A-18
Restarting All Processes on Your Server A-19
Reviewing the Server Installation Log File A-19
Symantec Co-existence Issues A-19
Problems after Installing Windows Updates A-20
Backup of Cisco Security Manager Server A-20
Problem Connecting to an ASA Device with Higher Encryption A-21
Pop-up Showing Activation.jar in Use During the Time of Installation A-21
How to Set the Locale for the Windows Default User Template to U.S. English A-22
How to disable the RMI Registry Port A-25

APPENDIX B Permissions Matrix for Image Manager B-1

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.

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.
- Provides instructions for installing Security Manager server and Auto Update Server and for installing dedicated client software for Security Manager.
- 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 x.

Audience

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

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font
Selecting a menu item in paragraphs	**Option > Network Preferences**
Selecting a menu item in tables	Option > Network Preferences

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

Table 1 Security Manager Documentation

Document Title	Available Formats
Release Notes for Cisco Security Manager	Also covers Auto Update Server. http://www.cisco.com/c/en/us/support/security/security-manager/products-release-notes-list.html
Supported Devices and Software Versions for Cisco Security Manager	Includes support information for Auto Update Server. http://www.cisco.com/c/en/us/support/security/security-manager/products-device-support-tables-list.html

Table 1 Security Manager Documentation (continued)

Document Title	Available Formats
Installation Guide for Cisco Security Manager (This guide)	http://www.cisco.com/c/en/us/support/security/security-manager/products-installation-guides-list.html
User Guide for Cisco Security Manager	http://www.cisco.com/c/en/us/support/security/security-manager/products-user-guide-list.html
User Guide for Auto Update Server	http://www.cisco.com/c/en/us/support/security/security-manager/products-user-guide-list.html
Context-sensitive online help	Select an option in the GUI, then click Help.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Overview

This chapter contains the following sections:

- Introduction to Component Applications, page 1-1
- Introduction to Related Applications, page 1-3

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 1-3

Note From version 4.17, though Cisco Security Manager continues to manage the following devices, it will not provide support for any enhancements:

- Cisco Catalyst 6500 and 7600 Series Firewall Services Modules (EOL8184)
- Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2 (EOL8843)
- Cisco Intrusion Prevention System: IPS 4200, 4300, and 4500 Series Sensors (EOL9916)
- Cisco SR 500 Series Secure Routers (EOL7687, EOL7657)
- PIX Firewalls (EOL)

Common Services

Common Services 4.2.2 is bundled by default with Security Manager 4.18.

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[1] libraries
- An embedded SQL database
- The Apache webserver
- The Tomcat servlet engine
- The CiscoWorks home page
- Backup and restore functions

Note Device and Credential Repository (DCR) functionality within Common Services is not supported in Security Manager 4.18.

Security Manager

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

Note For more information about Security Manager, visit http://www.cisco.com/go/csmanager. For more information about Cisco Security MARS, visit http://www.cisco.com/go/mars.

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

Security Manager offers the following features and capabilities:

- Service-level and device-level provisioning of VPN, firewall, and intrusion prevention systems from one desktop
- Device configuration rollback
- Network visualization in the form of topology maps
- Workflow mode
- Predefined and user-defined FlexConfig service templates
- Integrated inventory, credentials, grouping, and shared 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) and Security Device Manager (SDM)
  - When you install the server software, you also install a cross-launch point to (but not actual installation of) Cisco Prime Security Manager.

1. Cisco Security Manager was using OpenSSL for the Transport Layer Security (TLS) and Secure Socket Layer (SSL) protocols. Beginning with version 4.13, Cisco Security Manager replaced OpenSSL with Cisco SSL. In this version 4.18, Cisco SSL version 1.0.2o is being used.

  - You can add ASA devices from Security Manager to Auto Update Server (AUS).
- Integrated monitoring of events generated by ASA devices. You can selectively monitor, view, and examine events from ASA 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 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.

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. Using the Security Manager client you highlight specific firewall rules and request to see the events related to those rules or signatures. Using MARS you can select firewall 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 8-12. 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. The 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/c/en/us/support/security/security-manager/products-release-notes-list.html. For more information about the Configuration Engine, visit http://www.cisco.com/c/en/us/products/cloud-systems-management/configuration-engine/index.html.

Effect of Enabling Event Management

If you enable Event Management on your Security Manager server, you cannot use that server for the following services:

- Syslog on CiscoWorks Common Services

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 3-1 on page 3-2 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 3-3 on page 3-5); however, the Common Services syslog service port is still changed.

Licensing for Security Manager

With the information in this chapter, you can determine which license you need to install and use Cisco Security Manager 4.18. This chapter also has descriptions of the various licenses available, such as standard, professional, and evaluation.

Other than a few notes, this chapter does not discuss license installation. Refer to Chapter 5, "Installing and Upgrading Server Applications"

This chapter discusses device count, with the purpose of helping you determine which Security Manager server license you need.

License Types

The Cisco Security Manager has two base license types, Standard and Professional. Apart from the base licenses, Cisco Security Manager offers:

- Base Licenses (Standard and Professional)
- Standard-to-Professional Upgrade License
- Incremental ("Add-on") Licenses
- API License

Base Licenses (Standard and Professional)

Table 2-1 displays the list of the Standard and Professional base licenses available for Cisco Security Manager 4.18.

Table 2-1 List of the Base Licenses Available

License Name	License Abbreviation	Number of Devices that can be Managed (Refer to Understanding Device Count for Purchasing License, page 2-4)
Standard-5	ST5	5
Standard-10	ST10	10

Table 2-1 List of the Base Licenses Available (continued)

License Name	License Abbreviation	Number of Devices that can be Managed (Refer to Understanding Device Count for Purchasing License, page 2-4)
Standard-25	ST25	25
Professional-50	PRO50	50
Professional-100	PRO100	100
Professional-250	PRO250	250

Table 2-2 provides a comparison of Professional base versions with Standard base versions.

Table 2-2 Comparison of Professional Base Versions with Standard Base Versions

Feature	Supported in Professional?	Supported in Standard?
Support of incremental ("add-on") device license packages in increments of 50, 100, and 250 devices	Yes	No
Support for the management of Cisco Catalyst 6500 and 7600 Series switches and associated services modules	Yes	No
Support for the management of firewall service modules	Yes	No
Support for temporary licenses (licenses with an expiration date)	Yes	No (only permanent licenses are supported)

To obtain a 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 at http://www.cisco.com/go/license.
- If you are not a registered Cisco.com user, start at http://tools.cisco.com/RPF/register/register.do.

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.

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

Standard-to-Professional Upgrade License

When your needs have outgrown the capabilities of the Standard license, such as, to manage Catalyst security blades or when deployment grows beyond 25 devices, you need to upgrade to Cisco Security Manager Professional. You can purchase the Standard-to-Professional upgrade license. However, this upgrade license can be applied only if the base license is a Standard-25 ("ST25") license. The orderable part ID (PID) for the Standard-to-Professional upgrade license is L-CSMSTPR-U-K9.

Incremental ("Add-on") Licenses

If your base license is a Professional version (not a Standard version or the evaluation version), you can purchase incremental ("add-on") licenses to increase the number of devices that you are allowed to manage. You can purchase as many incremental licenses as you wish.

Incremental ("add-on") licenses for previous versions are valid for the current version. For example, if you have a Professional-50 license for Security Manager 4.18, you can use a 4.17 incremental device license.

Incremental licenses are available in increments of 50, 100, and 250 devices.

API License

Cisco Partners who want to use the API need to have an API license. They need to have a base PRO license in order to purchase a API license. There are two kinds of API licenses:

- A developer license. This is a 90-day license that is to be used by developers to integrate their products with Security Manager.
- A production license. This license is required by the end customers who use certain third-party products.

Note There is no API evaluation license. Both the developer license and the production license need to be ordered explicitly by Cisco Partners who want to use the API.

The orderable part ID (PID) for the Northbound API license is L-CSMPR-API.

Licensing and Deployment Scenarios

Active/Active

You are required to purchase two licenses of Cisco Security Manager in Active/Active setup.

Active and Standby

A Cisco Security Manager license allows the use of Cisco Security Manager on a single server. A standby Cisco Security Manager server, such as one 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. This is true even when high availability (HA) configuration is being used.

Note Users who use a standby server are responsible for manually restoring the database from their active server on a regular basis.

License Types and Applicability

The Cisco Security Manager 4.18 licenses and their applicability are depicted in Table 2-3

Table 2-3 Licenses and their Applicability

License	Applicability	Description
L-CSMST-5-K9 L-CSMST-10-K9 L-CSMST-25-K9 L-CSMPR-50-K9 L-CSMPR-100-K9 L-CSMPR-250-K9	Base Licenses (standard and professional license)	
L-CSMPR-LIC-50/100/250	Incremental license	Can be applied on any professional licenses
L-CSMSTPR-U-K9	Upgrade from standard to professional license	Upgrade from Cisco Security Manager Standard 25-Device Limit to Cisco Security Manager Professional
L-CSMPR-API	For API	

Licenses for Component Applications

Some component applications do not require a license file:

- Common Services.
- Auto Update Server.

Understanding Device Count for Purchasing License

Security Manager consumes one device count (of the number allowed by the license) when you add any of the following to the device inventory:

- Each physical device
- Each security context
- Each added Cisco Catalyst 6500 Series services module
- 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 device count; however, additional virtual sensors (added after the first sensor) do consume a device count.

In the case of a Firewall Services Module (FWSM) or ASA device, the module itself consumes a device count and then consumes an additional device count for each additional security context. For example, an FWSM with two security contexts would consume three device counts: one for the module, one for the admin context, and one for the second security context.

Unmanaged devices are a special case. 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 device count.

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 count.

To determine your device count, which you will need to do to determine which Security Manager server license you need, refer to Table 2-4.

Tip For the purpose of determining which Security Manager server license you need, devices are counted for Security Manager 4.18 in the same way that they were for Security Manager 4.17.

Table 2-4 Determining Your Device Count

Device	Mode (also called Context)	Device Count (also called License Count or simply License)	Comments
Standalone Firewall Devices			
Any standalone firewall device	Single-context mode	1	
Any standalone firewall device	Multi-context mode	*c*, where *c* is the context count other than the system context	
Firewall Blades			
Any standalone firewall blade	Single-context mode	1	
Any standalone firewall blade	Multi-context mode	*c*, where *c* is the context count other than the system context	**Example:** Refer to "Example for any Standalone Firewall Blade in Multi-context Mode" below this table.
Firewalls in Failover Configuration			
Any firewall in failover configuration	Single-context mode	1	

Table 2-4 Determining Your Device Count

Device	Mode (also called Context)	Device Count (also called License Count or simply License)	Comments
Any firewall in failover configuration	Multi-context mode	*c*, where *c* is the context count other than the system context	
Standalone IPS devices			
Any standalone IPS device		*n*, where *n* is the virtual sensor count and includes virtual sensor vs0	Additional virtual sensors (added after the first sensor) consume 1 license each.
Non-standalone IPS devices			
IPS modules, IPS blades, and IPS virtual machines		*n*, where *n* is the virtual sensor count and includes virtual sensor vs0	IPS modules, IPS blades, and IPS virtual machines are discovered independently in Security Manager. IPS virtual machines are used in Cisco ASA-5500 Series Adaptive Security Appliances, which are 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X.
IPS Modules or Virtual Machines that are part of an ASA Failover Configuration			
Each IPS device		*n*, where *n* is the virtual sensor count and includes virtual sensor vs0	Additional virtual sensors (added after the first sensor) consume 1 license each.
Licenses Related to ASA Load Balancing Clusters			
Each ASA load balance cluster	Single-context mode	*N*, where *N* is the number of nodes in the single-context ASA cluster	System & Admin context represents 1 context
Each ASA load balance cluster	Multi-context mode	*N* * *c*, where *N* is the number of nodes in the multi-context ASA cluster and *c* is the context count	System & Admin context represents 1 context. See also Example for Licenses Related to ASA Load Balancing Clusters.

Table 2-4 Determining Your Device Count

Device	Mode (also called Context)	Device Count (also called License Count or simply License)	Comments
Excluded Devices			
Advanced Inspection and Prevention Security Services Modules (AIP-SSMs)		0 However, additional virtual sensors (added after the first sensor) consume 1 license each.	Additional virtual sensors (added after the first sensor) consume 1 license each.
IDS Network Modules		0 However, additional virtual sensors (added after the first sensor) consume 1 license each.	Additional virtual sensors (added after the first sensor) consume 1 license each.
IPS Advanced Integration Modules (IPS AIMs)		0	
Any other modules supported for devices other than the AIP-SSC 5 and the Catalyst 6500 or 7600 installed in the host device		0	

Example for any Standalone Firewall Blade in Multi-context Mode

This subsection gives an example of context that will be useful in understanding device count.

The following command was run in system context on a firewall with two security contexts—admin and ctx1:

```
r41-appinfra-arsenal# sh context
Context Name Class Interfaces Mode URL
*admin default GigabitEthernet3/2, Routed disk0:/admin.cfg
Management0/0
ctx1 default Routed disk0:/ctx1.cfg

Total active Security Contexts: 2
r41-appinfra-arsenal# sh context count

Total active Security Contexts: 2
```

Example for Licenses Related to ASA Load Balancing Clusters

This subsection gives an example of the device count for an ASA load balancing cluster in multi-context mode.

```
3 Nodes with 4 security contexts each: License Count = 3 * 5 = 15.
```

Determining Which License You Need

The license that you need depends upon whether you are performing a new installation or upgrading from one of several previous versions:

- New Installation of Security Manager 4.18, page 2-8
- Upgrade from Security Manager 4.x, page 2-8

New Installation of Security Manager 4.18

A new installation of Cisco Security Manager 4.18 requires the purchase of the appropriate Cisco Security Manager license.

Upgrade from Security Manager 4.x

- If you have a valid SAS contract, you can upgrade to any latest version of Cisco Security Manager at no additional cost. The current license will be recognized and retained by the Security Manager installation program, so you are not required to apply for license during upgrade.
- Users without SAS contracts must either purchase a SAS contract or purchase a valid Security Manager 4.18 license.

Note With a SAS contract, users can upgrade to the latest version for free.

90-day Evaluation License

If you provide no license during installation, the resulting installation will be an evaluation version. You can also select **Evaluation Only** during installation. Refer to Installing Security Manager Server, Common Services, and AUS, page 5-3.

The evaluation license is limited to 50 devices.

The evaluation license provides the same privileges as the Professional Edition licenses, except that you cannot apply incremental licenses to the evaluation version.

Choosing the Right License when you are a New 4.x Customer

A typical scenario for a new 4.x Cisco Security Manager customer and the licensing options are explained as follows:

1. [BASE] Selection of CSM Base Product Version
   a. Based on the number of devices you need to manage using Cisco Security Manager (after accounting for future growth prospects), obtain
   - L-CSMST5-K9/L-CSMST10-K9/ L-CSMST25-K9 for networks of 5, 10, 25 or less devices respectively.

- L-CSMPR-50-K9/L-CSMPR-100-K9/L-CSMPR-250-K9 for larger networks. In addition, consider [INCREMENTAL] licenses.

b. If you need to manage Catalyst 6500 or FWSM/IDSM switch blades, choose L-CSMPR-50-K9.

c. If you obtained a standard license, but later needed to manage Catalyst switches or switch blades, or needed to manage more than 25 devices, obtain L-CSMSTPR-U-K9 to upgrade to the PRO version of the product.

d. If you already purchased a PRO license, but later needed to manage more than 50 devices, obtain the incremental license of 4.x.

2. [INCREMENTAL] Incremental licenses allow you to manage more devices. Based on the size of the network you need to manage, obtain:

a. L-CSMPR-LIC-50/L-CSMPR-LIC-100/L-CSMPR-LIC-250 to add management of 50, 100, or 250 additional devices respectively.

b. For larger networks,

- Purchase multiple units of [INCREMENTAL] licenses if you are looking for installing these on the same Cisco Security Manager server
- Purchase [BASE] licenses and/or [INCREMENTAL] licenses if you are looking for installing multiple Cisco Security Manager servers to obtain better performance.

3. [SUPPORT] In addition to the [BASE] and [INCREMENTAL] licenses, you will have to purchase equivalent SAS contracts. Having a SAS contract will enable you to upgrade to any latest version of Cisco Security Manager without any additional cost.

Choosing the Right License when you are an Existing 4.x Customer

A typical scenario for an existing 4.x Cisco Security Manager customer and the licensing options are explained as follows:

1. [BASE] To upgrade from CSM 4.x Standard to CSM 4.x PRO, purchase the L-CSMSTPR-U-K9 and then add incremental as you grow.
2. [INCREMENTAL] Any existing incremental licenses you already own will also be applicable for the latest Cisco Security Manager version. You do not need to obtain new incremental licenses to manage same number of devices. If you intend to enable event management for larger networks, you may need to consider deploying multiple Cisco Security Manager servers. This involves obtaining additional [BASE] product licenses.
3. [SUPPORT] CSM 4.x support contracts will continue to support CSM 4.18.

Installing a License for Security Manager or Component Applications

During the installation of Security Manager, you are asked for license information. Refer to Installing Security Manager Server, Common Services, and AUS, page 5-3.

During the installation of Common Services and AUS, you are not asked for license information. Common Services does not require a license file. Auto Update Server does not require a license file.

Updating a License for Security Manager or Component Applications

To learn how to update a license file for Security Manager or a component application, see Updating Security Manager, page 5-24.

Additional Documentation on Licensing

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.

