



Installing Management Center for Cisco Security Agents 5.2

Americas Headquarters

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

Customer Order Number: DOC-78-17916

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.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

Installing Management Center for Cisco Security Agents 5.2
Copyright © 2007 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface v

- Audience **1-v**
- Conventions **1-vi**
- Obtaining Documentation **1-vii**
 - Cisco.com **1-vii**
 - Product Documentation DVD **1-vii**
 - Ordering Documentation **1-viii**
- Documentation Feedback **1-viii**
- Cisco Product Security Overview **1-viii**
 - Reporting Security Problems in Cisco Products **1-ix**
- Product Alerts and Field Notices **1-x**
- Obtaining Technical Assistance **1-x**
 - Cisco Support Website **1-x**
 - Submitting a Service Request **1-xi**
 - Definitions of Service Request Severity **1-xii**
- Obtaining Additional Publications and Information **1-xiii**

CHAPTER 1

Preparing to Install 1-1

- How the Cisco Security Agent Works **1-1**
- Cisco Security Agent Overview **1-2**
- Before Proceeding **1-3**
- System Requirements **1-3**
- Environment Requirements **1-9**

- DNS and WINS Environments 1-9
- Browser Requirements 1-9
- Time and Date Requirements 1-10
- Port Availability 1-10
- Windows Cluster Support 1-11
- Internationalization Support 1-11
 - Internationalization Support Tables 1-12
- About CSA MC 1-17

CHAPTER 2

Deployment Planning 2-1

- Overview 2-1
- Piloting the Product 2-2
 - Running a Pilot Program 2-2
- Scalable Deployments 2-3
 - Hardware Sizing 2-3
 - Software Considerations 2-5
 - Configuration Recommendations for Scalability 2-5
 - Factors in Network Sizing 2-6
 - Factors in Database Sizing 2-7
- Policy Tuning and Troubleshooting 2-7
 - Overall Guidelines 2-7
 - Using Test Mode 2-10
 - Disabling Specific Rules 2-11
 - Caching and Resetting Query Responses 2-12
 - Setting Up Exception Rules 2-13

CHAPTER 3

Installing the Management Center for Cisco Security Agents 3-1

- Overview 3-1

Licensing Information	3-2
Installing V5.2 and Migrating Configurations and Hosts from Previous Versions	3-3
Installation and Migration Overview	3-3
Local and Remote DB Installation Overview	3-6
Installing CSA MC with a Local Database	3-8
Installing CSA MC with a Remote Database	3-21
Installing CSA MC with a Previous Version's Database (Same System Installation)	3-32
Note for installing two CSA MCs on two separate machines	3-37
Installation Log	3-38
Accessing Management Center for Cisco Security Agents	3-39
Migration Instructions	3-40
Initiating Secure Communications	3-44
Internet Explorer 7.0: Importing the Root Certificate	3-48
Uninstalling Management Center for Cisco Security Agents	3-49
Copying Cisco Trust Agent Installer Files	3-50

CHAPTER 4**Quick Start Configuration** 4-1

Overview	4-1
Access Management Center for Cisco Security Agents	4-2
Administrator Roles in CSA MC	4-3
Administrator Authentication	4-3
Cisco Security Agent Policies	4-4
Configure a Group	4-5
Build an Agent Kit	4-7
The Cisco Security Agent	4-11
View Registered Hosts	4-12
Configure a Rule Module	4-12

- Configure a Policy 4-18
 - Attach a Rule Module to a Policy 4-19
 - Attach a Policy to a Group 4-19
 - Generate Rule Programs 4-20

APPENDIX A

Cisco Security Agent Installation and Overview A-1

- Overview A-1
- Downloading and Installing A-2
 - The Cisco Security Agent User Interface A-4
- Installing the Solaris Agent A-6
- Installing the Linux Agent A-8

APPENDIX B

Third Party Copyright Notices B-1



Preface

This manual describes how to configure the Management Center for Cisco Security Agents on Microsoft Windows 2003 operating systems and the Cisco Security Agent on supported Microsoft Windows 2003, Microsoft Windows XP, Microsoft Windows 2000, Microsoft Windows NT, Sun Solaris 9, Sun Solaris 8, RedHat Enterprise Linux 4.0, and RedHat Enterprise Linux 3.0 operating systems.

In addition to the information contained in this manual, the release notes contain the latest information for this release. Note that this manual does not provide tutorial information on the use of any operating systems.

Audience

This manual is for system managers or network administrators who install, configure, and maintain Management Center for Cisco Security Agents software. Installers should be knowledgeable about networking concepts and system management and have experience installing software on Windows operating systems.

Conventions

This manual uses the following conventions.