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

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, and Security Manager client software:

- Required Services and Ports, page 3-1
- Windows Firewall Configuration Script, page 3-3
- Server Requirements and Recommendations, page 3-4
- Client Requirements, page 3-11

Required Services and Ports

Note Security Manager will use predefined and dynamic ports for its internal operation. Port scanners might block those ports and will not let Security Manager to execute those processes. Therefore port scanners such as Qualys should not be enabled. If enabled, it may crash Security Manager process that may require a complete re installation of Security Manager.

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 3-1 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 3-1 Basic Required Ports to Open on the Security Manager Server

Communication	Service	Protocol	Port	In	Out
Security Manager Client to the Security Manager Server.	HTTP, HTTPS	TCP	1741/443	X	—
Security Manager Client to device managers included in the product (such as ASDM).	HTTPS	TCP	443	X	—
Security Manager Server to Devices. **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.	HTTPS	TCP	443	—	X
	SSH	TCP	22	—	X
	Telnet	TCP	23	—	X
Security Manager to an e-mail server. This port is required only if you configure e-mail notification settings for any of the various functions that can provide these notifications.	SMTP	TCP	25	—	X
Syslog service used by the Security Manager Event Viewer.	Syslog	UDP	514	X	—
Health and Performance Monitor	HTTP, HTTPS	TCP	2012 and 4444	X	X

- **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 3-2. Open only ports required by applications that you are actually using.

Table 3-2 Ports Required for Optional Server Applications

Communication	Service	Protocol	Port	In	Out
Security Manager Server to and from CS-MARS.	HTTPS	TCP	443	X	X
Security Manager Server to Cisco Secure Access Control Server (ACS).	HTTP, HTTPS	TCP	• 2002 • If port restriction is enabled on the ACS server, allow all ports in the range for HTTP/HTTPS communication. • If port restriction is disabled, allow all HTTP/HTTPS traffic between the Security Manager server and ACS.	—	X
Security Manager Server to an External AAA Server (configurable in a non-ACS mode).	RADIUS LDAP Kerberos	TCP	1645, 1646, 1812(new), 389, 636 (SSL), 88	—	X

Table 3-2 Ports Required for Optional Server Applications (continued)

Communication	Service	Protocol	Port	In	Out
Security Manager Server to Configuration Engine.	HTTPS	TCP	443	—	X
Security Manager Server to AUS.	HTTPS	TCP	443	—	X
Device to AUS. Used to retrieve images and configurations.	HTTP	TCP	1751	X	—
Security Manager Server to TMS Server.	FTP	TCP	21	—	X
Internet browser running on a client system to the browser interface on the Security Manager or AUS server.	HTTP, HTTPS	TCP	1741/443	X	—

Windows Firewall Configuration Script

Beginning with Version 4.4, Security Manager included a Windows Firewall configuration script in the server installer. This script automates the process of opening and closing the ports necessary for Windows Firewall to work correctly and securely; its purpose is to harden your Security Manager server.

At the time of installation, this script is copied to *NMSROOT* but not executed. You can run this script manually to configure Windows Firewall on your Security Manager server; doing so will secure the server by blocking unnecessary ports. [*NMSROOT* is the path to the Security Manager installation directory. The default is **C:\Program Files (x86)\CSCOpx**.]

This script opens only those "IN" ports that are needed for Security Manager to perform its tasks. Hence the "Firewall.txt" file has the ports that are the bare minimum for Security Manager. If, later, you discover that you want some other port to be open, you can do that.

To run the Windows Firewall script, follow this procedure:

Step 1 Make sure Powershell scripts can run unrestricted:

a. Open the Powershell Command Line Tool.

b. Execute the command "Set-ExecutionPolicy Unrestricted"

Step 2 In NMSROOT, open a command prompt and execute firewall.bat:

a. Output will appear in the folder NMSROOT/log.

b. Windows.FW_Config.wfw is the backup of the Windows Firewall configuration before executing the script.

c. initialfirewallsettings.txt lists the ports that were open BEFORE running the script.

d. finalfirewallsettings.txt lists the ports that are open AFTER running the script.

Step 3 Enable Windows Firewall and use private network settings: Control Panel > Windows Firewall > Turn Windows Firewall on or off > [General tab] > On.

Step 4 Disable Powershell scripts for security:

a. Open the Powershell Command Line Tool.

b. Execute the command "Set-ExecutionPolicy Restricted"

Step 5 [optional] Verify added firewall rules by using Windows Firewall with Advanced Security (not available in Windows 2008 Enterprise Server (Service Pack 2)—64-bit)

Server Requirements and Recommendations

Note Customers upgrading their Operating System while migrating to Cisco Security Manager 4.9 or later, must buy the appropriate Windows license.

Unless otherwise noted, this section applies to all applications (Security Manager and Auto Update Server).

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.

We recommend that you install Security Manager on a dedicated server in a controlled environment.

For additional best practices and related guidance, see Chapter 4, "Preparing a Server for Installation."

Recommended Server

Cisco recommends that you install Security Manager on a server that is equivalent to Cisco UCS C220 M3 server.

Installation Practices to Avoid:

- Do not install any application on a primary or backup domain controller. Cisco does not support any use of Common Services on a Windows domain controller.
- Do not install any application in an encrypted directory. Common Services does not support directory encryption.
- Do not install any application 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.

Table 3-3 Server Hardware Requirements and Recommendations

Component	Description
Operating System	One of the following: • Microsoft Windows Server 2016 Standard— 64-bit • Microsoft Windows Server 2016 Datacenter—64-bit • Microsoft Windows Server 2012 R2 Standard—64-bit • Microsoft Windows Server 2012 Standard—64-bit • Microsoft Windows Server 2012 R2 Datacenter—64-bit • Microsoft Windows Server 2012 Datacenter—64-bit English and Japanese are the only supported languages. For complete information, see Understanding Regional and Language Options and Related Settings, page 3-9. 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.
System Hardware	• Processor: Intel Quadcore Xeon 5600 Series or above • Color monitor with at least 1280 x 1024 resolution and a video card capable of 16-bit colors. For AUS-only servers, you can get by with 1024 x 768 resolution. • DVD-ROM drive. • 1 Gbps network adapter. • Keyboard. • Mouse.

Table 3-3 Server Hardware Requirements and Recommendations (continued)

Component	Description
Memory (RAM)	16 GB is the minimum needed to use all features of Security Manager. With less memory, features such as Event Management and Report Management are affected. In particular, if the amount of RAM available to the operating system is less than 8 GB, Event Management and Report Manager are disabled during installation. If the memory available to the OS is between 8 and 12 GB, you can turn off Event Management and Report Management, presuming that you do not plan to use them. Configuration Management will be usable in such systems. **Tip** To turn off Event Management, follow this path: Configuration Manager > Tools > Security Manager Administration > Event Management > Enable Event Management > [clear checkbox]. **Tip** To turn off Report Management, simply close the Report Manager application. Although not recommended, you can enable Event Management and Report Management for low memory systems from the Security Manager client after completing the installation (select Tools > Security Manager Administration > Event Management). Keep in mind that enabling Event Management and Report Management on a system with low memory can severely affect the performance of the entire application. If you install AUS on a separate server, the following minimum applies: • AUS-only server—4 GB. We recommend more than 4 GB.
File system	NTFS.
Disk Optimization	Diskeeper 2010 Server. This is a recommendation, not a requirement. Disk optimization can improve performance if the cause of poor performance is disk fragmentation.

Table 3-3 Server Hardware Requirements and Recommendations (continued)

Component	Description
Hard drive space	Use a suitable combination of HDDs in a RAID configuration to achieve the disk space required, which is as follows: • 100 GB for the OS partition is recommended by Cisco. • 150 GB for the application (Security Manager) partition is recommended by Cisco. The *minimum* free disk space required for the Security Manager installation alone is 7 GB. If this is not met, then the installation will be aborted. **Note** Cisco strongly recommends installing the OS and application on separate partitions. **Note** The application partition mentioned above and any other event store partitions may not be relevant when using Veritas in HA (high availability) mode. Please refer to the applicable Security Manager high availability documentation (http://www.cisco.com/c/en/us/support/security/security-manager/products-installation-guides-list.html) and Veritas documentation for further details. • An additional 1.0 TB for log storage for the Event Viewer on a separate partition: This is a requirement, but ONLY if you plan to use Event Viewer. Cisco recommends creating this separate partition on a directly attached storage device. • An additional 1.0 TB or more: This is a requirement, but ONLY if you plan to enable Event Archival. Event Archival functionality creates a secondary storage of events when log storage is required beyond primary storage capacity (for long term preservation etc.). The Secondary Event Store size is required to be bigger than the configured primary storage size, so an additional 1.0 TB or more of disk space is required to use Event Archival. Both primary & secondary event stores can be on a SAN but it is recommended to create the primary store partition on a directly attached storage (DAS) for optimum performance. For more information on SAN storage, see Using SAN Storage, page 3-10 Cisco recommends RAID 10 for better performance. RAID 5 can be used if desired. **Tips** • 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 event store (primary/secondary) is filled. Smaller disk size causes quicker rollovers. Based on your expected EPS rate and rollover requirements, you can increase or decrease the minimum disk size when using Event Management.
IP address	One static IP address. Dynamic addresses are not supported. **Tip** Security Manager can have multiple network interface cards but teaming multiple NICs for load balancing is not recommended.

Table 3-3 Server Hardware Requirements and Recommendations (continued)

Component	Description
Virtual Memory (Paging File)	1.5 x installed memory. This is a recommendation from Microsoft for Windows platforms. It is not a Cisco requirement. Memory paging is necessitated only if the installed RAM on the system is insufficient to handle the load. **Caution:** A special consideration applies if you are using Windows Server 2012 or 2012 R2 (Standard or Datacenter)—64-bit. If you choose to automatically manage paging file size, the installation of Security Manager might fail with an error message recommending you to configure the virtual memory before running the installation program. To successfully install Security Manager, follow these steps: 1. Deselect (clear) the checkbox "Automatically manage paging file size for all drives". (The navigation path to this checkbox is Control Panel > System> Advanced System Settings > Performance > Settings > Advanced tab> Virtual Memory > Change.) 2. Create the paging file with a minimum size of 4 GB. The paging file value is configured based on the swap size. The default values of the paging configuration are 10240 and 16384 respectively. 3. Start installing Security Manager.
Antivirus	Real-time protection disabled. This is a recommendation, not a requirement. The system can have an anti-virus application installed, but Cisco recommends disabling real-time protection because it causes a performance penalty. The user can choose to run a quick scan which is scheduled to run at times when there is not much load on the server. **Note** It is mandatory to exclude the NMSROOT directory and the eventing folder from scanning.
Browser	One of the following: • Internet Explorer 8.x, 9.x, 10.x, or 11.x, but only in Compatibility View **Note** When using Internet Explorer (any version) to download the client, ensure that the following setting is correct: Internet Explorer > Tools > Internet Options > Advanced > Security > clear the "Do not save encrypted pages to disk" checkbox. If this setting is not correct (i.e., the checkbox is checked), attempts to download the client will fail. **Tip** To use Compatibility View in Internet Explorer, navigate to Tools > Compatibility View Settings, and add the Security Manager server as a "website to be displayed in Compatibility View." • Firefox 15.0.1 and above supported and recommended
Java Plug-in	There is no requirement to have JRE installed. It is required to have Java scripts enabled in the web browser. The version supported is JRE 1.7 update 181.

Table 3-3 Server Hardware Requirements and Recommendations (continued)

Component	Description
Optional Virtualization Software	You can, optionally, install the application on a system running the following versions of VMware: ESXi versions from 5 update 2 up to ESXi 6.0. 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). **Tip** 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.
High Availability Support (HA Support)	One of the following: • Veritas Storage Foundation 6.0.1 • Veritas Storage Foundation 6.0.2 • Veritas Storage Foundation 6.1 • Veritas Storage Foundation 7.0 • Veritas Storage Foundation 7.2

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.)

Tip For a detailed procedure, refer to How to Set the Locale for the Windows Default User Template to U.S. English, page A-22.

Note You must change the default system locale to U.S. English before installing Security Manager; changing the default system locale and rebooting the server does not change the default profile. It is not sufficient for the current user only to have the proper settings; this is because Security Manager creates a new account (“casuser”) that runs all Security Manager server processes.

In addition, the Regional and Language Options in the server operating system must be set correctly. Also, peripheral devices such as keyboards that use other languages can affect the way Security Manager functions.

To successfully install Security Manager, you must adhere to the following Regional and Language Options and related settings:

- 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; 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.
- You must ensure that the system locale in the Windows Registry is in a supported language. In order to change it, follow this procedure:
  1. In a command window, execute one of the following commands: **regedit.exe** or **regedt32.exe.**
  2. Make sure that the localname is supported. The following example is for U.S. English:

     \HKEY_USERS\.DEFAULT\Control Panel\International

     and change LocaleName to en-US

Note Paths and file names are restricted to characters in the English alphabet. Japanese characters are not supported for paths or file names. When selecting files on a Windows Japanese OS system, the usual file separator character \ is supported, although you should be aware that it might appear as the Yen symbol (U+00A5).

Using SAN Storage

You can use SAN storage with Security Manager provided that the storage has acceptable I/O rates and capacity. The following are the main items within Security Manager that require storage, and the storage options that you have in addition to using disk storage that is directly installed in the server:

- Security Manager installation folder (CSCOpx and subfolders)—The application is best installed on a local drive. However, the folder can be direct attached storage (DAS) or block-based SAN storage (FC, FCoE, iSCSI). The high-availability configuration for Security Manager, described in *High Availability Installation Guide for Cisco Security Manager*, requires a shared cluster volume.
- Primary storage for the Event Manager service—If you use Event Viewer to monitor events, you must specify a primary storage location. The primary storage can be direct attached storage (DAS) or block storage (SAN protocol: FC, FCoE, iSCSI) mapped as a local drive.
- Extended storage for the Event Manager service—Any extended storage location is expected to be on SAN storage. The extended storage should be direct attached storage (DAS) or block storage (SAN protocol: FC, FCoE, iSCSI) mapped as a local drive.

Tips

- CIFS and NFS are not supported.
- The supported network storage types are also supported in VMware configurations.

Requirement for iSCSI Volumes

iSCSI volumes using a software initiator may not be available when Security Manager services are about to start after a system reboot. It may take some time for them to be properly initialized.

If Security Manager services have not started, then you need to configure dependency and service startup settings for them (the Security Manager services).

To configure dependency and startup settings, follow this procedure:

Step 1 Execute the following commands in a Windows command prompt to change the startup type of the Cisco Security Manager Daemon Manager, syslog, and tftp services to “Delayed auto start”:

```
sc config CRMDmgtd start= delayed-auto
sc config crmlog start= delayed-auto
sc config crmtftp start= delayed-auto
```

Step 2 Set the dependency of Microsoft iSCSi to the Cisco Security Manager Daemon Manager service by executing the following command:

```
sc config CRMDmgtd depend= MSiSCSI
```

Tip In these commands, the option name includes the equals sign. A space is required between the equals sign and the value.

Step 3 Verify the dependency settings of the Cisco Security Manager Daemon Manager service by executing the following command. It should display the iSCSI initiator dependency setting as "DEPENDENCIES : MSiSCSI"

```
sc qc CRMDmgtd
```

Client Requirements

Table 3-4 describes Security Manager Client requirements and restrictions.

Note The date and time formats that you select for the client must be the same as those used by your server machine. If they are not, Device View in Security Manager may not load properly.

Table 3-4 Client Requirements and Restrictions

Component	Requirement
System hardware	• One CPU with a minimum speed of 2 GHz. • Color monitor with at least 1280 x 1024 resolution and a video card capable of 16-bit colors. • Keyboard. • Mouse.

Table 3-4 Client Requirements and Restrictions (continued)

Component	Requirement
Operating System	One of the following: • Microsoft Windows Server 2016 Standard— 64-bit • Microsoft Windows Server 2016 Datacenter— 64-bit • Microsoft Windows 7 • Microsoft Windows 8—64-bit and 32-bit • Microsoft Windows 8.1 Enterprise Edition—64-bit and 32-bit • Microsoft Windows 10 —64-bit and 32-bit • Microsoft Windows Server 2012 R2 Standard—64-bit • Microsoft Windows Server 2012 Standard—64-bit • Microsoft Windows Server 2012 R2 Datacenter—64-bit • Microsoft Windows Server 2012 Datacenter—64-bit **Note** 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.)
Memory (RAM)	For 32 bit systems: • Minimum: 2 GB • Recommended: > 2 GB For 64 bit systems: • Minimum: 4 GB • Recommended: > 4 GB. **Note** The minimum memory requirement would increase if you enable conflict detection. In such a case, in the client lax file, increase the memory space to the required value.

Table 3-4 Client Requirements and Restrictions (continued)

Component	Requirement
Virtual Memory (Paging File)	512 MB. **Caution:** You must deselect (clear) the checkbox "Automatically manage paging file size for all drives". (The navigation path to this checkbox is Control Panel > System > Advanced System Settings > Performance > Settings > Advanced tab> Virtual Memory > Change.) The paging file value is configured based on the swap size. The default values of the paging configuration are 10240 and 16384 respectively **Caution:** A special consideration applies if you are using Windows Server 2012 or 2012 R2 (Standard or Datacenter)—64-bit. You need to be aware of this consideration if your server has two independent partitions (e.g., C: and F:). If you follow these steps, ***the installation will fail***: 1. Uncheck (clear the checkbox for) "Automatically manage paging file size for all drives." 2. On your non-system partition (e.g., F:), create the paging file. 3. On your system partition (e.g., C:), retain the option to automatically manage paging file size. 4. Start installing Security Manager. The installer quits with an error message stating not to use a system-managed paging file size.
Hard Drive Space	10 GB free disk space.
Browser	One of the following: • Internet Explorer 8.x, 9.x, 10.x, or 11.x, but only in Compatibility View **Note** When using Internet Explorer (any version) to download the client, ensure that the following setting is correct: Internet Explorer > Tools > Internet Options > Advanced > Security > clear the "Do not save encrypted pages to disk" checkbox. If this setting is not correct (i.e., the checkbox is checked), attempts to download the client will fail. **Tip** To use Compatibility View in Internet Explorer, navigate to Tools > Compatibility View Settings, and add the Security Manager server as a "website to be displayed in Compatibility View." • Firefox 15.0.1 and above supported and recommended
Java Plug-in	There is no requirement to have JRE installed. It is required to have Java scripts enabled in the web browser. The version supported is JRE 1.7 update 181. The Security Manager client includes an embedded and completely isolated version of Java (JRE 1.7.x). This Java version does not interfere with your browser settings or with other Java-based applications.
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 some features of the client might work with lesser privileges, only Administrator users are fully supported.

Preparing a Server for Installation

After you verify that the target server meets the requirements described in Chapter 3, "Requirements and Dependencies," you can use these checklists to prepare and optimize your server for installation:

- Best Practices for Enhanced Server Performance and Security, page 4-1
- Readiness Checklist for Installation, page 4-3

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.

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.

✓	Task
❑	1. **Find and organize the installer applications for any recommended updates, patches, service packs, hot fixes, and security software to install on the server.**
❑	2. **Upgrade the server BIOS if an upgrade is available.**
❑	3. **Cisco recommends that you do not install any other product on the Security Manager Server.** 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 4.18 and any release of Common Services earlier than 4.2.2. 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. **Security Manager can have multiple network interface cards but teaming multiple NICs for load balancing is not recommended.**

✓	Task
❑	5. **Perform a clean installation of only the baseline server OS, without any manufacturer customizations for server management.**
❑	6. **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**. **Note** Back up your Security Manager Server and stop Security Manager services before any patches or Windows updates are applied. Cisco recommends that you apply patches and Windows updates during the maintenance window, when Security Manager is not running.
❑	7. **Install any recommended updates for drivers and firmware on the target server.**
❑	8. **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.
❑	9. **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 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.
❑	10. **"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.
❑	11. **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**.
❑	12. **Remove unused, unneeded, and incompatible applications.** For example: • Microsoft Internet Information Server (IIS) is not compatible with Security Manager. If IIS is installed, you must uninstall it before you install Security Manager. • 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 http://www.cisco.com/go/csmanager. We do support the installation of Security Manager and AUS on the same server, but we recommend that configuration only for very small networks. • 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 4.2.2. • 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. • We do not support the coexistence of Security Manager on the same server with Cisco Secure ACS for Windows.
❑	13. **Disable unused and unneeded services.** At a minimum, Windows requires the following services to run: DNS Client, Event Log, Plug & Play, Protected Storage, and Security Accounts Manager. Check your software and server hardware documentation to learn if your particular server requires any other services.
❑	14. **Disable all network protocols except TCP and UDP.** Any protocol can be used to gain access to your server. Limiting the network protocols limits the access points to your server.

✓	Task
❑	15. **Avoid creating network shares.** If you must create a network share, secure the shared resources with strong passwords. **Note** We strongly discourage network shares. We recommend that you disable NETBIOS completely.
❑	16. **Configure server boot settings.** Set a zero-second startup time, set Windows to load by default, and enable automatic reboot in cases of system failure.

Readiness Checklist for Installation

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

✓	Readiness Factor
❑	The following patches are required to run the critical Cisco Security Manager services on the Microsoft Windows Server 2012 R2. Failing to install the patches will bring down the services. Ensure that you have these patches installed on your server, else install the patches in the following order: a. KB2919442 b. Run the clearcompressionflag.exe **Note** The clearcompressionflag.exe file is part of the cumulative set of security updates. This tool prepares the computer for the Windows Updates in the background. The executable file can be downloaded from the Microsoft site: https://support.microsoft.com/en-in/kb/2919355. c. KB2919355, KB2932046, KB2959977, KB2937592, KB2938439, and KB2934018 d. KB2999226 You can also install these patches after installing the Cisco Security Manager to bring up the critical services. To register the services with the windows services, you must run the "RegisterApache.bat" script which is located in "<CSMInstalledDirectory>\CSCOpx\bin", and then restart the server.
❑	⚠ **Caution** A server can be vulnerable to attack when you uninstall or disable security applications. 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. **Note** Re-enable your antivirus software after installation, but you must exclude the NMSROOT directory and eventing folder from scanning as long as Security Manager is installed on the server.

✓	Readiness Factor
❑	**Tip** You will invalidate the SSL certificate on your server if you set the server date and time outside the range of time in which the SSL certificate is valid. If the server SSL certificate is invalid, the DCRServer process cannot start. 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. **Tip** If a change to the date and time settings on your server invalidates the SSL certificate, a "java.security.cert.CertificateNotYetValidException" error is visible in your *NMSROOT*\log\DCRServer.log file, where *NMSROOT* is the path to the Security Manager installation directory. The default is **C:\Program Files (x86)\CSCOpx**.
❑	3. **Confirm that required services and ports are enabled and available for use by Security Manager.** Security Manager uses predefined and dynamic ports for its internal operation. Port scanners might block those ports and will not let Security Manager to execute those processes. Therefore port scanners like Qualys should not be enabled. If enabled, it may result in a Security Manager process crash issue which in turn may require a complete reinstallation of Security Manager. See **Required Services and Ports, page 3-1****.**
❑	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. If Terminal Services is enabled on the target server in Application mode when you try to install Security Manager, an error will stop the installation.
❑	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 installation, you should place your license file on the target server before installation.** You will be prompted to select this file during installation. **Note** The path to the license file must not contain special characters such as the ampersand (&).
❑	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.
❑	10. **If the Cisco Security Manager client is already installed on the server, the client needs to be stopped.** This condition is checked during installation.

✓	Readiness Factor
❑	**11. 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. **Procedure** To enable or disable FIPS on Windows Server 2008, follow these steps: **a.** Go to **Start > Administrative Tools > Local Security Policy**. The Local Security Policy window appears. **b.** Click **Local Polices > Security Options**. **c.** Select **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**. **d.** Right-click the selected policy and click **Properties**. **e.** Select **Enabled** or **Disabled** to enable or disable FIPS compliant algorithms. **f.** Click **Apply**. You must reboot the server for the changes to take effect.
❑	**12. Disable Internet Explorer Enhanced Security Configuration (IE ESC).** This needs to be done because client download is prevented by IE ESC. **Procedure** To disable IE ESC on the server where you are preparing to install Security Manager, follow these steps: **a.** In Windows, open Server Manager. You can do this by right-clicking **Computer** and then clicking **Manage**. **b.** Under Security Information, click **Configure IE ESC** and then turn off IE ESC.
❑	**13. Disable port scanner software.** Security Manager uses predefined and dynamic ports for its internal operation. Port Scanners might block these ports and will not allow Security Manager to execute those processes.Therefore port scanners like Qualys should not be enabled. If enabled, it may result in a Security Manager process crash which in turn may require a complete reinstallation of Security Manager.

CHAPTER 5

Installing and Upgrading Server Applications

This chapter explains how to install the Security Manager server software and other server applications, namely CiscoWorks Common Services and AUS.

- Understanding the Required Server User Accounts, page 5-1
- Using Remote Desktop Connection or VNC To Install Server Applications, page 5-2
- Installing Security Manager Server, Common Services, and AUS, page 5-3
- Upgrading Server Applications, page 5-6
- Migrating Security Manager to a New Computer or Operating System, page 5-22
- Updating Security Manager, page 5-24
- Obtaining Service Packs and Point Patches, page 5-25
- Uninstalling Server Applications, page 5-25
- Downgrading Server Applications, page 5-26

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
  - Logging in to the client
  - Performing successful backups of all databases

The following five permissions are assigned and set, automatically, at the time of Security Manager installation:

- Access this computer from network - casusers
- Deny access to this computer from network - casuser
- Deny logon locally - casuser
- Log on as batch job - casuser, casusers
- Log on as a service – casuser

- *System Identity*—The system identity user account is equivalent to a Windows administrator and provides access to all Common Services and Security Manager tasks. This account does not have a fixed name; you can create the account using whatever name fits your needs. If you create the account in Common Services, you must assign it system administrator privileges; if you use Cisco Secure Access Control Server (ACS) for user authentication, you must assign it all privileges.

  If you install Cisco Security Management suite applications on separate servers (the recommended approach), you must create the same system identity user account on all servers within the multi-server setup. Communication among your servers relies on a trust model that uses certificates and shared secrets. The system identity user is considered the trustworthy account by other servers in the multi-server setup and therefore facilitates communication between servers that are part of a domain.

You can create as many additional user accounts as needed. Each user should have a unique account. To create these additional accounts, you must have system administrator authority (for example, using the admin account). When you create a user account, you must assign it a role, and this role defines what the user can do in the applications, even to the extent of what the user can see. For more information on the various types of available permissions, and how to use ACS for controlling access to the applications, see Chapter 8, “Managing User Accounts.”

Using Remote Desktop Connection or VNC To Install Server Applications

We recommend that you install server applications when you are logged directly in to the server.

However, if you must perform 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 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. If you use Remote Desktop Connection, Cisco recommends using a Remote Desktop Protocol console session and not a non-console session.

Installing Security Manager Server, Common Services, and AUS

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

Note You cannot install the Cisco Security Manager bundle on a standalone Auto Update Server (AUS) installation. To install the Security Manager bundle, you must first uninstall AUS and then proceed to install the Security Manager bundle.

- CiscoWorks Common Services 4.2.2—This is the foundation software that is required by the server applications. Beginning with Security Manager 4.4, the CiscoWorks Common Services check box no longer appears on the component selection page; installation of Common Services is selected by default.

Note Beginning with version 4.18, JRE 1.7 Update 181 will be installed for fresh installation.

- Cisco Security Manager 4.18—This is the main server software for Security Manager.
- Auto Update Server 4.18—This is a web-based interface for upgrading device configuration files and software images on Adaptive Security Appliances (ASA) that use the auto update feature.
- Cisco Security Manager client 4.18—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 6, "Installing and Configuring the Client."

Tip Beginning with Security Manager 4.4, AUS and the Security Manager client are installed in parallel to improve installation time.

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 5-6.

Before You Begin

- Refer to the "Licensing for Security Manager" chapter of this installation guide
- 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 5-18. Ensure that the backup completes successfully, and that your existing applications are functioning normally before installing an upgrade.
- When installing a permanent license for Security Manager, you must stage the license file on a disk that is local to your Security Manager server. The license file must be on the server to select it during installation, because 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.) Do not place the file in any folder in which you will install the product.

Note The path to the license file must not contain special characters such as the ampersand (&).

- Ensure that you go through the Readiness Checklist for Installation, page 4-3.
- Ensure that the server meets the requirements listed in Server Requirements and Recommendations, page 3-4.
- 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.
- 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 8-12.

  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.
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 compressed installation file for Security Manager.

- Using your choice of file compression utilities, such as WinZip or the Compressed (zipped) Folders Extraction Wizard, which is provided with operating systems supported by Security Manager 4.18, 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:\CSM" is a better choice than "C:\Cisco_Security_Manager\server\installation_directory." Start the installation program, **Setup.exe**, which normally unzips to the same directory as the compressed file.

Tip 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 (x86)\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.

Note The location that you select to use for the backup must be outside *NMSROOT*. The location *NMSROOT* is the path to the Security Manager installation directory. The default is **C:\Program Files (x86)\CSCOpx.** In particular, note that *NMSROOT*\backup must not be used for the backup.

- 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. Also, if you specify a folder other than the default folder, the path must not contain any special characters.
  The Windows Server 2012 R2 disables 8dot3 name generation on non-system drives, therefore user cannot select the Program Files (x86) folder on non-system drive paths. As a result, after setting the 8dot3 notation, the user must restart the server. Short names will not be created for existing folders after you enable 8dot3 naming on the specific drive; you must remove and recreate the folders, after a restart in order to force the short names to be created. If the existing folder was not empty, make sure that you select a new folder to proceed with installation.

Note Make sure that the installation directory path on a non-system drive, does not contain the special characters-"(" and ")". Installation will not proceed if these special characters are present.

- Applications—The applications you want to install—Security Manager, AUS, or both. CiscoWorks Common Services 4.2.2 is installed automatically when you install Security Manager or AUS.
- 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.

Note The path to the license file must not contain special characters such as the ampersand (&).

  - **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 5-1.
- 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.

Note If you have security policies on password complexity restrictions, this account creation may not succeed. In such cases, you need to manually create the casuser account (see further instructions for the casuser password in Table A-3, Causes and Workarounds for LiaisonServlet Error).

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

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, upgrading from Microsoft Windows Server 2008 R2 with SP1 Enterprise—64-bit to Microsoft Windows Server 2012 Standard—64-bit. If you are performing a Security Manager upgrade while also performing 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 5-22.
  - An error message will pop up if there is any database migration error; this will be at a point where installation can be taken forward without stopping.

Note During local upgrade, the installer checks to see if Performance Monitor or Resource Manager Essentials is installed. If one or both of them are found, the installer exits with an error message stating that Performance Monitor or Resource Manager Essentials (or both) needs to be uninstalled.

- 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 5-16.

- 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.

Note A special note applies to all indirect upgrades with event management enabled (Configuration Manager > Tools > Security Manager Administration... > Event Management > [Event Management group] > Enable Event Management. Under these conditions, a detailed view of an event (Launch > Event Viewer > Event Details > Details) will throw an error. The root cause of this error is restoring an old version of the event database followed by loading the event data. To work around this problem, identify all of your old partitions (the ones containing event data generated before your indirect upgrade) and move them to the secondary partition ("Extended Data Store Location" in the Security Manager GUI at Configuration Manager > Tools > Security Manager Administration... > Event Management).

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 Security Manager 3.0.x, you need to upgrade to 3.2.2, and then follow the indirect upgrade path to upgrade from 3.2.2 to 4.18.

Table 5-1 explains the software versions that are supported for each upgrade path.

The following upgrade paths are supported:

- 4.16 (including any service pack) > 4.18
- 4.17 (including any service pack) > 4.18

Table 5-1 Application Upgrade Paths

Upgrade Path	Applications	Supported Older Versions	Upgrade Procedure
Local	Security Manager 4.18 Auto Update Server 4.18	4.16 and 4.17	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-16. 2. Then, install the software; see Installing Security Manager Server, Common Services, and AUS, page 5-3. 3. Finally, make any required post-upgrade changes; see Making Required Changes After Upgrade, page 5-22.
Remote	Security Manager 4.18 Auto Update Server 4.18	4.16 and 4.17	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-16. 2. Back up the database; see Backing Up the Database for Remote Upgrades, page 5-18. 3. Install the application, see: Installing Security Manager Server, Common Services, and AUS, page 5-3 4. If necessary, transfer the database backup to the server. 5. Recover the database; see Restoring the Server Database, page 5-21. 6. Finally, make any required post-upgrade changes; see Making Required Changes After Upgrade, page 5-22.

Table 5-1 Application Upgrade Paths (continued)

Upgrade Path	Applications	Supported Older Versions	Upgrade Procedure
Indirect	Security Manager 4.18	4.15	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-16. 2. Next, upgrade to 4.16, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.16. 3. Finally, upgrade to 4.18 and carefully follow the data migration instructions in this installation guide's chapter on upgrade for 4.18.
Indirect	Security Manager 4.18	4.13 and 4.14	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-16. 2. Next, upgrade to 4.15, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.15. 3. Next, upgrade to 4.17, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.17. 4. Finally, upgrade to 4.18 and carefully follow the data migration instructions in this installation guide's chapter on upgrade for 4.18.
Indirect	Security Manager 4.18	4.11 and 4.12	1. Commit any pending data; see: – Resolving database errors while upgrading from Cisco Security Manager 4.12 SP2, page 5-15. – Ensuring Security Manager Pending Data is Submitted and Approved, page 5-16. 2. Next, upgrade to 4.13, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.13. 3. Next, upgrade to 4.15, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.15. 4. Next, upgrade to 4.17, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.17. 5. Finally, upgrade to 4.18 and carefully follow the data migration instructions in this installation guide's chapter on upgrade for 4.18.

Table 5-1 Application Upgrade Paths (continued)

Upgrade Path	Applications	Supported Older Versions	Upgrade Procedure
Indirect	Security Manager 4.18	4.9 and 4.10	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-16. 2. Next, upgrade to 4.11, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.11. 3. Next, upgrade to 4.13, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.13. 4. Next, upgrade to 4.15, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.15. 5. Next, upgrade to 4.17, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.17. 6. Finally, upgrade to 4.18 and carefully follow the data migration instructions in this installation guide's chapter on upgrade for 4.18.
Indirect	Security Manager 4.18	4.7 and 4.8	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-16. 2. Next, upgrade to 4.9, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.9. 3. Next, upgrade to 4.11, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.11. 4. Next, upgrade to 4.13, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.13. 5. Next, upgrade to 4.15, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.15. 6. Next, upgrade to 4.17, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.17. 7. Finally, upgrade to 4.18 and carefully follow the data migration instructions in this installation guide's chapter on upgrade for 4.18.