Convention	Purpose	Example
Bold text	User interface field names and menu options.	Click the Groups option. The Groups edit page appears.
<i>Italicized</i> text	Used to <i>emphasize</i> text.	You must <i>save</i> your configuration before you can deploy your rule sets.
Keys connected by the plus sign	Keys pressed simultaneously.	Ctrl+Alt+Delete
Keys not connected by plus signs	Keys pressed sequentially.	Esc 0 2 7
Monospaced font	Text displayed at the command line.	>ping www.example.com



Tip

Identifies information to help you get the most benefit from your product.



Note

Means *reader take note*. Notes identify important information that you should reflect upon before continuing, contain helpful suggestions, or provide references to materials not contained in the document.



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage, loss of data, or a potential breach in your network security.

Obtaining Documentation

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

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

To register as a Cisco.com user, go to this URL:

<http://tools.cisco.com/RPF/register/register.do>

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

<http://www.cisco.com/en/US/support/index.html>

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

**Tip****Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended

solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

<http://www.cisco.com/offer/subscribe>

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:
<http://www.cisco.com/univercd/cc/td/doc/abtnucd/136957.htm>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>



CHAPTER 1

Preparing to Install

How the Cisco Security Agent Works

The Cisco Security Agent provides distributed security to your enterprise by deploying agents that defend against the proliferation of attacks across networks and systems. These agents operate using a set of rules provided by the Management Center for Cisco Security Agents and selectively assigned to each client node on your network by the network administrator.

This section includes the following topics.

- [Cisco Security Agent Overview, page 1-2](#)
- [Before Proceeding, page 1-3](#)
- [System Requirements, page 1-3](#)
- [Environment Requirements, page 1-9](#)
- [DNS and WINS Environments, page 1-9](#)
- [Browser Requirements, page 1-9](#)
- [Time and Date Requirements, page 1-10](#)
- [Port Availability, page 1-10](#)
- [Windows Cluster Support, page 1-11](#)
- [Internationalization Support, page 1-11](#)
- [Internationalization Support Tables, page 1-12](#)
- [About CSA MC, page 1-17](#)

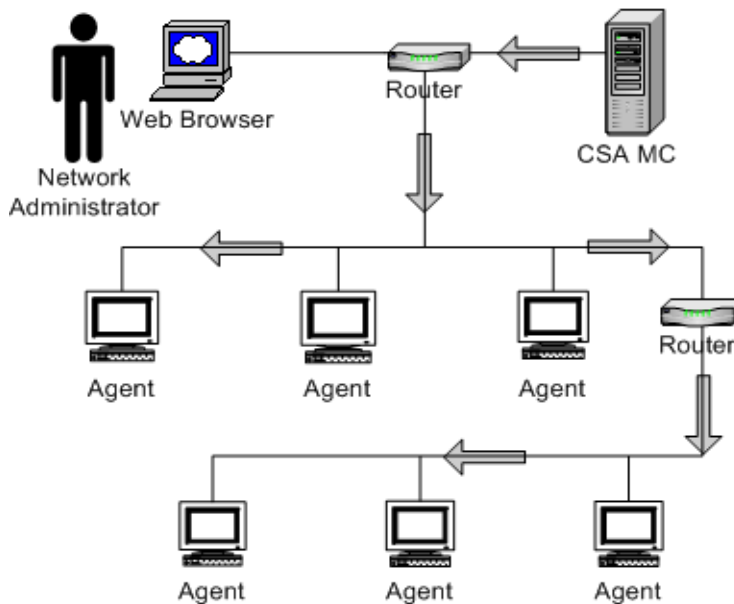
Cisco Security Agent Overview

Cisco Security Agent contains two components:

- The Management Center for Cisco Security Agents (CSA MC)- installs on a secured server and includes a web server, a configuration database, and a web-based user interface.
- The Cisco Security Agent (the agent)- installs on desktops and servers across your enterprise and enforces security policies on those systems.

Administrators configure security policies on CSA MC using the web-based interface. They distribute these policies to agents installed on end user systems and servers. Policies can allow or deny specific system actions. The agents check policies before allowing applications access to system resources.

Figure 1-1 *Product Deployment*



Before Proceeding

Before installing CSA MC software, refer to the Release Notes for up-to-date information. Not doing so can result in the misconfiguration of your system.

Make sure that your system is compatible with the Cisco product you are installing and that it has the appropriate software installed.

Read through the following information before installing the CSA MC software.

System Requirements



Note

The acronym CSA MC is used to represent the Management Center for Cisco Security Agents.

[Table 1-1](#) shows the minimum CSA MC server requirements for Windows 2003 systems. These requirements are sufficient if you are running a pilot of the product or for deployments up to 1,000 agents. If you are planning to deploy CSA MC with more than 1,000 agents, these requirements are insufficient. See [Scalable Deployments, page 2-3](#) for more detailed system requirements.