Table 5-1 Application Upgrade Paths (continued)

Upgrade Path	Applications	Supported Older Versions	Upgrade Procedure
Indirect	Security Manager 4.18	4.5 and 4.6	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-16. 2. Next, upgrade to 4.7, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.7. 3. Next, upgrade to 4.9, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.9. 4. Next, upgrade to 4.11, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.11. 5. Next, upgrade to 4.13, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.13. 6. Next, upgrade to 4.15, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.15. 7. Next, upgrade to 4.17, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.17. 8. Finally, upgrade to 4.18 and carefully follow the data migration instructions in this installation guide's chapter on upgrade for 4.18.

Table 5-1 Application Upgrade Paths (continued)

Upgrade Path	Applications	Supported Older Versions	Upgrade Procedure
Indirect	Security Manager 4.18	4.3 and 4.4	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-16 2. Next, upgrade to 4.5, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.5. 3. Next, upgrade to 4.7, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.7. 4. Next, upgrade to 4.9, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.9. 5. Next, upgrade to 4.11, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.11. 6. Next, upgrade to 4.13, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.13. 7. Next, upgrade to 4.15, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.15. 8. Next, upgrade to 4.17, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.17. 9. Finally, upgrade to 4.18 and carefully follow the data migration instructions in this installation guide's chapter on upgrade for 4.18.

Table 5-1 Application Upgrade Paths (continued)

Upgrade Path	Applications	Supported Older Versions	Upgrade Procedure
Indirect	Security Manager 4.18	4.2	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-16 2. Next, upgrade to 4.4, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.4. 3. Next, upgrade to 4.6, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.6. 4. Next, upgrade to 4.8, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.8. 5. Next, upgrade to 4.10, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.10. 6. Next, upgrade to 4.12, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.12. 7. Next, upgrade to 4.14, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.14. 8. Next, upgrade to 4.16, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.16. 9. Finally, upgrade to 4.18 and carefully follow the data migration instructions in this installation guide's chapter on upgrade for 4.18.

Table 5-1 Application Upgrade Paths (continued)

Upgrade Path	Applications	Supported Older Versions	Upgrade Procedure
Indirect	Security Manager 4.18	4.1, 4.1.1	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-16 2. Next, upgrade to 4.2, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.2. 3. Next, upgrade to 4.4, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.4. 4. Next, upgrade to 4.6, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.6. 5. Next, upgrade to 4.8, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.8. 6. Next, upgrade to 4.10, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.10. 7. Next, upgrade to 4.12, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.12. 8. Next, upgrade to 4.14, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.14. 9. Next, upgrade to 4.16, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.16. 10. Finally, upgrade to 4.18 and carefully follow the data migration instructions in this installation guide's chapter on upgrade for 4.18.

Table 5-1 Application Upgrade Paths (continued)

Upgrade Path	Applications	Supported Older Versions	Upgrade Procedure
Indirect	Security Manager 4.18	3.3.x	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-16. 2. Next, perform a remote upgrade to 4.0, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.3. 3. Next, perform a remote upgrade to 4.3, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.3. 4. Next, upgrade to 4.5, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.5. 5. Next, upgrade to 4.7, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.7. 6. Next, upgrade to 4.9, being careful to follow the data migration instruction in the installation guide's chapter on upgrade for 4.9. 7. Next, upgrade to 4.11, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.11. 8. Next, upgrade to 4.12, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.12. 9. Next, upgrade to 4.14, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.14. 10. Next, upgrade to 4.16, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.16. 11. Finally, upgrade to 4.18 and carefully follow the data migration instructions in this installation guide's chapter on upgrade for 4.18.

Table 5-1 Application Upgrade Paths (continued)

Upgrade Path	Applications	Supported Older Versions	Upgrade Procedure
Indirect	Security Manager 4.18	3.2.x (3.2.2 only)	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-16. 2. Next, upgrade to 4.1, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.0. 3. Next, upgrade to 4.3, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.3. 4. Next, upgrade to 4.5, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.5. 5. Next, upgrade to 4.7, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.7. 6. Next, upgrade to 4.9, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.9. 7. Next, upgrade to 4.11 and carefully follow the data migration instructions in the installation guide's chapter on upgrade for 4.11. 8. Next, upgrade to 4.12, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.12. 9. Next, upgrade to 4.14, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.14. 10. Next, upgrade to 4.16, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.16. 11. Finally, upgrade to 4.18 and carefully follow the data migration instructions in this installation guide's chapter on upgrade for 4.18.

Resolving database errors while upgrading from Cisco Security Manager 4.12 SP2

While performing an inline (local) or remote upgrade from Cisco Security Manager 4.12 SP2, you may encounter a database migration error which impacts device deployment and configuration.

Note Inline upgrades are not supported for upgrades from Cisco Security Manager 4.12 SP2. Follow the remote upgrade procedure and refer to the steps below to resolve the database migration issues.

Perform the steps below to resolve the database migration issues:

Step 1 After installing Cisco Security Manager 4.18, navigate to ~CSCOpx\upgrade\data\412999999, open the **Admin_properties.sql** file in a text editor, such as Notepad.

Step 2 Locate the following content:

```
INSERT INTO ADMIN_PROPERTIES (PROPERTY,VALUE,DEFAULTVALUE) values
('workflow.deployjob.submittercanapprove','true','true')
```

Step 3 Replace this content with the following:

```
if not exists (select 1 from ADMIN_PROPERTIES where PROPERTY =
'workflow.deployjob.submittercanapprove') then
       INSERT INTO ADMIN_PROPERTIES (PROPERTY,VALUE,DEFAULTVALUE) values
('workflow.deployjob.submittercanapprove','true','true')
end if;
```

Step 4 Save the **Admin_properties.sql** file.

Step 5 Proceed to restore the Cisco Security Manager 4.12 SP2 database backup.

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

Tip *$NMSROOT* is the full pathname of the Common Services installation directory [the default is C:\Program Files (x86)\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.

Editing the csm.properties File After a Remote Upgrade

After a remote upgrade, you must edit the **csm.properties** file to include newly added properties. Follow these steps:

Step 1 From *$NMSROOT*\MDC\athena\config\ subdirectory, open **csm.properties** in a text editor, such as Notepad.

(*$NMSROOT* is the full pathname of the Common Services installation directory [the default is C:\Program Files (x86)\CSCOpx])

Step 2 Add the following content to the end of the **csm.properties** file.

```
##
# Customize Activity Report Generation
##
# Report generation timeout in minutes
# Set to 10 minutes by default
#generate_activity_report_timeout=10
# Generate PDF Report
#generate_activity_pdf_report=true
# Generate HTML Report
#generate_activity_html_report=false
#
```

```
#CSCup28957::This will allow user to exclude the list of operation rows in all applicable
policies from activity change report.
#excluded operations should be in comma separated and if it is empty or commented then
it will include all operations.
#excluded operations::Add,Delete,Modify,Move,ReOrder,Assign,UnAssign. These names should
not be modified.
#By default it is empty,if we need to exclude operation then add required excluded
operation.
#ex: 1.ActChangeReport.excludedOperations=ReOrder,
2.ActChangeReport.excludedOperations=Add,ReOrder ,
3.ActChangeReport.excludedOperations=Add,Modify,Move,ReOrder
ActChangeReport.excludedOperations=
```

Note The above lines of code are commented by default. If you want to use the default values or modify the values of a particular property in the file, you must first uncomment the given line of code. For example, if you want Security Manager to generate Activity Reports in PDF format, you must change the given property as follows:

```
# Generate PDF Report
generate_activity_pdf_report=true
```

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

Step 4 Restart the **Cisco Security Manager Daemon Manager** service from **Start > Programs > Administrative Tools > Services.**

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.

Note Beginning with Security Manager 4.4, a new attribute, PURGE_DBBACKUP_LOG, has been added to the backup.properties file; it has a default value of 20, meaning that backups will be purged after 20 days. If this new attribute is set to NIL, then backups will not be purged. The dbbackup.log is created with a timestamp format of dbbackup_[YYYY-MM-DD_HH-mm-ss].log. At any point of time, a minimum of 5 dbbackup.log files will be maintained irrespective of purge configuration.

Note To back up the database, the Short Date format should be either M/d/YYYY or M/d/yy. To change the Short Date format to either M/d/YYYY or M/d/yy, select Start > Control Panel > Region and Language > Formats > Short Date, and then change the Short Date format to either M/d/YYYY or M/d/yy.

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 5-22.

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 5-16).

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 6-12).

b. Click the **Server Administration** panel. Then select **Server > 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 5-22.

Step 1 Ensure that pending data is committed (see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-16).

Step 2 At a command prompt, enter **net stop crmdmgtd** to stop all processes.

Step 3 Back up the database by entering the following command:

*$NMSROOT***bin\perl** *$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 (x86)\CSCOpx].
- *backup_directory*—The directory where you want to create the backup. For example, C:\Backups.

Note The location that you select to use for the backup must be outside *NMSROOT*. The location *NMSROOT* is the path to the Security Manager installation directory. The default is **C:\Program Files (x86)\CSCOpx.** In particular, note that *NMSROOT*\backup must not be used for the backup.

Note The backup directory should not contain any special characters.

- *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 size 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 command shown below assumes that you are in the directory containing the perl and backup.pl commands. (When you are in that directory, though, you must still specify the entire path of perl and backup.pl, fully qualified in the DOS 8.1 format with no spaces.)

The command shown below creates a compressed backup and log file in the backups directory and sends notifications to admin@domain.com.

When you use the backup.pl command, you must specify a backup generation if you want to include the compress parameter.

If you specify any parameter after the log file parameter, you must include values for all preceding parameters.

In this example, *$NMSROOT is* D:\CSM, not the default value of C:\Program Files (x86)\CSCOpx.

D:\CSM\bin\perl D:\CSM\bin\backup.pl C:\backups C:\backups\backup.log email=admin@domain.com 0 compress

Step 4 Examine the log file to verify that the database was backed up.

Note If Security Manager restarts unexpectedly during the database backup process, the backup is interrupted and a backup lock file **backup.lock** is created in the *NMSROOT* directory. Delete the **backup.lock** file to proceed with backup.

Step 5 At a command prompt, enter **net start crmdmgtd** to restart all processes.

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 5-6.
- 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 5-22.

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** *help*] [**-m** *Email*]

where:

- *$NMSROOT*—The full pathname of the Common Services installation directory [the default is C:\Program Files (x86)\CSCOpx].
- **-t** *temporary_directory*—(Optional) This is the directory or folder used by the restore program to store its temporary files. By default this directory is *$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.
- **-m**—Use to send email on the restore status as Success or Failure.

For example, to restore the most recent version from the c:\var\backup directory, enter the following command (note that this is for a 64-bit OS):

C:\Progra~2\CSCOpx\bin\perl C:\Progra~2\CSCOpx\bin\restorebackup.pl -d C:\var\backup

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 are handled in Cisco Security Manager. You are therefore required to 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:

Note Additionally, refer to the Important Notes section of the release notes for this release for other considerations that might apply to your installation of Security Manager after an upgrade.

- 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 must 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

Note Customers upgrading their Operating System while migrating to Cisco Security Manager 4.9 or later, must buy the appropriate Windows license.

Certain circumstances might require you to move Security Manager to a new server. This move might be to a new physical machine, or you might want to perform a major upgrade to the operating system on the server (such as moving from Microsoft Windows Server 2008 R2 with SP1 Enterprise—64-bit to Microsoft Windows Server 2012 Standard—64-bit or to Microsoft Windows Server 2012 Datacenter—64-bit).

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 5-6; 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.

Before You Begin

This procedure assumes that you want the target server (the server to which you are moving 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***MDC\eventing\database**, where NMSROOT is the installation directory [usually C:\Program Files (x86)\CSCOpx].

b. Stop all processes by entering the following at the command line:

net stop crmdmgtd

c. Make a copy of the *NMSROOT***MDC\eventing\config\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 5-19.

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:

net stop crmdmgtd

b. Copy the backed up *NMSROOT***MDC\eventing\config\collector.properties** file from the source computer to the target server, overwriting the file on the target server.

c. If you did not restart processes after completing the database restore, restart them now:

net start 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. 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

Although you can specify permanent license files during installation, you can also add licenses after you install Security Manager. AUS does not require a license.

Before You Begin

You must copy the license file to the server machine or to the client machine before adding it (the license) to the application. If you use the client machine, you must enable the client-side browser.

Note The path to the license file must not contain special characters such as the ampersand (&).

Tip You can also apply a license while logging into Security Manager: Security Manager will prompt with the message "Upgrade license" or "Continue Evaluation." By clicking "Upgrade License," you can apply the license.

Procedure

To install a license for Security Manager, follow these steps:

Step 1 Log in to the server using the Security Manager client application (see Logging In to Security Manager Using the Security Manager Client, page 6-10).

Step 2 Select **Tools > Security Manager Administration** and select **Licensing** from the table of contents.

Step 3 Click **CSM** if the tab is not active.

Step 4 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.

Note The path and file name are restricted to characters in the English alphabet. Japanese characters are not supported. When selecting files on a Windows Japanese OS system, the usual file separator character \ is supported, although you should be aware that it might appear as the Yen symbol (U+00A5).

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.

- To learn when Cisco has prepared a new service pack, and to download any service pack that matters to you, open Security Manager, then select **Help > Security Manager Online**. Alternatively, go to http://www.cisco.com/go/csmanager.
- If your organization submits a Cisco TAC service request, TAC will tell you if an unscheduled point patch exists that might solve the problem you have described. Cisco does not distribute Security Manager point patches in any other way.

Service packs and point patches provide server support for client software updates and detect version level mismatches between a client and its server.

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 5-18.

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.

Procedure

To uninstall server applications, follow these steps:

Step 1 Select **Start > Programs > Cisco Security Manager > Uninstall Cisco Security Manager**.

By default, all applications will be uninstalled.

Step 2 The uninstaller removes all applications.

Note If the uninstallation causes an error, see Server Problems During Uninstallation, page A-9, and the "Troubleshooting and FAQs" chapter in *Installing and Getting Started With CiscoWorks LAN Management Solution 3.1*: http://www.cisco.com/en/US/products/sw/cscowork/ps3996/prod_installation_guides_list.html.

Step 3 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 4 Perform the following steps 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 (x86)\CSCOpx**. Other values, such as **E:\Program Files (x86)\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\Wow6432Node\Cisco\Resource Manager
- My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\MDC

d. Delete any folders under *NMSROOT* that were not deleted during uninstallation.

Step 5 If you disabled Windows Defender before uninstalling the applications, re-enable it now.

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 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 5-21.

If you downgrade Security Manager, you must also downgrade Auto Update Server 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 you 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 AUS 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 6-1
- Tips for Installing the Security Manager Client, page 6-5
- Installing the Security Manager Client, page 6-6
- Logging In to the Applications, page 6-10
- Uninstalling Security Manager Client, page 6-12

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:

- HTTP/HTTPS Proxy Exception, page 6-1
- Configuring Browser Cookies, page 6-2
- Configuring Internet Explorer Settings, page 6-2
- Configuring Firefox Settings, page 6-3
- Enabling and Configuring Exceptions in Third-party Tools, page 6-5

HTTP/HTTPS Proxy Exception

If you use an HTTP/HTTPS proxy, you need to configure a proxy exception for the Security Manager server.

This requirement applies to Internet Explorer and Firefox, for which additional configuration details are provided in the sections that follow.

Configuring Browser Cookies

When more than one browser is installed, the default browser's cookies should be enabled. More specifically, Internet Explorer Privacy Settings should be set at the Medium level or lower (IE > Tools > Internet Options > Privacy Settings <= Medium).

Blocking cookies can cause Security Manager user login to fail even after a clean installation of Security Manager. If user login fails after a clean installation of Security Manager, you may see the following error message: “CMF session id cannot be assigned.”

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 If you are using Internet Explorer 8.x, 9.x, 10.x, or 11.x, use Compatibility View; Internet Explorer 8.x, 9.x, 10.x, and 11.x are supported only in Compatibility View. To use Compatibility View, open Internet Explorer, navigate to Tools > Compatibility View Settings, and add the Security Manager server as a website to be displayed in Compatibility View.

Step 2 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**. Refer to http://windows.microsoft.com/en-US/windows-vista/Internet-Explorer-Pop-up-Blocker-frequently-asked-questions.

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

Step 3 In Internet Explorer, select **Tools > Internet Options**. All subsequent steps in this procedure are performed in the Internet Options dialog box.

Step 4 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 5 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 6 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 7 (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 8 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 6-3
- Editing the Size of the Disk Cache, page 6-4
- Disabling the Popup Blocker or Creating an Allow List, page 6-4
- Enabling JavaScript, page 6-4
- Displaying Online Help on a New Tab in the Most Recent Window and Reusing Existing Windows on Subsequent Requests, page 6-5

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:

```
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:

Step 1 Select **Tools > Options**, then click **Advanced**.

Step 2 Reserve more space for the cache if the setting is too small, then click **OK**.

Disabling the Popup Blocker or Creating an Allow List

Procedure

To disable popup blockers, do the following:

Step 1 Select **Tools > Options**, then click the **Content** icon.

Step 2 Deselect the **Block pop-up windows** check box.

Alternatively, to create an allow 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 an allow 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 for normal day-to-day operations. 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.

  On the other hand, you can start the client more than once to connect to different Security Manager servers that are running the same version.

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 3-11.

If you run into problems during installation, see the following topics:

- Configuring a Non-Default HTTP or HTTPS Port, page 6-9
- Unable to Upgrade From a Previous Version of the Client, page 6-9
- Client Problems During Installation, page A-11.

Before You Begin

- Ensure that your browser is configured correctly. See Configuring Web Browser Clients, page 6-1.
- Ensure that Windows Firewall is configured correctly. On the operating systems supported by Security Manager, Windows Firewall is enabled by default. As a result, inbound connections for HTTP, HTTPS and syslog are blocked. For example, an admin can access the Security Manager client installation URL locally on the server but not from remote workstations. Another example is syslog data not showing up in Event Viewer. You must disable Windows Firewall or configure inbound rules to permit the management traffic in question.

Caution If you disable Windows Firewall on your workstation, it is vulnerable to malicious activity that Windows Firewall acts to prevent when it is enabled.

- 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 on your workstation, 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.

Tip To disable Cisco Security Agent on your workstation, use one of the following two methods: (1) right-click the Cisco Security Agent icon in the system tray and select **Security Level > Off** or (2) open **Services** (Control Panel > Administrative Tools > Services), right-click **Cisco Security Agent**, and click **Stop**. For both of these two methods, you then need to take the following step for some versions of Windows: open **Services** right-click **Cisco Security Agent Monitor**, and click **Stop**. After you finish installing the client, re-start Cisco Security Agent.

Caution While Cisco Security Agent is disabled on your workstation, it is vulnerable to malicious activity that Cisco Security Agent acts to prevent when it is enabled.

- If you already have the Security Manager client installed on the workstation, the installation program must 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 On the Cisco Security Management Suite home page, click **Cisco Security Manager Client Installer**.

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).

Note A special consideration applies if you are using Internet Explorer 10.x. When you click **Cisco Security Manager Client Installer**, you receive a prompt for user action (save or run), just as you do for all versions of Internet Explorer supported by Cisco Security Manager 4.18. If you choose the option to run, a dialog box appears and states that this option is not recommended; you then receive another prompt for user action. When you receive that prompt and click the **Actions** button, the SmartScreen Filter dialog box for Internet Explorer appears.
Important--You need to choose the option **Run Anyway** to start the client installation process.

Step 5 The installation wizard displays a "Welcome" screen.

The Security Manager client is installed as a single application with six views—Configuration Manager, Event Viewer, Report Manager, Health and Performance Manager, Image Manager, and Dashboard. Each can be launched independently in one of the following three ways (further information is available in Logging In to Security Manager Using the Security Manager Client, page 6-10):

- Start > All Programs > Cisco Security Manager Client [folder] > Cisco Security Manager Client
- [login screen]
- [after starting one of the views] Launch > [choose a different one of the views]

Note A desktop icon is also created for Cisco Security Manager. This icon opens the Cisco Security Management Suite home page.

Step 6 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 6-9.
- 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 > All Programs > Cisco Security Manager Client [folder] > 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 (x86)\Cisco Systems.

Step 7 Continue to follow the installation wizard instructions.

Step 8 After you click Done to complete the installation, if you disabled an antivirus application temporarily, re-enable it.

If the Cisco Security Agent on your workstation 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 to configure security settings on your workstation, and many different products that you may have installed, 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 note:

Note If Microsoft Windows User Account Control (UAC) is turned on, you must install and run the client with "Run as administrator."

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 (x86)\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:

Step 1 Start the Registry Editor by selecting **Start > Run** and entering **regedit**.

Step 2 Remove the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\f427e21299b0dd254754c0d2778feec4-837992615

Step 3 Delete the previous installation directory, usually C:\Program Files (x86)\Cisco Systems\Cisco Security Manager Client.

Step 4 Rename the following folder:

C:\Program Files (x86)\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 (x86)\Common Files\InstallShield directory, then try again. Also see Client Problems During Installation, page A-11.

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 permit (or click **Yes**) 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 6-12 and Installing the Security Manager Client, page 6-6.

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 6-10
- Logging In to Server Applications Using a Web Browser, page 6-12

Logging In to Security Manager Using the Security Manager Client

The Security Manager client is installed as an application suite with six applications—Configuration Manager, Event Viewer, Report Manager, Health and Performance Monitor, Image Manager, and Dashboard. Each can be launched independently in one of the three ways described in the procedure below.

Use the Configuration Manager application (which is part of the Security Manager client application suite) to perform most Security Manager tasks.

Tip You must log in to the client 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 Launch your choice of Configuration Manager, Event Viewer, Report Manager, Health and Performance Monitor, Image Manager, or Dashboard. Each can be launched independently in one of the following three ways:

- Start > All Programs > Cisco Security Manager Client [folder] > Cisco Security Manager Client
- [login screen]
- [after starting one of the applications] Launch > [choose a different one of the applications in the Security Manager client application suite]. The login dialog window does not appear.

Step 2 In the Security Manager login dialog window, enter or select the DNS name of the server you want to log in to.

Note If you enter or select the IP address—instead of the DNS name—some features may not function as intended in an Internet Explorer 7 environment. To ensure the correct function of all Security Manager features, enter the DNS name of the server to which you want to log in.

Step 3 Enter your Security Manager username and password.

Step 4 If the server uses HTTPS for connections, ensure that the HTTPS check box is selected; otherwise, deselect it. Click **Login**.

Step 5 If the server prompts you to download and install a client software update, see Patching a Client, page 6-10.

Step 6 If you log in to a Security Manager server that is running a higher version than your client, a notification will be displayed and you will have the option of downloading the matching client version.

Step 7 If there are no sessions running with the username and password that you just entered, the client application (Configuration Manager, Event Viewer, Report Manager, Health and Performance Monitor, Image Manager, or Dashboard) logs in to the server and opens the client interface.

Step 8 If there is already a session running with the username and password that you just entered, an informational message appears to inform you that there is an easier way to launch the new application with the same session from the existing application. That way is the following:

[after starting one of the applications] Launch > [choose a different one of the applications in the Security Manager client application suite].

Step 9 The new application is launched from the existing session, or, if it is already running, it is brought to focus.

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 10 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, and Auto Update Server 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 6-1.

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**.
- 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 **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 > All Programs > Cisco Security Manager Client > Uninstall Cisco Security Manager Client** and follow the uninstallation wizard prompts.

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 7-1
- Verifying that Required Processes Are Running, page 7-2
- Configuration of Heap Sizes for Security Manager Processes using MRF, page 7-2
- Best Practices for Ongoing Server Security, page 7-7
- Verifying an Installation or an Upgrade, page 7-8
- (Optional) Changing the Hostname of the Security Manager Server, page 7-8
- Where To Go Next, page 7-9

Server Tasks To Complete Immediately

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

✓	Task
❑	1. **Re-enable or re-install antivirus scanners and similar products.** If you uninstalled or temporarily disabled any server security software, such as an antivirus tool, re-install or restart that software now, then restart your server if required.Make sure to exclude the NMSROOT directory and the eventing folder from scanning as long as Security Manager is installed on the server. **Note** 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.
❑	2. **Re-enable the services and server processes that you disabled for installation.** Do not re-enable IIS.
❑	3. **Re-enable any mission-critical applications that you disabled for installation, including those that use any Sybase technology or software code.**
❑	4. **On the server, add a self-signed certificate to the list of trusted certificates.** To learn how, see your browser documentation.
❑	5. **Check for updates on Cisco.com for Security Manager and its related applications.** If you learn that updates are available, install the ones that are relevant to your organization and network.

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 7-1 to understand which applications require which processes.

Table 7-1 Application Process Requirements

This application:	Requires these Daemon Manager processes:
Common Services	Apache CmfDbEngine CmfDbMonitor CMFOGSServer CSRegistryServer DCRServer diskWatcher EDS EDS-GCF ESS EssMonitor jrm LicenseServer Proxy Tomcat TomcatMonitor NameServer NameServiceMonitor EventFramework
Cisco Security Manager	AthenaOGSServer ccrWrapper CsmReportServer rptDbEngine rptDbMonitor VmsBackendServer vmsDbEngine vmsDbMonitor VmsEventServer CsmHPMServer
Auto Update Server	AusDbEngine AusDbMonitor

Configuration of Heap Sizes for Security Manager Processes using MRF

Memory Reservation Framework (MRF), a feature introduced in Security Manager 4.1, provides Cisco Security Manager administrators the capability to modify heap sizes of key processes; doing so can enhance the performance of the server. MRF enables processes to adjust heap sizes on the basis of the RAM installed on the server.

The Security Manager processes that can be configured using MRF are listed in Table 7-2.

Table 7-2 Security Manager Processes that Can Be Configured by Using MRF

Process	Name as shown in pdshow	Description
Backend Process	VmsBackendServer	Performs device discovery and deployment operations.
Tomcat	Tomcat	Hosts applications responsible for editing and validating policies, etc.
Report Server	CsmReportServer	Generates reporting data.
Event Server	VmsEventServer	Collects events being sent from devices.

Note There is no MRF configuration for the HPM (Health and Performance Monitor) server.

Note You can learn more about the pdshow command in the previous section, Verifying that Required Processes Are Running, and in the Common Services documentation.

Default Configuration

The processes listed in Table 7-3, which are the Security Manager processes that can be configured by using MRF, are pre-configured with default values for heap sizes. Table 7-3 lists the default minimum and maximum heap sizes in megabytes for different amounts of RAM available to the server for each Security Manager process that can be configured by using MRF.

Table 7-3 Default Heap Sizes Preconfigured for Security Manager Processes

Physical RAM on server (GB)	VmsBackendServer	Tomcat	CsmReportServer	VmsEventServer	CsmHPMServer
< 8	1024, 2048	512, 1024	1024, 1024	1024, 2048	512, 1024
8	1024, 3072	1024, 2048	1024, 1024	1024, 3072	512, 1024
12	2048, 4096	2048, 3072	1024, 2048	2048, 4096	512, 1024
16	2048, 4096	2048, 4096	1024, 4096	4096, 4096	512, 1024
24	4096, 8192	4096, 4096	1024, 4096	4096, 8192	512, 1024
>= 28	8192, 8192	4096, 4096	1024, 4096	4096, 8192	512, 1024

Some RAM is reserved for the operating system and for other processes and is not listed here. For example, consider the case of 16 GB RAM in Table 7-3. The total maximum heap size for all 4 processes is (4096 + 4096 + 1024 + 4096) = 13312 Mb or 13 Gb. There is 3 GB additional RAM available for the operating system and for other processes.

Configuration Commands

MRF provides a command and a set of sub-commands to read and modify heap sizes for Security Manager server processes. Minimum and maximum heap sizes can be set for the process by using the mrf command. Information on using of this command is displayed by executing this command as follows:

```
> mrf
mrf help
            Prints this message.
mrf backup
            Backup existing configuration
mrf revert
            Restores backed up configuration
mrf set_heap_params process X-Y [min],[max]
            Sets minimum and maximum heap sizes
            process -> process name
            X-Y -> Memory Range in MB to which heap sizes apply
            [min],[max] -> minimum and maximum heap sizes in MB. These are optional but
atleast one should be specified.
mrf get_heap_params process [memory]
            Prints minimum and maximum heap sizes in MB
            process -> process name
            [memory] -> memory size in MB for which heap sizes are to be printed. If not
specified heap sizes are to be printed for current system memory.
```

Make sure that only valid process names are used while running **mrf** commands. No error is thrown when an invalid process name is specified. Valid process names are listed in Table 7-2. Process names are case-sensitive.

Configuring Heap Sizes for Processes

Configuring heap sizes for Security Manager processes can be thought of as consisting of the following three major steps:

1. Save Existing Configuration
2. Read Existing Configuration
3. Modify Configuration

1. Save Existing Configuration

Configuring a process heap size is a critical procedure that can affect the performance of Security Manager, so Cisco recommends that it be done only under the guidance of application experts.

Also, as a precautionary measure, Cisco recommends that you save your existing memory configurations for processes before changing them, and MRF provides two methods for doing so.

1. The first method can be used if you are testing the configuration changes. In this case the old configuration can be saved, and new modifications can be reverted to old configurations, by using the two commands listed below, respectively:

```
mrf backup
mrf revert
```

2. The second method is useful if you would like to revert to old values after you have used the new configuration for a significant period. There are two ways of doing this; you can use one or the other of the following ways:
   a. You can run mrf revert, provided you have not run mrf backup after you did the configuration changes.
   b. You will be taking a backup of your Cisco Security Manager Server before you make configuration changes. If you want to revert the changes, then restore the backup. In this case, data changes done after backup was taken will be lost.

2. Read Existing Configuration

Now that you have saved your data, you can query existing values for the processes by using the following command:

mrf get_heap_params *[process name] [memory]*

If memory is not specified in this command, the current RAM size will be used. Usually you are interested in the current RAM size. The parameter *[process name]* has one of the values listed in Table 7-2. Process names are case-sensitive.

The output of the command appears as shown below. Values are in MB.

```
Minimum Heap Size = 1024
Maximum Heap Size = 2048
```

3. Modify Configuration

After you have verified the current configuration, you can proceed to modify the configuration as described in this section.

To configure the heap sizes, use the following command:

mrf set_heap_params *[process name] [X-Y] [min],[max]*

The parameter *[process name]* can be any of the processes listed in Table 7-2. Process names are case-sensitive.

You need to restart the Security Manager server after executing this command for the changes to take effect.

Note Changes made by using **mrf set_heap_params** can be lost if the backup that was taken before modifying heap parameters is restored. In this case, if you want to retain the new values, you can follow these steps:

1. Run, mrf backup
2. Do application restore.
3. Run, mrf revert

This command uses the following syntax:

mrf set_heap_params *[process name] [X-Y] [min],[max]*

Sets minimum and maximum heap sizes

[X-Y[: memory range in MB to which heap sizes apply

[min],[max]: minimum and maximum heap sizes in MB. These are optional but at least one should be specified.

The parameter *[process name]* has one of the values listed in Table 7-2. Process names are case-sensitive.

Examples of Modify Configuration

The following examples illustrate how you can modify heap size configurations:

- mrf set_heap_params Tomcat 7372-8192 2048,4096

  Sets minimum and maximum heap sizes to 2048 MB and 4096 MB, respectively, for the Tomcat process when the RAM size is in the range of 7372 MB to 8192 MB

- mrf set_heap_params Tomcat 7372-8192 2048

  Sets the minimum heap size to 2048 MB for the Tomcat process when the RAM size is in the range of 7372 MB to 8192 MB

- mrf set_heap_params Tomcat 7372-8192,4096

  Sets the maximum heap size to 4096 MB for the Tomcat process when the RAM size is in the range of 7372 MB to 8192 MB

- mrf set_heap_params Tomcat 8080-8080 2048,4096

  Sets the minimum and maximum heap sizes to 2048 MB and 4096 MB, respectively, for the Tomcat process when the RAM size is 8080 MB. You can execute the **getramsize** command to get the existing RAM size in MB.

Verification of Modify Configuration

After heap parameters are set, you can verify the changes by executing the **mrf get_heap_params** command.

Summary of Configuring Heap Sizes for Processes

The three major steps described in this section for configuring heap sizes for Security Manager processes can be summarized by the following commands, listed in their order of execution:

```
mrf backup
mrf get_heap_params process
mrf set_heap_params Tomcat 7372-8192 2048,4096
mrf revert #if required to revert changes
```

Typical scenarios in which the User Might Have to Reconfigure Heap Sizes

Scenario 1

A Security Manager 4.0 user potentially may be using a maximum heap size of 4 GB for the Backend Process (VmsBackendServer). This is more than the default maximum heap size of 3 GB allocated in Security Manager 4.1 for 8 GB RAM. In this scenario, the user may have to reconfigure the Backend Process heap size to 4 GB. The user can choose to do this in case Event Management, which uses the Event Server process (VmsEventServer) is not enabled.

Scenario 2

Suppose Security Manager is being used in configuration-only mode (Event Management and reporting are disabled). In this scenario, the Backend Process and Tomcat heap sizes can be increased.

Scenario 3

Suppose Security Manager is being used in configuration-only mode (Event Management and reporting are disabled) and Event Management needs to be enabled. In this scenario, the Backend process and Tomcat heap sizes should be decreased, before enabling Event Management, so that the total of all heap sizes of Security Manager processes does not exceed the RAM size available to the server.

Scenario 4

Event Management and the Backend process are memory-intensive and need higher RAM allocation. (If event Management is unused, that RAM could be allocated for the Backend process by increasing its maximum heap size.)

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:

✓	Task
❑	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. **Note** Remove the logs/ database backup files regularly in order to maintain sufficient free space on your hard disk at all times. It is recommended to have a minimum of 10GB hard disk space free.
❑	6. **Back up your Security Manager Server regularly.** If regular backups have not been made, or if several changes have been made to your Security Manager installation, back up your Security Manager server before running any Windows Update.

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-6.

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 3-11.

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

(Optional) Changing the Hostname of the Security Manager Server

If you are required to change the hostname of the Security Manager Server, follow the steps below:

Step 1 Change the hostname in the OS:

a. Right-click **Computer** and select **Properties** or open **Control Panel** and select **System.**

b. Under **Computer Name, Domain and Workgroup Settings**, click **Change Settings**.

c. Click **Change** to modify the **Computer Name** (hostname).

d. Restart the computer.

Step 2 Stop the Security Manager Daemon Manager by entering **net stop crmdmgtd** in the command window.

Step 3 Execute the Security Manager Server hostname change script by running the following command in a command window:

```
NMSROOT\bin\perl NMSROOT\bin\hostnamechange.pl
```

In this command, NMSROOT is the path to the Security Manager installation directory.

Tip **hostnamechange.pl** is a utility that updates the hostname changes in the Common Services-related directories, files, database entries and registry entries after the hostname is changed in the OS.

Step 4 Restart the computer.

Note In this step, you must restart the computer. Restarting the Security Manager Daemon Manager is not sufficient.

Where To Go Next

If you want to:	Do this:
Understand the basics	See the interactive *JumpStart* guide that opens when you start Security Manager.
Get up and running with the product quickly	See the "Getting Started with Security Manager" topic in the online help, or see Chapter 1 of *User Guide for Cisco Security Manager*.
Complete the product configuration	See the "Completing the Initial Security Manager Configuration" topic in the online help, or see Chapter 1 of *User Guide for Cisco Security Manager*.
Manage user authentication and authorization	See the following topics: • User Permissions, page 8-3 • Integrating Security Manager with Cisco Secure ACS, page 8-12
Bootstrap your devices	See the "Preparing Devices for Management" topic in the online help, or see Chapter 2 of *User Guide for Cisco Security Manager 4.18,* available at http://www.cisco.com/c/en/us/support/security/security-manager/products-user-guide-list.html.

Managing User Accounts

Managing user accounts involves account creation and user permissions:

- Account Creation, page 8-1. Your account can be a local account on the Security Manager Server, an ACS account on the CiscoWorks Common Services server, or a non-ACS account on the Common Services server.
- User Permissions, page 8-3. Your permissions (or privileges) are the tasks that you are authorized to perform. Your permissions are defined by your role within Security Manager. Your role within Security Manager is established after your username and password are authenticated. Authentication is done by Security Manager during login.

Account Creation

To use Cisco Security Manager, you must log in with the **admin** account that you created during installation and create an account for each user. You can create the following types of accounts:

- Local Account, page 8-1
- ACS Account, page 8-2
- Non-ACS Account, page 8-2

Local Account

To create a local account:

1. Do one of the following:
   - If you currently have the Security Manager client open and are logged in with an admin account, you can select **Tools > Security Manager Administration** and select **Server Security** from the table of contents. The Server Security page has buttons that link to and open specific pages in Common Services. Click **Local User Setup** to navigate to the Local User Setup page in Common Services.
   - Using your web browser, link to the Security Manager server using the URL https://*servername*, where *servername* is the IP address or DNS name of the server. This URL opens the Security Manager home page. Click **Server Administration** to open Common Services. Point to **Server > Single-Server Management > Local User Setup** to navigate to the Local User Setup page in Common Services.
2. Click **Add**.

ACS Account

To create an ACS account:

1. Do one of the following:
   - If you currently have the Security Manager client open and are logged in with an admin account, you can select **Tools > Security Manager Administration** and select **Server Security** from the table of contents. The Server Security page has buttons that link to and open specific pages in Common Services. Click **AAA Setup** to navigate to the Authentication Mode Setup page in Common Services.
   - Using your web browser, link to the Security Manager server using the URL https://*servername*, where *servername* is the IP address or DNS name of the server. This URL opens the Security Manager home page. Click **Server Administration** to open Common Services. Point to **Server > AAA Mode Setup** to navigate to the Authentication Mode Setup page in Common Services.
2. Select **ACS** under AAA Mode Setup.

Tip An ACS account uses (1) the ACS type of AAA Mode Setup (this is on the Authentication Mode Setup page) and (2) the ACS login module in CiscoWorks Common Services. However, you do not need to select the ACS login module; it is selected for you automatically when you select the ACS type of AAA Mode Setup.

Non-ACS Account

To create a non-ACS account:

1. Do one of the following:
   - If you currently have the Security Manager client open and are logged in with an admin account, you can select **Tools > Security Manager Administration** and select **Server Security** from the table of contents. The Server Security page has buttons that link to and open specific pages in Common Services. Click **AAA Setup** to navigate to the Authentication Mode Setup page in Common Services.
   - Using your web browser, link to the Security Manager server using the URL https://*servername*, where *servername* is the IP address or DNS name of the server. This URL opens the Security Manager home page. Click **Server Administration** to open Common Services. Point to **Server > AAA Mode Setup** to navigate to the Authentication Mode Setup page in Common Services.
2. Select **Local RBAC** under AAA Mode Setup.

Tip A non-ACS account uses (1) the Local RBAC type of AAA Mode Setup (this is on the Authentication Mode Setup page) and (2) one of the following login modules in CiscoWorks Common Services: CiscoWorks Local (the default login module), Local NT System, MS Active Directory, RADIUS, or TACACS+.

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 on ACS integration, refer to the following sections of this chapter:

- Integrating Security Manager with Cisco Secure ACS, page 8-12
- Troubleshooting Security Manager-ACS Interactions, page 8-28

Prior to Security Manager 4.3, the major advantages of using Cisco Secure ACS were (1) the ability to create highly granular user roles with specialized permission sets (for example, allowing the user to configure certain policy types but not others) and (2) the ability to restrict users to certain devices by configuring network device groups (NDGs). These granular privileges (effectively "role-based access control," or RBAC) were not available in Security Manager 4.2 and earlier versions, unless you used Cisco Secure ACS. These granular privileges (RBAC) are available in Security Manager 4.3 and later because they use Common Services 4.0 or later, in which local RBAC is available without the use of ACS.

Security Manager 4.18 retains compatibility with ACS 4.2. See Integrating Security Manager with Cisco Secure ACS, page 8-12.

Note Users who wish to migrate their RBAC abilities from ACS to Common Services must do so manually; there are no migration scripts or other migration support.

Tip 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 8-10.

The following topics describe user permissions:

- Security Manager ACS Permissions, page 8-4
- Understanding CiscoWorks Roles, page 8-6
- Understanding Cisco Secure ACS Roles, page 8-9
- Default Associations Between Permissions and Roles in Security Manager, page 8-11

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 8-10).

- **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.
  - **View > Topology**. Allows you to view maps configured in Map view.
  - **View > Event Viewer**. Allows you to view events in the Event Viewer in both the Real Time Viewer and the Historical Viewer.
  - **View > Report Manager**. Allows you to view reports in Report Manager.
  - **View > Schedule Reports**. Allows you to schedule reports in Report Manager.
  - **View > Health and Performance Manager**. Allows you to launch the Health and Performance Manager.
  - **View > Image Manager**. Allows you to launch the Image Manager.
- **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.
  - **Modify > Manage Event Monitoring**. Allows you to enable and disable the monitoring in Security Manager for any device, so that Security Manager starts or stops event reception and processing from that device.
  - **Modify > Modify Image Repository**. Allows you to modify items in the Image Repository and to check for image updates from Cisco.com.
- **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.
  - 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 8-6
- Selecting an Authorization Type and Assigning Roles to Users in Common Services, page 8-7

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**—Can approve the modification of changes and CLI changes.
- **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**—Can only deploy changes.

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 8-9.

- **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.

Tip In Security Manager, the System Administrator role has the highest level of permissions.

- **Super Admin—**Can perform all CiscoWorks operations including the administration and approval tasks. By default, this role has full privileges.

Tip In Security Manager, the Super Admin role does not have the highest level of permissions. Also, the Super Admin role is specific to Common Services and not to ACS.

- **Security Administrator—**Can only modify, assign, and submit changes.
- **Security Approver—**Can approve only the modification of changes.

Image Manager

Additional tasks for each of the default roles are defined for Image Manager, a feature that first appeared in Security Manager 4.3 and continues to be available in Security Manager 4.18:

- Launching Image Manager
- Adding images to the repository in Security Manager
- Creating image upgrade jobs

When using a local account (unique to Security Manager, defined on the Security Manager server), these additional tasks are assigned to different roles as listed in Table 8-1.

Table 8-1 Image Manager Tasks for Default Roles

	Tasks		
Role	**Launch and View**	**Add Images to Repository**	**Create Image Upgrade Jobs**
Help Desk	Yes	No	No
Approver	Yes	No	No
Network Operator	Yes	No	No
Network Administrator	Yes	Yes	Yes
System Administrator	Yes	Yes	Yes
Security Administrator	Yes	No	No

For details about which Security Manager permissions are associated with each CiscoWorks role, see Default Associations Between Permissions and Roles in Security Manager, page 8-11.

For a detailed series of tables that shows the RBAC permissions matrix for Image Manager, see Appendix B, "Permissions Matrix for Image Manager."

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 Selecting an Authorization Type and Assigning Roles to Users in Common Services, page 8-7.
- To generate a permissions table in CiscoWorks, select **Server > Reports > Permission** and click **Generate Report**.

Selecting an Authorization Type and Assigning Roles to Users in Common Services

In CiscoWorks Common Services 4.2.2, the Local User Setup > Add page is used (1) to select one of the three authorization types that are available for local users and (2) to assign roles to users. The three authorization types are the following:

- Full Authorization
- Enable Task Authorization

- Enable Device Authorization

You must select one of these three authorization types (Full Authorization, Enable Task Authorization, or Enable Device Authorization) when you add a local user in Common Services.

Selecting any of these three authorization types enables you to select the roles that the local user should have. Selecting the roles that the local user should have is important because it defines the operations that the user is authorized to perform.

For example, if you select the Help Desk role, the user is limited to view operations and cannot modify any data. For another example, if you assign the Network Operator role, the user is also able to modify the configuration archive. You can assign more than one role to a particular user.

By default the Help Desk role is enabled. You can also clear default roles, and you can set any roles to be default roles.

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

Related Topics

- Security Manager ACS Permissions, page 8-4
- Default Associations Between Permissions and Roles in Security Manager, page 8-11
- Understanding CiscoWorks Roles, page 8-6

Step 1 Navigate to the Local User Setup page in Common Services by following this path:

Server where Security Manager is installed >

desktop icon for Cisco Security Manager application >

admin account login (or user account with sufficient privileges) >

Server Administration >

Server > [menu selector symbol] >

Security >

Single-Server Management >

Local User Setup

Step 2 Do one of the following:

- To create a user, click **Add** and enter the appropriate information in the following fields: Username, Password, Verify Password, and Email.
- To change the authorizations of an existing user, check the check box next to the username and click **Edit**.

Step 3 Select **Full Authorization** if you want the user to have all the roles (Help Desk, Approver, Network Operator, Network Administrator, System Administrator, Super Admin, Security Administrator, and Security Approver) that are available in Security Manager.

Tip If you select **Full Authorization**, you cannot also select **Enable Task Authorization** or **Enable Device Authorization** (as indicated by the radio button format).

Skip to Step 6 in this procedure.

Step 4 Select **Enable Task Authorization** if you want the new user to have only roles that you select (such as Network Operator only).

Tip If you select **Enable Task Authorization**, you cannot also select **Full Authorization** or **Enable Device Authorization** (as indicated by the radio button format).

a. Select one or more of the following roles: Help Desk, Approver, Network Operator, Network Administrator, System Administrator, Super Admin, Security Administrator, and Security Approver. For more information about each role, see CiscoWorks Common Services Default Roles, page 8-6.

b. Skip to Step 8 in this procedure.

Step 5 Select **Enable Device Authorization** if you want the new user to be authorized only for device groups that you select, not all of the device groups that are present in your Security Manager installation. (You can define device groups on the Device Groups page at Security Manager > Tools > Security Manager Administration > Device Groups.)

Tip If you select **Enable Device Authorization**, you cannot also select **Full Authorization** or **Enable Task Authorization** (as indicated by the radio button format).

a. Select the device group(s) that you want the new user to be authorized for.

b. Select one or more of the following roles: Help Desk, Approver, Network Operator, Network Administrator, System Administrator, Super Admin, Security Administrator, and Security Approver. For more information about each role, see CiscoWorks Common Services Default Roles, page 8-6.

Step 6 Click **OK** to save your changes.

Step 7 Restart the Security Manager client.

Understanding Cisco Secure ACS Roles

Prior to Common Services 4.0 (used with Security Manager 4.3 and 4.4) and Common Services 4.2.2 (used with Security Manager from version 4.5 to version 4.18), Cisco Secure ACS provided greater flexibility than Common Services for managing Security Manager permissions because it (ACS) supported application-specific roles (effectively “role-based access control,” or RBAC).

These granular privileges (RBAC) are available in Common Services 4.0 and 4.2.2, in which local RBAC is available without the use of ACS. 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 8-10
- Customizing Cisco Secure ACS Roles, page 8-10

Cisco Secure ACS Default Roles

Cisco Secure ACS includes the same roles as CiscoWorks (see Understanding CiscoWorks Roles, page 8-6), 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.
- **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 8-6.

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 8-10.

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 8-11.

Related Topics

- Integrating Security Manager with Cisco Secure ACS, page 8-12
- User Permissions, page 8-3

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.

Related Topics

- Security Manager ACS Permissions, page 8-4
- Default Associations Between Permissions and Roles in Security Manager, page 8-11

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 8-4.

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 8-2 shows how Security Manager permissions are associated with CiscoWorks Common Services roles and the default roles in Cisco Secure ACS. Some roles (Super Admin, Security Administrator, and Security Approver) are not listed because they are not specifically associated with the default roles in Cisco Secure ACS. For information about the specific permissions, see Security Manager ACS Permissions, page 8-4.

Table 8-2 Default Permission to Role Associations in Security Manager and CiscoWorks Common Services

	Roles						
Permissions	**System Admin.**	**Security Admin.**	**Security Approver**	**Network Admin.**	**Approver**	**Network Operator**	**Help Desk**
View Permissions							
View Device	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View Policy	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View Objects	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View Topology	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View CLI	Yes	Yes	Yes	Yes	Yes	Yes	No
View Admin	Yes	Yes	Yes	Yes	Yes	Yes	No
View Config Archive	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View Device Managers	Yes	Yes	Yes	Yes	Yes	Yes	No
Modify Permissions							
Modify Device	Yes	Yes	No	No	No	No	No
Modify Hierarchy	Yes	Yes	No	No	No	No	No

Table 8-2 Default Permission to Role Associations in Security Manager and CiscoWorks Common Services

	Roles						
Permissions	**System Admin.**	**Security Admin.**	**Security Approver**	**Network Admin.**	**Approver**	**Network Operator**	**Help Desk**
Modify Policy	Yes	Yes	No	No	No	No	No
Modify Image	Yes	Yes	No	No	No	No	No
Modify Objects	Yes	Yes	No	No	No	No	No
Modify Topology	Yes	Yes	No	No	No	No	No
Modify Admin	Yes	No	No	No	No	No	No
Modify Config Archive	Yes	Yes	No	Yes	No	Yes	No
Additional Permissions							
Assign Policy	Yes	Yes	No	No	No	No	No
Approve Policy	Yes	No	Yes	No	No	No	No
Approve CLI	Yes	No	No	No	Yes	No	No
Discover (Import)	Yes	Yes	No	No	No	No	No
Deploy	Yes	No	No	Yes	No	No	No
Control	Yes	No	No	Yes	No	Yes	No
Submit	Yes	Yes	No	No	No	No	No

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 (1) the administrator name and password that you use to log in to the Cisco Secure ACS and (2) the shared key configured in ACS on external user addition. Fulfilling these requirements ensures the validity of communications between Security Manager and Cisco Secure ACS.

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 8-13
- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14
- Integration Procedures Performed in Cisco Secure ACS, page 8-15
- Integration Procedures Performed in CiscoWorks, page 8-21
- Restarting the Daemon Manager, page 8-25
- Assigning Roles to User Groups in Cisco Secure ACS, page 8-25

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 ASA security contexts devices. These are described in Adding Devices as AAA Clients Without NDGs, page 8-17.
- Network Device Groups must be enabled.

Tips

- If you already have devices imported into Security Manager prior to ACS integration, we recommend adding those devices to ACS as AAA clients before the integration. The name of the AAA client must match the display name of the device in Cisco Security Manager. If you do not do so, the devices will not show up in the Device list of Security Manager after the ACS integration.
- 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.

Related Topics

- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14
- Integrating Security Manager with Cisco Secure ACS, page 8-12

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 8-13
- Integrating Security Manager with Cisco Secure ACS, page 8-12

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 8-9
- *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 5-3
- *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 8-15.

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.

For more information, see Integration Procedures Performed in CiscoWorks, page 8-21.

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 8-25.

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 8-25.

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 8-15
2. Adding Managed Devices as AAA Clients in Cisco Secure ACS, page 8-17
3. Creating an Administration Control User in Cisco Secure ACS, page 8-20

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 8-10.

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 8-22.

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 8-13
- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14
- Assigning Roles to User Groups in Cisco Secure ACS, page 8-25

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**.

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 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.

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 8-11. For more information about customizing user roles, see Customizing Cisco Secure ACS Roles, page 8-10.

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 8-25.

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 8-22.

Step 5 Continue with Adding Managed Devices as AAA Clients in Cisco Secure ACS, page 8-17.

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, each context must be added individually to Cisco Secure ACS.

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 only to certain NDGs, add the devices as described in Configuring Network Device Groups for Use in Security Manager, page 8-18.

Note While devices do not need to be broken out into Network Device Groups, Security Manager expects the Security Manager Network Device to be in an NDG. "Not Assigned" is not an NDG. It is best to move all devices out of Not Assigned and into a Default NDG if multiple NDGs are not desired.

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 8-13
- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14

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 the ASA security context:
<parent_display_name>_<context_name>

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.

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 8-20.

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 8-18
- Activating the NDG Feature, page 8-19
- Creating NDGs, page 8-19
- Associating NDGs and Roles with User Groups, page 8-26

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 8-18
- User Permissions, page 8-3

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 8-19
- Associating NDGs and Roles with User Groups, page 8-26
- NDGs and User Permissions, page 8-18
- Configuring Network Device Groups for Use in Security Manager, page 8-18

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 8-19.

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 8-19.

Related Topics

- Associating NDGs and Roles with User Groups, page 8-26
- NDGs and User Permissions, page 8-18
- Configuring Network Device Groups for Use in Security Manager, page 8-18

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 8-17.

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 8-20.

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 8-26.

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 8-23.

Related Topics

- ACS Integration Requirements, page 8-13
- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14

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 8-15), 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 8-21
- Defining the System Identity User, page 8-22
- Configuring the AAA Setup Mode in CiscoWorks, page 8-23
- Configuring an SMTP Server and System Administrator Email Address for ACS Status Notifications, page 8-24

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 8-15). This local user account is later used for the system identity setup. For more information, see Defining the System Identity User, page 8-22.

Related Topics

- ACS Integration Requirements, page 8-13
- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14

Step 1 Navigate to the Local User Setup page in Common Services by following this path:

Server where Security Manager is installed >

desktop icon for Cisco Security Manager application >

admin account login >

Server Administration >

Server > [menu selector symbol] >

Security >

Single-Server Management >

Local User Setup

Step 2 Click **Add**.

Step 3 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 8-15.

Step 4 Check all check boxes under Roles.

Step 5 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 8-15
- Creating a Local User in CiscoWorks, page 8-21

Related Topics

- ACS Integration Requirements, page 8-13
- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14

Step 1 Navigate to the System Identify Setup page in Common Services by following this path:

Server where Security Manager is installed >