Table 1-1 Minimum Server Requirements

System Component	Requirement
Hardware	<ul style="list-style-type: none"> IBM PC-compatible computer Color monitor with video card capable of 16-bit
Processor	1 GHz or faster Pentium processor
Operating System	Windows 2003 R2 Standard or Enterprise Editions Note To run terminal services on the CSA MC system, you must edit the MC policy.
File System	NTFS
Memory	1 GB minimum memory

System Component	Requirement
Virtual Memory	2 GB virtual memory
Hard Drive Space	9 GB minimum available disk drive space

- Pager alerts require a Hayes Compatible Modem.
- For optimal viewing of the CSA MC UI, you should set your display to a resolution of 1024x768 or higher.
- On a system where CSA MC has never been installed, the CSA MC setup program first installs Microsoft SQL Server Express and the required .NET environment. If the CSA MC installation detects any other database type attached to an existing installation of Microsoft SQL Server Express, the installation will abort. This database configuration is not supported.

If you are planning to deploy no more than 1,000 agents, the shipped version of Microsoft SQL Server Express should be adequate. For a larger deployment, you also have the option of installing Microsoft SQL Server 2005 or Microsoft SQL Server 2000 instead of using the Microsoft SQL Server Express database that is provided. Note that if you are using SQL Server 2005 or 2000, it must be licensed separately and it must be installed on the system before you begin the CSA MC installation. See [Chapter 3, “Installing the Management Center for Cisco Security Agents”](#) for details.

We also recommend that you format the disk to which you are installing CSA MC as NTFS. FAT32 limits all file sizes to 4 GB.

To run the Cisco Security Agent on Windows servers and desktop systems, the requirements are as follows:

Table 1-2 Agent Requirements (Windows)

System Component	Requirement
Processor	Intel Pentium 200 MHz or higher Note Up to eight physical processors are supported.
Operating Systems	<ul style="list-style-type: none"> • Windows Server 2003 (Standard, Enterprise, Web, or Small Business Editions) Service Pack 0 or 1 • Windows XP (Professional, Tablet PC Edition 2005, or Home Edition) Service Pack 0, 1, or 2 • Windows 2000 (Professional, Server or Advanced Server) with Service Pack 0, 1, 2, 3, or 4 • Windows NT (Workstation, Server or Enterprise Server) with Service Pack 6a Note Citrix Metaframe and Citrix XP are supported. Terminal Services are supported on Windows 2003, Windows XP, and Windows 2000 (Terminal Services are not supported on Windows NT.) Supported language versions are as follows: <ul style="list-style-type: none"> • For Windows 2003, XP, and 2000, all language versions, except Arabic and Hebrew, are supported. • For Windows NT, US English is the only supported language version.
Memory	128 MB minimum—all supported Windows platforms

System Component	Requirement
Hard Drive Space	50 MB or higher Note This includes program and data.
Network	Ethernet or Dial up Note Maximum of 64 IP addresses supported on a system.

To run the Cisco Security Agent on your Solaris server systems, the requirements are as follows:

Table 1-3 Agent Requirements (Solaris)

System Component	Requirement
Processor	UltraSPARC 400 MHz or higher Note Uni-processor, dual processor, and quad processor systems are supported.
Operating Systems	Solaris 9, 64 bit, patch version 111711-11 or higher, and 111712-11 or higher installed. Solaris 8, 64 bit 12/02 Edition or higher (This corresponds to kernel Generic_108528-18 or higher.) Note If you have the minimal Sun Solaris 8 installation (Core group) on the system to which you are installing the agent, the Solaris machine will be missing certain libraries and utilities the agent requires. Before you install the agent, you must install the "SUNWlibCx" library which can be found on the Solaris 8 Software disc (1 of 2) in the /Solaris_8/Product directory. Install using the pkgadd -d . SUNWlibCx command.
Memory	256 MB minimum
Hard Drive Space	50 MB or higher Note This includes program and data.
Network	Ethernet Note Maximum of 64 IP addresses supported on a system.

**Caution**

On Solaris systems running Cisco Security Agents, if you add a new type of Ethernet interface to the system, you must reboot that system twice for the agent to detect it and apply rules to it accordingly.

To run the Cisco Security Agent on your Linux systems, the requirements are as follows:

Table 1-4 Agent Requirements (Linux)

System Component	Requirement
Processor	500 MHz or faster x86 processor (32 bits only) Note Uni-processor, dual processor, and quad processor systems are supported.
Operating Systems	RedHat Enterprise Linux 4.0 WS, ES, or AS RedHat Enterprise Linux 3.0 WS, ES, or AS
Memory	256 MB minimum
Hard Drive Space	50 MB or higher Note This includes program and data.
Network	Ethernet Note Maximum of 64 IP addresses supported on a system.

**Note**

Agent systems must be able to communicate with CSA MC over HTTPS.

**Note**

The Cisco Security Agent uses approximately 30 MB of memory. This applies to agents running on all supported Windows and UNIX platforms.

**Caution**

When upgrading or changing operating systems, uninstall the agent first. When the new operating system is in place, you can install a new agent kit. Because the agent installation examines the operating system at install time and copies components accordingly, existing agent components may not be compatible with operating system changes.

Environment Requirements

The following are recommendations for a secure setup and deployment of CSA MC.

- The system on which you are installing the CSA MC software should be placed in a physically secure, locked down location with restricted access.
- Do not install any software on the CSA MC system that is not required by the product itself.
- You must have administrator privileges on the system in question to perform the installation.
- The CSA MC system must have a static IP address or a fixed DHCP address.

DNS and WINS Environments

For agents and browsers to successfully communicate with CSA MC, the CSA MC machine name must be resolvable through DNS (Domain Name Service) or WINS (Windows Internet Naming Service).

Browser Requirements

You use a web browser to access CSA MC either locally or from a remote system. Browser requirements are as follows:

Internet Explorer:

- Version 6.0 or later

- You must have cookies enabled. This means using a maximum setting of "medium" as your Internet security setting. Locate this feature from the following menu, Tools>Internet Options. Click the Security tab.
- JavaScript must be enabled.
- If you are using Internet Explorer Version 6.0 SP1 or higher, your CSA MC FQDN cannot contain non-alphanumeric characters other than '-' and '.'. For example, if the server system name contains an underscore "_", CSA MC will not work properly.

FireFox:

- Version 1.5.0.x or higher
- You must have cookies enabled. Locate this feature from the following menu, Tools>Options>Privacy>Cookies.
- JavaScript must be enabled.

Time and Date Requirements

Before you install CSA MC, make sure that the system to which you plan install the software has the correct and current time, date, and time zone settings. If these settings are not current, you will encounter MC/agent certificate issues.

Port Availability

CSA MC acts as a web server and requires that no other web server software is running on the CSA MC system. Having multiple web servers running on the same system causes port conflicts.



Caution

By default, Windows 2003 has the World Wide Web Publishing service running. If the CSA MC installation detects this service running, the CSA MC installation will disable all Web publishing services in order for its own installation to proceed.

Windows Cluster Support

Cisco Security Agent supports Network Load Balancing and Server Cluster for Windows 2003 and 2000 Server platforms. Cluster support may require certain network permissions to operate. As with other network services, your CSA MC policies must account for these network permissions. (Component Load Balancing, and Solaris and Linux Clusters are not officially supported in this release.)

Internationalization Support

All Cisco Security Agent kits contain localized support for English, French, German, Italian, Japanese, Korean, Simplified Chinese, and Spanish language desktops. This support is automatic in each agent kit and no action is required by the administrator. The agent UI, events, and help system will appear in the language of the end user's desktop.

The following table lists CSA localized support and qualification for various OS types.

Table 1-5 CSA Localizations

Language	Operating System	Localized	Qualified
Chinese (Simplified)	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes
French	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes
German	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes
Italian	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes

Language	Operating System	Localized	Qualified
	Windows 2003	Yes	Yes
Japanese	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes
Korean	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes
Spanish	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes

Explanation of terms:

Localized: Cisco Security Agent kits contain localized support for the languages identified in [Table 1-5](#). This support is automatic in each agent kit and no action is required by the administrator. The agent UI, events, and help system will appear in the language of the end user's desktop. All localized languages are agent qualified and supported. (CSA MC is not localized.)

Qualified: The Cisco Security Agent was tested on these language platforms. Cisco security agent drivers are able to handle the local characters in file paths and registry paths. All qualified languages are supported.

Supported: The Cisco Security Agent is suitable to run on these language platforms. The localized characters are supported by all agent functions.

Refer to the following tables.

Internationalization Support Tables

The following tables detail the level of support for each localized version of Windows operating systems. **Note that support for a localized operating system is different from localized agent.** A localized operating system may be supported even though the corresponding language is not translated in the agent. In this case, the dialogs will appear in English. The tables below define the operating system support, not agent language support. Note, for Multilingual User

Interface (MUI) supported languages, installs are *always* in English (Installshield does not support MUI), and the UI/dialogs are in English unless the desktop is Chinese (Simplified), French, German, Italian, Japanese, Korean, or Spanish.

Any Windows 2000, Windows XP or Windows 2003 platforms/versions not mentioned in the tables below should be treated as not supported.

The following letter combinations are used to describe the level of support:

Table 1-6 Support Level Key

L	Agent localized, supported and qualified. (Note: L(S) – Localized and supported only)
T	Supported and qualified.
S	Supported but not qualified – Bugs will be fixed when reported by customers, but the exact configuration was not tested.
NA	Not applicable – Microsoft does not ship this combination.
NS	Not supported.