desktop icon for Cisco Security Manager application >

admin account login >

Server Administration >

Server > [menu selector symbol] >

Security >

Multi-Server Trust Management >

System Identity Setup

Step 2 Enter the name of the system identity user that you created in Cisco Secure ACS. See Defining Users and User Groups in Cisco Secure ACS, page 8-15.

Step 3 Enter and verify the password for this user.

Step 4 Click **Apply**.

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 re-register 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 re-register the new applications and Cisco Security Manager. In addition to re registering Security Manager with ACS, you must configure your existing system identity user and grant it the newly introduced permissions; otherwise, RBAC will not work properly. Please refer to Defining the System Identity User, page 8-22.

Related Topics

- ACS Integration Requirements, page 8-13
- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14

Step 1 Navigate to the AAA Mode Setup page in Common Services by following this path:

Server where Security Manager is installed >

desktop icon for Cisco Security Manager application >

admin account login >

Server Administration >

Server > [menu selector symbol] >

Security >

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 8-20.

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 8-17.

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 8-25.

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 8-25.

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 Navigate to the System Preferences page in Common Services by following this path:

Server where Security Manager is installed >

desktop icon for Cisco Security Manager application >

admin account login >

Server Administration >

Server > [menu selector symbol] >

Admin >

System Preferences

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 8-14
- ACS Integration Requirements, page 8-13

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.

Step 5 Continue with Assigning Roles to User Groups in Cisco Secure ACS, page 8-25.

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 8-25
- Associating NDGs and Roles with User Groups, page 8-26

Note Cisco Security Manager and ACS integration works better by creating a special NDG that contains the CiscoWorks/Security Manager servers.

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 8-10.

Before You Begin

- Create a user group for each default role. See Defining Users and User Groups in Cisco Secure ACS, page 8-15.
- Complete the procedures described in these topics:
  - Integration Procedures Performed in Cisco Secure ACS, page 8-15
  - Integration Procedures Performed in CiscoWorks, page 8-21

Related Topics

- Understanding CiscoWorks Roles, page 8-6
- Understanding Cisco Secure ACS Roles, page 8-9

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 8-15), 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.

e. Click **Submit** to save the group settings.

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 8-10.

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 8-18.

Related Topics

- ACS Integration Requirements, page 8-13
- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14

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 8-10.

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 8-28
- Authentication Fails When in ACS Mode, page 8-29
- System Administrator Granted Read-Only Access, page 8-29
- ACS Changes Not Appearing in Security Manager, page 8-30
- Devices Configured in ACS Not Appearing in Security Manager, page 8-30
- Working in Security Manager after Cisco Secure ACS Becomes Unreachable, page 8-30
- Restoring Access to Cisco Secure ACS, page 8-31
- Authentication Problems with Multihomed Devices, page 8-31
- Authentication Problems with Devices Behind a NAT Boundary, page 8-31

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, 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 8-17.

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*.

Local RBAC Using Common Services 4.2.2

Prior to Security Manager 4.3, the major advantages of using Cisco Secure ACS were (1) the ability to create highly granular user roles with specialized permission sets (for example, allowing the user to configure certain policy types but not others) and (2) the ability to restrict users to certain devices by configuring network device groups (NDGs). These granular privileges (effectively “role-based access control,” or RBAC) were not available in Security Manager 4.2 and earlier versions, unless you used Cisco Secure ACS. These granular privileges (RBAC) are available in Security Manager 4.3 and later because they use Common Services 4.0 or later, in which local RBAC is available without the use of ACS.

Security Manager 4.18 retains compatibility with ACS 4.2. See Integrating Security Manager with Cisco Secure ACS, page 8-12.

Note Users who wish to migrate their RBAC abilities from ACS to Common Services must do so manually; there are no migration scripts or other migration support.

Common Services 4.2.2 provides device-level RBAC, defining custom roles for users, and customizing existing roles for users. The following features are available:

- Managing users (add, remove, edit)
- Managing network device groups (NDGs) to provide device-level RBAC
- Managing custom roles
- Mapping roles to device groups
- Granular privileges for policy object types and policy types, such as “view network objects,” “modify service objects,” and “modify access rules.”

You can implement local RBAC using Common Services 4.2.2 by completing tasks in the following areas:

- Authentication Mode Setup, page 8-32
- User Management, page 8-32
- Group Management, page 8-33
- Role Management, page 8-33

Authentication Mode Setup

Follow the steps to set up a non-ACS account. See Non-ACS Account, page 8-2.

Then select the **CiscoWorks Local** login module.

Tip CiscoWorks Local is the default value for a clean installation of Security Manager.

User Management

Navigate to the Local User Setup page in Common Services:

Server where Security Manager is installed >

desktop icon for Cisco Security Manager application >

user account login >

Server Administration >

Home >

System Tasks >

Local User Setup

On the Local User Setup page, you can select a user and then choose one of the following actions:

- Import Users

- Export Users
- Edit
- Delete
- Add
- Modify My Profile

If you select more than one user, Edit is not available.

If you select no users, you can choose one of the following actions:

- Import Users
- Add
- Modify My Profile

If you select **Edit** or **Add**, you can select one of these three authorization types:

- Full Authorization
- Enable Task Authorization
- Enable Device Authorization

Group Management

Navigate to the Device Groups page in Security Manager:

Server where Security Manager is installed >

desktop icon for Configuration Manager application >

user account login >

Tools >

Security Manager Administration >

Device Groups

You cannot manage device groups through the Common Services interface (Server where Security Manager is installed > desktop icon for Cisco Security Manager application).

Role Management

Navigate to the Role Management Setup page:

Server where Security Manager is installed >

desktop icon for Cisco Security Manager application >

user account login >

Server Administration >

Server > [menu selector symbol] >

Security >

Single-Server Management >

Role Management Setup

The Role Management Setup page displays the default roles, which are Approver, Help Desk, Network Administrator, Network Operator, Security Administrator, Security Approver, Super Admin, and System Administrator. The Role Management Setup page also displays custom roles, if any, that you have added.

On the Role Management page, you can perform the following operations: Add, Edit, Delete, Copy, Export, Import, Set as default, and Clear default.

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.

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-11
- Running a Server Self-Test, page A-17
- Collecting Server Troubleshooting Information, page A-18
- Viewing and Changing Server Process Status, page A-18
- Reviewing the Server Installation Log File, page A-19
- Symantec Co-existence Issues, page A-19
- Problems after Installing Windows Updates, page A-20
- Backup of Cisco Security Manager Server, page A-20
- Problem Connecting to an ASA Device with Higher Encryption, page A-21
- Pop-up Showing Activation.jar in Use During the Time of Installation, page A-21
- How to Set the Locale for the Windows Default User Template to U.S. English, page A-22
- How to disable the RMI Registry Port, page A-25

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 3-1. 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 A-1 Required Services and Ports

Service	Used For, or Used By	Port Number/ Range of Ports	Protocol	Inbound	Outbound
FTP	Security Manager communication with TMS server	21	TCP	—	X
SSH	Common Services	22	TCP	—	X
	Security Manager	22	TCP	—	X
Telnet	Security Manager	23	TCP	—	X
SMTP	Common Services	25	TCP	—	X
TACACS+ (for ACS)	Common Services	49	TCP	—	X
TFTP	Common Services	69	UDP	X	X
HTTP	Common Services	80	TCP	—	X
	Security Manager		TCP	—	X
SNMP (polling)	Common Services	161	UDP	—	X
	Performance Monitor	161	UDP	—	X
SNMP (traps)	Common Services	162	UDP	—	X
	Performance Monitor	162	UDP	X	—
HTTPS (SSL)	Common Services	443[1]	TCP	X	—
	Security Manager		TCP	X	X
	AUS		TCP	X	—
	Performance Monitor		TCP	X	—
Syslog[2]	Security Manager	514	UDP	X	—
	Common Services (without Security Manager installed)	514 or 49514 (see footnote for this row)	UDP	X	—
	Performance Monitor (without Security Manager installed)	514	UDP	X	—
Remote Copy Protocol	Common Services	514	TCP	X	X

Table A-1 Required Services and Ports (continued)

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

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-6
- Server Problems During Uninstallation, page A-9

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 A-2 Installation Error Messages (Server)

Message	Reason for Message	User Action
`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\Wow6432Node\Cisco\Resource Manager\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 2-10.
`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.

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

Message	Reason for Message	User Action
The Windows 2012 R2 server may not have the following Microsoft Windows patches: a. KB2919442 b. Run clearcompressionflag.exe c. KB2919355, KB2932046, KB2959977, KB2937592, KB2938439, and KB2934018 d. KB2999226 These patches are required to register critical Cisco Security Manager services in this server. Ensure that you install these patches in the aforesaid order. We recommend you to install these patches before installing the Cisco Security Manager. Alternatively, you can also install these patches after installing the Cisco Security Manager, and then run the "<CSMInstalledDirectory>\CSCOpx\bin\RegisterApache.bat " CSM scripts to register the services. For more information, refer the Installation Guide for Cisco Security Manager. To continue with installation, click OK. To abort the installation, click Cancel.	The recommended Windows Update patches may be missing in your Windows 2012 R2 server.	Ensure you have the required patches installed in your server, before you begin installing Cisco Security Manager. You may proceed installing Cisco Security Manager, and then install these patches. However, you will be required to register Apache Services with the windows services. For more information, refer Readiness Checklist for Installation, page 4-3.
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 and Recommendations, page 3-4.
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.	Temporary files that are supposed to be deleted automatically during software installations have not been deleted on your server.	Search the temporary directory on your server for subdirectories with names that include the "_istmp" string. Delete all such subdirectories.

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

Message	Reason for Message	User Action
`Windows cannot find 'C:\Documents and Settings\Administrator\WINDOWS\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.`	You left Terminal Services enabled during installation, even though we do not support this. See Readiness Checklist for Installation, page 4-3.	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 http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/3.1/install/guide/IGSG31.html 2. Try again to install Security Manager.
`Setup has detected that unInstallShield is in use. Close unInstallShield and restart setup. Error 432.`	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.	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.

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. I want to change the hostname of the Security Manager Server. How do I achieve this?

A. You can change the hostname of the Security Manager Server by performing the steps detailed in (Optional) Changing the Hostname of the Security Manager Server, page 7-8.

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 2-10.
- 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 and Recommendations, page 3-4.) 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 5-25.
- 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 5-3). You must uninstall and re-install the server software. See Uninstalling Server Applications, page 5-25.
- Your client system does not meet the minimum requirements. See Client Requirements, page 3-11.
- 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 3-11.

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 A-3 Causes and Workarounds for LiaisonServlet Error

Cause	Workaround
Anti-virus application installed on server	Uninstall the anti-virus application.
IIS installed on server	IIS is not compatible with Security Manager and must be uninstalled.
Services required by Security Manager do not start in proper order	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.

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

Cause	Workaround

casuser password	The following five permissions are assigned and set, automatically, at the time of Security Manager installation:
	• Access this computer from network - casusers
	• Deny access to this computer from network - casuser
	• Deny logon locally - casuser
	• Log on as batch job - casuser, casusers
	• Log on as a service – casuser
	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 prompt on the server using the Run as administrator option.
	2. Type `NMSRoot\setup\support\resetCasuser.exe` and then press **Enter**.
	Note The location *NMSROOT* is the path to the Security Manager installation directory. The default is **C:\Program Files (x86)\CSCOpx.**
	3. Of the two option displayed, choose option 2 - Enter casuser password. You will be prompted to enter a password for casuser and then to reenter the password for confirmation.
	4. If local security policy is configured, add the casuser account to the 'Log on as a service' operation in the local security policy.
	5. Run the following command to apply the casuser permission to *NMSROOT*:
	`C:\Windows\System32\cacls.exe "NMSROOT" /E /T /G Administrators:F casusers:F`
	6. Run the following command to set the casuser to database services:
	`NMSROOT\bin\perl NMSROOT\bin\ChangeService2Casuser.pl "casuser" "casuserpassword"`

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 and Recommendations, page 3-4). 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 4-3. 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.

Q. Validation and some other operations fail with SQL query exception in logs. What happened?

A. It is possible that the Sybase temp directory ran out of disk space and, therefore, Sybase failed to create temp files. By default, Sybase creates temp files under the Windows temp directory. If the system variable SA_TMP is defined, then temp files are created in the directory specified by SA_TMP. Clear the disk space where the Sybase temp directory is located and then restart Security Manager.

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-10, where they are sorted alphabetically by their first word. For additional information about uninstallation error messages, see the Common Services documentation in your installation of Security Manager.

Table A-4 Uninstallation Error Messages

Message	Reason for Message	User Action
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. 0 file(s) copied. 1 file(s) copied.	Uninstallation failed.	Reboot the server, then complete the procedure described in Uninstalling Server Applications, page 5-25.
Windows Management Instrumentation (WMI) is running. 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.	Either your organization uses WMI or someone enabled the WMI service accidentally on your server.	Click **Yes**.

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.

Troubleshooting the Security Manager Client

This section answers questions that you might have about:

- Client Problems During Installation, page A-11
- Client Problems After Installation, page A-14

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-5 Installation Error Messages (Client)

Message	Reason for Message	User Action
`Could not install engine jar`	Previous software installations and uninstallations caused InstallShield to run incorrectly.	1. Navigate to: **C:\Program Files (x86)\ 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.

Table A-5 Installation Error Messages (Client) (continued)

Message	Reason for Message	User Action

`Error - Cannot Connect to Server`
 	
`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.`
	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`
 	
`Installation cannot proceed while the Cisco Security Agent is running`
 	
`Do you want to disable the Cisco Security Agent and continue with the installation?`
	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.

`Error - Cisco Security Agent not Stopped`
 	
`The installation will be aborted because the Cisco Security Agent could not be stopped.`
 	
`Please attempt to disable Cisco Security Agent before repeating the installation process.`
	Security Manager client was unable to stop the Cisco Security Agent.	Click **OK** to close this error message and abort the installation. Manually disable the Cisco Security Agent before retrying the installation.

Table A-5 Installation Error Messages (Client) (continued)

Message	Reason for Message	User Action
`Error occurred during the installation: null.`	Previous software installations and uninstallations caused InstallShield to run incorrectly.	1. Navigate to C:\Program Files (x86)\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 2008, 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**.

`Please read the information below.`
 	
`The following errors were generated:`
 	
• `WARNING: The <drive> partition has insufficient space to install the items selected.`
	You tried to install Security Manager Client on a drive or partition that does not have enough free space.	Click **Back**, then select a different location in which to install Security Manager Client.

`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.

Q. What should I do if the client installer suspends operation (hangs)?

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

- 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\Wow6432Node\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 (x86)\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 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.)

Note You might have to create an entry for your DNS additional entry which will point to the same IP address (which will be used in the Security Manager client application's "Server Name" field) in the httpd.conf configuration file under *NMSROOT~/MDC/Apache/conf/* and restart the Daemon Manager. Such an entry can help you establish connections to your server. Examples: `ServerName`, `foo.example.com`. [**Tip**: The location *NMSROOT* is the path to the Security Manager installation directory. The default is **C:\Program Files (x86)\CSCOpx.]**

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...?

... repeatedly that the server is checking its license.	Verify that your server meets the minimum hardware and software requirements. See Server Requirements and Recommendations, page 3-4.
`Synchronizing with DCR.`	There are two possible explanations: • 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 (x86)\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.

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. Why is the Activity Report not displayed when I use Internet Explorer as my default browser?

A. 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: http://support.microsoft.com/kb/281679/EN-US.

Q. How can I clear the server list from the Server Name field in the Login window?

A. 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 (x86)\Cisco Systems\Cisco Security Manager Client.

Q. The Security Manager client did not load because of a version mismatch. What does this mean?

A. 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.

Q. Where are the client log files located?

A. The client log files are located in C:\Program Files (x86)\Cisco Systems\Cisco Security Manager Client\logs. Each GUI session has its own log file.

Q. How do I know if Security Manager is running in HTTPS mode?

A. Do one of the following:

- 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.
- Go to Common Services > Server > Security > Single Server Management > 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.
- 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.

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 (x86)\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.

Running 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:	From a Security Manager server:
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 (x86)\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.	1. Open a Windows command window, for example, by selecting **Start > Run**, then enter **command**. 2. Enter **C:\Program Files (x86)\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-19.

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 **Cisco_Prime_install_*.log**.

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 Product Documentation, page x.

Symantec Co-existence Issues

If you are using Symantec Antivirus Corporate Edition 10.1.5.5000 and Security Manager on the same system and observe any issues during Security Manager startup, follow this procedure:

Procedure

Step 1 Disable Symantec Antivirus services completely.

Step 2 Restart Security Manager services. (See Restarting All Processes on Your Server, page A-19.)

Step 3 Restart the set of Symantec services (Symantec Antivirus, Symantec Antivirus Definition Watcher, Symantec Settings Manager, and Symantec Event Manager) in such a way that Symantec Event Manager is started last.

Problems after Installing Windows Updates

Problems can occur with the Security Manager Daemon Manager after installing Microsoft Windows updates. The reason is that installing Windows updates may update *.dll files that affect the functionality of Common Services and other applications that depend on them.

This problem can be recognized by the following symptoms: After a Windows update, Security Manager will start all processes; however, Security Manager will be unreachable over HTTPS and therefore from the Security Manager client, which uses HTTPS.

This problem occurs because Common Services relies on files and associations within Windows. These files can be altered to correct vulnerabilities and protect Windows from exploits. However, as an unintended side effect, these changes can cause the Security Manager server to act abnormally when it is restarted.

This problem can occur any time that Windows Update, or any other application, makes changes to Windows that affect *.dll files, executables, startup processes, Windows components, or partition sizes.

To resolve this problem in cases where changes in Windows have been made and Security Manager acts abnormally when it is restarted, Security Manager must be re-installed.

Ensure that you back up your Security Manager server before running Windows Update or any other installer package.

Backup of Cisco Security Manager Server

Cisco recommends you to backup Security Manager server regularly. In particular, if regular backups have not been made, or if many changes have been made to your Security Manager installation, you should backup your Security Manager server.

Problem When you backup, either manual or scheduled, it may fail to be completed. This failure may be caused due to "INFO: File not exists.SQL " or validation failure.

Solution Modify the Cisco Security Manager Install directory as follows:

Step 1 Navigate to **CSCOpx\lib\perl\install** folder and open the **InstallUtility.pl** file for editing.

Step 2 Find the following string:

```
$InstallUtility::dbeng = "dbeng12"
```

Step 3 Replace it with the following string:

```
$InstallUtility::dbeng = "dbeng12 -ch 50%%"
```

Step 4 Restart the Cisco Security Manager server and check for automatic backups.

Problem Connecting to an ASA Device with Higher Encryption

This troubleshooting topic may help you if you are unable to add and discover an ASA device with higher encryption. In particular, if you want to use AES-256, you must download and install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files. Security Manager does not include this extension, but it does support it.

Problem The problem occurs when the certificate contains a key longer than 1024 bits. The cryptography strength limitations placed by the default policy files included with Java Runtime Environment (JRE) give the highest strength cryptography algorithms and key lengths which are allowed for import to all countries.

Solution If your country does not place restrictions on the import of cryptography, you can download the unlimited strength policy files:

Step 1 Go to http://java.sun.com/javase/downloads/index.jsp.

Step 2 Download the "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6."

Step 3 Follow the instructions in the README.txt file in the downloaded package.

Pop-up Showing Activation.jar in Use During the Time of Installation

This troubleshooting topic may help you if, during installation, a pop-up window appears with the message "Activation.jar being used by some other service."

Tip This problem is extremely rare.

Before You Begin

Any anti-virus or monitoring agent process in the server should be shut down before the installation. For more information, refer to Readiness Checklist for Installation, page 4-3.

Problem

A pop-up window appears with the message "Activation.jar being used by some other service."

Solution

Use the following procedure.

Step 1 Click OK on the pop-up and complete the installation.

Step 2 Uninstall Security Manager and restart the server.

Step 3 Install Security Manager again.

Step 4 Immediately after the start of the installation, enter “services.msc” at a command prompt and press Enter.

Step 5 When the Services menu opens, keep refreshing it until “Cisco Security Manager Daemon Manager” appears.

Step 6 Right-click CSM Daemon Manager > Properties > Startup type and then click Disabled.

Step 7 Right-click CWCS syslog service > Properties > Startup type and click Disabled.

Step 8 After the installation is complete, and at the time of server restart, change the startup type of both of the above services from “Disabled” to “Automatic” mode.

How to Set the Locale for the Windows Default User Template to U.S. English

If you normally use a non-U.S. English Windows locale, you must change the default system locale to U.S. English before installing Security Manager; changing the default system locale and rebooting the server does not change the default profile. It is not sufficient for the current user only to have the proper settings; this is because Security Manager creates a new account (“casuser”) that runs all Security Manager server processes.

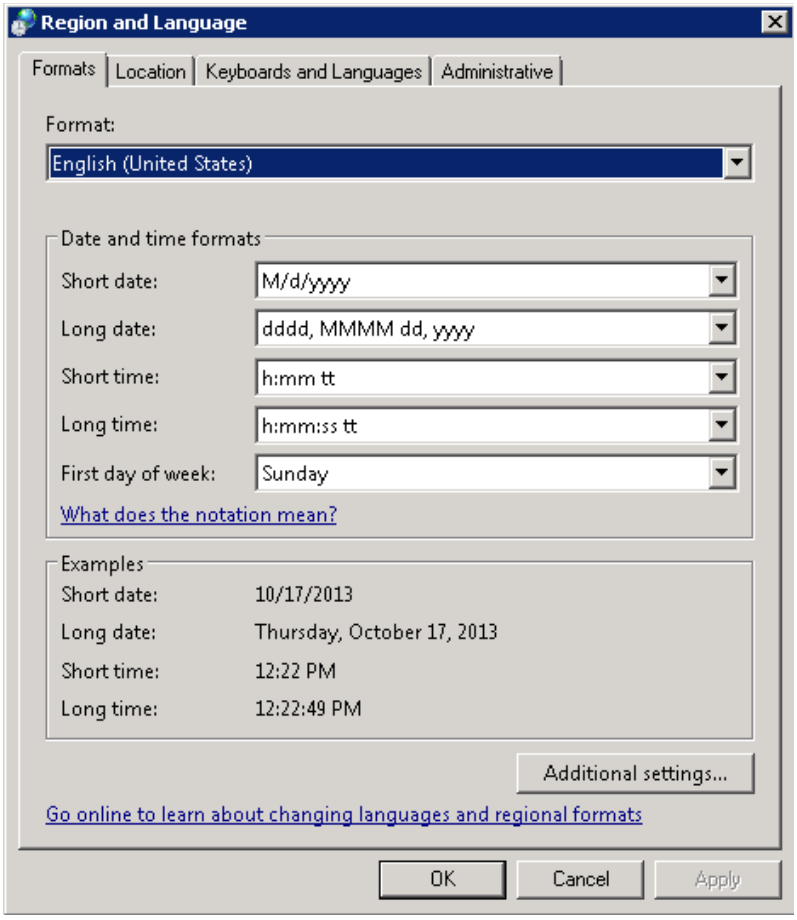
This section explains how to configure region and language settings on the Security Manager server, especially if you normally use a non-U.S. English Windows locale. The specific details apply to Microsoft Windows Server 2008 R2 with SP1 Enterprise—64-bit, but they are very similar for the other supported server operating systems, namely the following ones:

- Microsoft Windows Server 2012 Standard—64-bit
- Microsoft Windows Server 2012 Datacenter—64-bit

To ensure that all newly created users have the same settings as the current user, you need to copy the settings for the current user to new user accounts. This can be done as shown below.

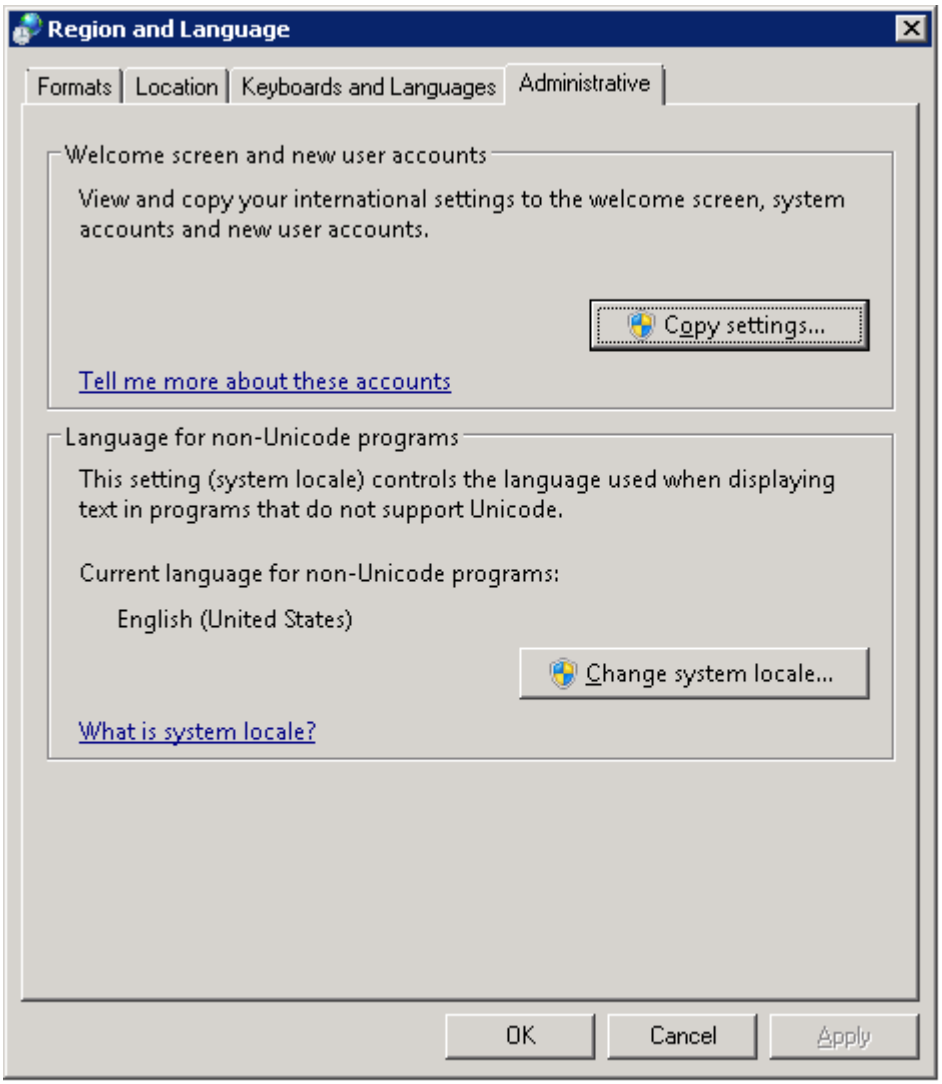
Ensure that the current user has proper U.S. English locale settingsin the Region and Language dialog box. (The navigation path to this dialog box is Start > Control Panel > Region and Language.)

Figure A-1 Windows Region and Language dialog box



Click the **Administrative** tab. Find the **Copy Settings...** button.

Figure A-2 Administrative tab



Click the **Copy settings...** button. The Welcome screen and new user account settings dialog box will appear.

Under “Copy your current settings to:” check the “New user accounts” box. This will ensure that all newly created users have the same configuration as the current settings.

Finally, install (or re-install) Cisco Security Manager server. In the new installation, the new account (“casuser”) that runs all Security Manager server processes will have a U.S. English default profile.

How to disable the RMI Registry Port

In a typical Cisco Security Manager configuration the RMI registry port is open by default. You may need to disable this in a typical Cisco Security Manager configuration. Follow the steps below, to disable the RMI Registry Port:

Problem

Disable the RMI Registry Port

Solution

Use the following procedure.

Step 1 Stop Cisco Security Manager Server.

Step 2 Export the ESS registry entry from the following Windows registry path in Cisco Security Manager Server.

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\Resource Manager\CurrentVersion\Daemons\ESS

Note This is recommended, to create a backup.

Step 3 Run the **ESS_Reg_Edit.bat** file. This file is available in Bug Search Kit (Attached in the defect CSCvc21327). The file will update the ESS registry entry by removing the JMX remote monitoring parameter in the Arguments Key.

Step 4 Locate the **activemq.xml** file at this location ~CSCOpx\objects\ess\conf\activemq.xml

Step 5 Modify the "createConnector" value as false as follows:

```
<managementContext>
        <managementContext createConnector="false"/>
 </managementContext>
```

Step 6 Save **activemq.xml**.

Step 7 Restart Cisco Security Manager.

Permissions Matrix for Image Manager

The RBAC (role-based access control) permissions matrix for Image Manager is shown in the following series of tables:

- Table B-1, Other Actions
- Table B-2, Image View
- Table B-3, Bundles View
- Table B-4, Device View
- Table B-5, Jobs View

More information on Image Manager and the views, actions, and permissions shown in these tables can be found in the *User Guide for Cisco Security Manager 4.10* at the following URL:

http://www.cisco.com/c/en/us/support/security/security-manager/products-user-guide-list.html

Table B-1 Other Actions

	Other Actions				
	Launch IM	**View Admin setting**	**Modify Admin Settings**	**View Config Archive**	**Modify Config Archive**
View Img Mgr	YES	NO	NO	NO	NO
View Admin	NO	YES	NO	NO	NO
View Devices	NO	NO	NO	NO	NO
ViewConfig Archive	NO	NO	NO	YES	NO
Modify Devices	NO	NO	NO	NO	NO
Modify Img Mgr Repository	NO	NO	NO	NO	NO
Modify admin	NO	NO	YES	NO	NO
Deploy	NO	NO	NO	NO	NO
Submit (WF) ?	NO	NO	NO	NO	NO
Approve (WF) ?	NO	NO	NO	NO	NO

Table B-2 Image View

	Image View								
	Navigate to Repository	Download Images							
		File System	CCO	Launch Install Wizard	Check Release Notes	Check for Updates	Delete from Repository	Add to Bundle	View Download Progress
View Img Mgr	YES	NO	NO	NO	YES	NO	NO	NO	YES
View Admin	NO	NO	NO	NO	NO	NO	NO	NO	NO
View Devices	NO	NO	NO	NO	NO	NO	NO	NO	NO
ViewConfig Archive	NO	NO	NO	NO	NO	NO	NO	NO	NO
Modify Devices	NO	NO	NO	YES	NO	NO	NO	NO	NO
Modify Img Mgr Repository	YES	YES	YES	NO	NO	YES	YES	YES	YES
Modify admin	NO	NO	NO	NO	NO	NO	NO	NO	NO
Deploy	NO	NO	NO	NO	NO	NO	NO	NO	NO
Submit (WF) ?	NO	NO	NO	NO	NO	NO	NO	NO	NO
Approve (WF) ?	NO	NO	NO	NO	NO	NO	NO	NO	NO

Table B-3 Bundles View

	Bundles View			
	View Bundle Names	**Check Bundle Contents**	**Modify Bundle Contents**	**Install Bundle**
View Img Mgr	YES	YES	NO	NO
View Admin	NO	NO	NO	NO
View Devices	NO	NO	NO	NO
ViewConfig Archive	NO	NO	NO	NO
Modify Devices	NO	NO	NO	NO
Modify Img Mgr Repository	YES	YES	YES	YES
Modify admin	NO	NO	NO	NO
Deploy	NO	NO	NO	NO
Submit (WF) ?	NO	NO	NO	NO
Approve (WF) ?	NO	NO	NO	NO

Table B-4 Device View

	Device View								
	View Devices and Device Groups	**View Device Inventory**	**View Device Detail Tabs - All 4**	**Delete Image from Flash**	**Download Image from Flash**	**Launch Img Install Wizard**	**Perform Image Upgrade**	**Add to Bundle**	**View Downloads**
View Img Mgr	YES	YES	YES	NO	NO	NO	NO	NO	YES
View Admin	NO	NO	NO	NO	NO	NO	NO	NO	NO
View Devices	NO	NO	NO	NO	NO	NO	NO	NO	NO
ViewConfig Archive	NO	NO	NO	NO	NO	NO	NO	NO	NO
Modify Devices	NO	NO	NO	YES	YES	YES	YES	NO	NO
Modify Img Mgr Repository	NO	NO	NO	NO	NO	NO	NO	YES	NO
Modify admin	NO	NO	NO	NO	NO	NO	NO	NO	NO
Deploy	NO	NO	NO	NO	NO	NO	NO	NO	NO
Submit (WF) ?	NO	NO	NO	NO	NO	NO	NO	NO	NO
Approve (WF) ?	NO	NO	NO	NO	NO	NO	NO	NO	NO

Table B-5 Jobs View

	Jobs View										
	Job Actions (NWF Mode)							Additional Job Options (WF Mode)			
	View jobs table and job details (all 3 tabs)	Refresh	Edit	Retry	Discard	Rollback	Abort	Approve	Reject	Submit	Deploy
View Img Mgr	YES	YES	NO	NO	NO	NO	NO	NO	NO	NO	NO
View Admin	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
View Devices	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
ViewConfig Archive	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
Modify Devices	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
Modify Img Mgr Repository	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
Modify admin	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
Deploy	NO	NO	YES	YES	YES	YES	YES	NO	NO	NO	YES
Submit (WF) ?	NO	YES	NO	NO	NO	NO	NO	NO	NO	YES	NO
Approve (WF) ?	NO	YES	NO	NO	NO	NO	NO	YES	YES	NO	NO