Table 1-7 Windows 2000 Support

	Professional	Server	Advanced Server
MUI	T	S	S
Arabic	NS	NA	NA
Chinese (Simplified)	L	L(S)	L(S)
Chinese (Traditional)	T	S	S
Czech	S	S	NA
Danish	T	NA	NA
Dutch	S	S	NA
English	L	L	L
Finnish	S	NA	NA
French	L	L(S)	L(S)
German	L	L(S)	L(S)

	Professional	Server	Advanced Server
Greek	S	NA	NA
Hebrew	NS	NA	NA
Hungarian	S	S	NA
Italian	L	L(S)	NA
Japanese	L	L(S)	L(S)
Korean	L	L(S)	L(S)
Norwegian	S	NA	NA
Polish	T	T	NA
Portuguese	S	S	NA
Russian	S	S	NA
Spanish	L	L(S)	L(S)
Swedish	S	S	NA
Turkish	S	S	NA

Table 1-8 Windows XP Support

	Professional	Home
Arabic	NS	NS
Chinese (Simplified)	L	L(S)
Chinese (Traditional)	T	S
Chinese (Hong Kong)	S	S
Czech	S	S
Danish	T	S
Dutch	S	S
English	L	L
Finnish	S	S
French	L	L(S)
German	L	L(S)

	Professional	Home
Greek	S	S
Hebrew	NS	NS
Hungarian	S	S
Italian	L	L(S)
Japanese	L	L(S)
Korean	L	L(S)
Norwegian	S	S
Polish	T	T
Portuguese	S	S
Russian	S	S
Spanish	L	L(S)
Swedish	S	S
Turkish	S	S

Table 1-9 Windows 2003 Support

	Standard	Web	Enterprise
Chinese (Simplified)	L	L(S)	L(S)
Chinese (Traditional)	T	S	S
Chinese (Hong Kong)	S	S	S
Czech	S	S	S
Dutch	S	NA	NA
English	L	L	L
French	L	L(S)	L(S)
German	L	L(S)	L(S)
Hungarian	S	S	S
Italian	L	L(S)	L(S)
Japanese	L	L(S)	L(S)
Korean	L	L(S)	L(S)

	Standard	Web	Enterprise
Polish	T	T	T
Portuguese	S	S	S
Russian	S	S	S
Spanish	L	L(S)	L(S)
Swedish	S	S	S
Turkish	S	S	S

On non-localized but tested and supported language platforms, the administrator is responsible for policy changes arising from directory naming variations between languages.

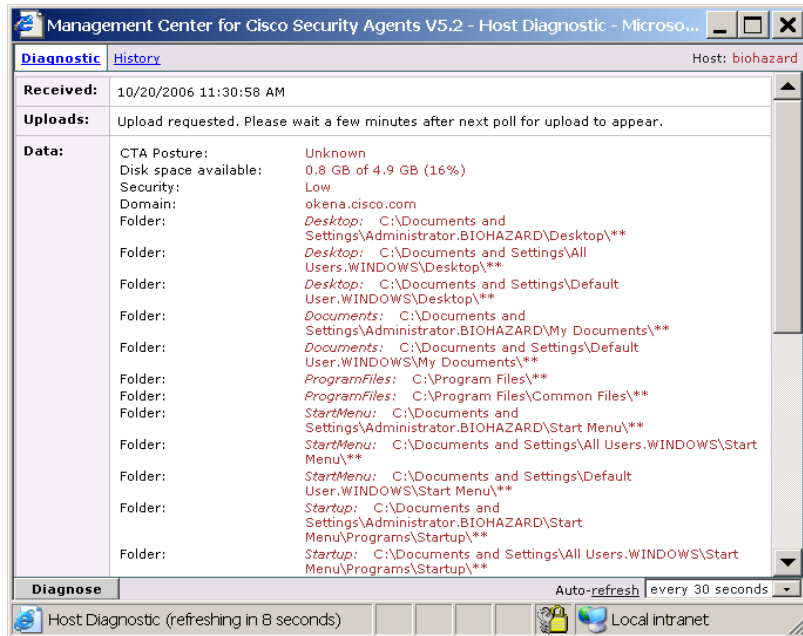
If the previous operating system tables do not indicate that CSA is localized (L) then the system administrator is responsible for checking to ensure that the tokens are in the language they expect and the directory path is the one they intend to protect.

To determine if language tokens are correct, follow this procedure:

-
- Step 1** Move your mouse over **Systems** in the menu bar and select **Hosts** from the drop-down menu.
 - Step 2** Click the link to the host name using the language you want to verify.
 - Step 3** In the Host Status area, click the **Detailed Status and Diagnostics** link.
 - Step 4** Click the **Diagnose** button.

Look at the folder information in the Data area of the Diagnosis Data page. (See [Figure 1-2](#).) These are the values of the directory tokens CSA needs for localization. Make sure that the folder paths are in the language you expect and that they protect the correct directory.

Figure 1-2 Diagnosis for Localized Host

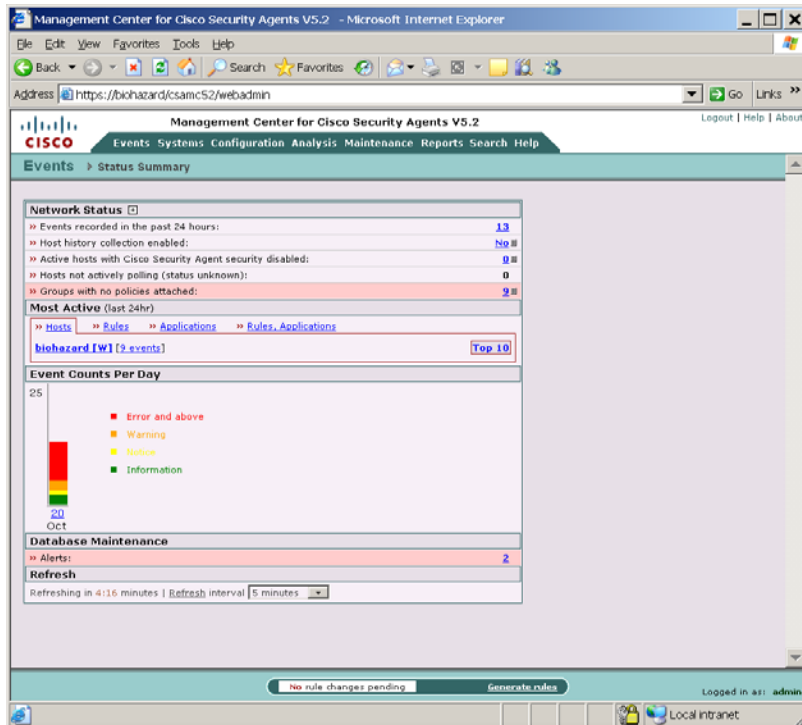


About CSA MC

The CSA MC user interface installs as part of the overall Cisco Security Agent solution installation. It is through a web-based interface that all security policies are configured and distributed to agents. CSA MC provides monitoring and reporting tools, letting you generate reports with varying views of your network enterprise health and status. Providing this web-based user interface allows an administrator to access CSA MC from any machine running a web browser.

See the User Guide for further details.

Figure 1-3 CSA MC, Top Level View





CHAPTER 2

Deployment Planning

Overview

This section provides information on deploying the product as part of pilot program and scaling the product to 100,000 agent deployments.

This section contains the following topics:

- [Piloting the Product, page 2-2](#)
- [Running a Pilot Program, page 2-2](#)
- [Scalable Deployments, page 2-3](#)
- [Hardware Sizing, page 2-3](#)
- [Software Considerations, page 2-5](#)
- [Configuration Recommendations for Scalability, page 2-5](#)
- [Factors in Network Sizing, page 2-6](#)
- [Factors in Database Sizing, page 2-7](#)
- [Policy Tuning and Troubleshooting, page 2-7](#)
- [Overall Guidelines, page 2-7](#)
- [Using Test Mode, page 2-10](#)
- [Disabling Specific Rules, page 2-11](#)
- [Caching and Resetting Query Responses, page 2-12](#)
- [Setting Up Exception Rules, page 2-13](#)

Piloting the Product

Before deploying Cisco Security Agents (CSA) on a large scale, it is critical that you run a manageable and modest initial pilot of the product. Even in a CSA upgrade situation, a pilot program is required. Due to the unique configuration of every individual enterprise, the pre-configured policies that ship with CSA will not fit every site perfectly. A certain amount of policy tuning is always necessary. This tuning is best done on a small sample of systems that are representative of the whole.

Once the pilot is operating satisfactorily, with CSA protecting systems using properly tuned policies, you can turn your pilot into a larger deployment.

The following sections provide a guideline for conducting a pilot of CSA and deploying the product on a large scale.

Running a Pilot Program

Your pilot program should proceed in the following manner:

- *How large should a pilot program be?* Select a logical, manageable, sample of systems on which agents will be installed. A good rule of thumb is to make your pilot approximately one /one-hundredth the size of what the entire deployment will be.

Details:

- If your entire deployment will be very small, be sure to pilot at least 15-20 systems.
- If your entire deployment will be very large, roll out your pilot in steps. For example, do not pilot 1,000 systems initially and all at once. Start with a smaller sample and gradually expand the pilot.

The pilot should include machines that you can access readily (either yourself or through a responsive end-user). If you will eventually be installing agents on multiple, supported operating systems, your pilot should include machines running those operating systems. Again, systems in your pilot should be representative of the whole deployment to which you intend to scale.

- *How long should a pilot program run?* Basically, the deploying and tuning of policies is an iterative process. Initially, you will have a great deal of event log noise to parse. You must examine the data coming in and edit your policies accordingly.

Details:

- Although every site is different, it would not be unusual to run a pilot program for approximately 90 days. All possible application usage should take place within the pilot time frame. It is important to note that this recommended time frame allows you to exercise applications, their deployment and usage, within an entire fiscal quarter. The idea being, every application you use and every manner in which you use it will occur during this piloting period.

Scalable Deployments

The Cisco Security Agent V5.x release offers scaling of agents to 100,000 systems. To reach this deployment number, there are recommended multi-tiered CSA MC server system hardware, CPU, and memory requirements. Please refer to the following section.

Hardware Sizing

This section provides three server configuration examples and three hardware configuration examples. The server and hardware combinations will be charted in three tables providing information on how many agents can be deployed using each server and hardware configuration combination. This should give you an idea of how to configure CSA to scale up to a 100,000 agent deployment.

For the purpose of this guide, we will use three server configuration examples.

Server Configurations:

1. Single server
2. Two servers: one server for polling and configuration, one database server
3. Three servers: one server for polling, one server for configuration, one database server

We will use the following hardware configurations.

Hardware Configurations:

1. Single processor Pentium 4 (3Ghz+) with 2 GB RAM
2. Dual processor Xeon (2.5 Ghz+) with 4 GB RAM
3. Quad processor Xeon (2.5 Ghz+) with 8 GB RAM
4. Eight-Way Xeon (2.5 Ghz+) with 8 GB RAM

The following tables approximate the number of agents you could deploy with each server configuration installed on one of four hardware configurations provided.

Table 2-1 Server Configuration 1: Single Server

Hardware Configuration	Number of Agents
Hardware Configuration 1	2,500
Hardware Configuration 2	5,000
Hardware Configuration 3	10,000
Hardware Configuration 4	20,000

Table 2-2 Server Configuration 2: Two Servers

Hardware Configuration	Number of Agents
Hardware Configuration 1	7,500
Hardware Configuration 2	15,000
Hardware Configuration 3	30,000
Hardware Configuration 4	75,000

Table 2-3 Server Configuration 3: Three Servers

Hardware Configuration	Number of Agents
Hardware Configuration 1	10,000
Hardware Configuration 2	20,000
Hardware Configuration 3	50,000
Hardware Configuration 4	100,000

Software Considerations

- CSA MC is only supported on Windows 2003 R2 Standard and Enterprise operating systems. Only Hardware Configurations 1 and 2 (referenced in previous tables) support Windows 2003 R2 Standard. Hardware Configuration 3 with 8GB RAM requires Windows 2003 R2 Enterprise to take advantage of the increased memory. Refer to the Microsoft web site product information section for details.
- To support any deployment over 1,000 agents, you should use Microsoft SQL Server 2005 in lieu of Microsoft SQL Server Express. Only Hardware Configuration 1 supports Microsoft SQL Server 2005 Workgroup or Standard editions with their 4GB RAM limitation.

**Note**

Your memory consumption needs should dictate your CSA MC operating system choice, i.e. Windows 2003 R2 Standard and Enterprise.

Configuration Recommendations for Scalability

If you intend to scale to a deployment of approximately 100,000 agents, there are some configuration recommendations you should consider.

Set Polling Interval

With 100,000 agents deployed across your enterprise, you want to ensure that no more than 20 agents are communicating with the MC approximately every second or so. Therefore, with a deployment of this size, it is recommended that you set the polling interval to no less than 1 hour. You can have some systems polling in every hour and others polling in later than that. But on average, a 1 hour or higher polling interval is appropriate. Be sure to have the polling hint functionality enabled, as well.

Use Content Engines

For large deployments, it is highly recommended that you use content engines with transparent web caching. It makes sense to direct groups of agents to different content engines in large deployment scenarios. Content engines reduce the load on the MC by caching rule downloads and software updates.

Factors in Network Sizing

You can use the following data points for computing product network usage. The following numbers average tasks based on the upper limit of a 100,000 agent deployment.

Agent and Configuration Statistics

- Number of agents: 100,000
- Polling interval: 24 hours
- Event retention: 60 days
- Event updates: 3 per agent per day

Task Size Statistics

- Hint message: 1 Kb
- Poll size: 2 Kb
- Event update size: 2.5 Kb
- Policy update size: 35 Kb
- Agent update size: 9,000 Kb
- Agent update (with CTA): 16,000 Kb
- Tracker (Product only): 100 Kb
- Tracker (Product and non-verbose network): 2,000 Kb
- Tracker (Product and verbose network): 8,000 Kb

Tracker Agent Installation Statistics

- Number of agents in Tracker (Product only) group: 1,000
- Number of agents in Tracker (Product and non-verbose network) group: 100
- Number of agents in Tracker (Product and verbose network) group: 10

Bandwidth Statistics

- Downstream from CSA MC: 1333.33 Kb/sec, continuous
- Upstream to CSA MC: 3600 Kb/sec, continuous
- Policy update (downstream): 5833.33 Kb/sec, during update timeframe
- Agent update (downstream): 2666666.67 Kb/sec, during update timeframe

- Agent update (with CTA) (downstream): 16666.67 Kb/sec, during update timeframe

As an example of how you could compute network load using the data points provided here, take 100,000 agents, each generating an average of 3 events per day, and multiply Event update size, by number of Event updates, by number of agents, per a time frame of your choosing and average out a network load.

Factors in Database Sizing

You can use the following data points for computing database sizing. The following numbers average table size based on the upper limit of a 100,000 agent deployment.

- Event table size: 11707.02 Mb
- Formatted event table: 13658.20 Mb
- Other tables: 20000 Mb
- Total database size; 45365.23 Mb

Policy Tuning and Troubleshooting

Once you have started your CSA pilot, you need to tune the policies to suit your needs and troubleshoot any problems that occur.

Overall Guidelines

This section presents some overall guidelines for tuning and troubleshooting your CSA pilot. Please read through this section carefully and consider the specific needs and requirements of your pilot before moving on to actually using the techniques. Here are the most important guidelines to follow when tuning and troubleshooting policies:

- *Never directly modify one of the supplied groups, policies, or rule modules.* If you need to change a group, policy, or rule module, make sure you *clone and rename* it first so you preserve it for use later. Modifying the supplied groups, policies, and rule modules directly makes it difficult to back out of any inadvertent mistakes.

- Use the supplied groups and if necessary define additional groups for *each distinct desktop and server type* in your network. In your pilot, you should have some participants that are using each desktop and server type so you can tune and troubleshoot all policies before deployment.

Group membership is cumulative, which can be useful in tuning and troubleshooting. For example, at the beginning of a pilot, participating hosts that are Windows desktops would be attached to the **All Windows and Desktops - All Types** groups on the **Systems -> Groups** menu. Once you have tuned the basic desktop policies, you might attach some of those hosts to the **Desktops - Remote or mobile** group. Once you are satisfied with the performance of the remote/mobile policies, you could define a new group for a specific department's applications, attach hosts to the new group, and pilot those policies.

- Start piloting all groups in *test mode* and examine the event log (**Events -> Event Log** menu) for possible tuning and troubleshooting needs before moving to enforcement mode (also known as live mode). With the current release, you can place *all policies for a group* in test mode or a *single rule module* in test mode. Therefore, as you tune and troubleshoot, you can incrementally move rule modules to enforcement mode if need be. Keep in mind when using test mode that the area under test is completely vulnerable from a security standpoint.
- Policy tuning and troubleshooting is an *iterative* process. Focus on a single policy for improvement at a time and then verify that the tuning and troubleshooting techniques did what you expected before deploying the improved policy.
- *Prioritize* the security features you want to implement with CSA policies. You can also prioritize applications and groups. By having clear priorities and working through a single policy improvement at a time, you can manage the complexity of deploying large policy sets in large networks. For example, based on priorities, you can keep a specific rule module in test mode while the rest of the rule modules in the policy are in live mode.
- Large policy sets can generate enormous numbers of log messages, so you need to use the tools provided that help *filter out* extraneous information and *isolate* the specific policy to be improved or behavior to be studied. For example, you can log only the events that result in Deny actions or create an exception rule that stops logging a specific event to reduce the overall number of log messages. In addition, host diagnostics can be used to filter rules based on the user state (that is, the user and group) the host is in, such as only

logging the behavior of the rules used by members of the Administrator group. Monitor policies can be used in clever ways to focus in on specific behavior without interrupting applications and services.

- Set up *separate agent kits* to support the different features of your pilot. For example, you might have some desktop kits that have all policies in test mode, some desktop kits with a basic set of well-tested policies in live mode plus one experimental policy in test mode, and so forth. Labelling these kits clearly will help your pilot participants download the right set of policies you want to test and give you clear feedback on areas needing improvement.

There are two general approaches to policy creation, and the approach you choose affects how you tune and troubleshoot the policies:

- Using the *supplied* Desktop and Server group policies plus a few application-specific policies. In this scenario, you attach each participating host to the following groups:
 - **<All <platform>>**
 - **Desktops - All types** or **Servers - All types**
 - A task-specific group, such as **Servers - Apache Web Servers** or **Servers - SQL Server 2000**

Then, you attach each group to the following policies:

- A **Virus Scanner** policy. CSA supplies policies for Norton, McAfee, and Trend antivirus software. If you are using a different antivirus product, you might need to use the generic Virus Scanner policy, or clone it and make modifications to suit your virus scanner application.
- An **Installation Applications** policy. CSA supplies installation software policies for Windows, Linux, and Solaris.



Note If you do not attach antivirus and installation policies to each participating group of hosts, the CSA event logs will contain a large number of false positives, making it difficult to manage the pilot.

After attaching the Desktop and Server groups, Virus Scanner policy, and Installation Application policy, you are ready to create agent kits, start the pilot, examine the event log, and stage the next policy additions. For example, if you have a prioritized list of applications to protect, start with the first on the list, use the **Analysis -> Application Behavior Investigation** tool to

understand the behavior of the application, craft a policy, place it in test mode on the pilot machines, and examine the event log. Use the techniques in the rest of this section to tune/troubleshoot that application's policy, re-examine the event log, and if you are satisfied with the result, place the application's policy in live mode on the pilot machines. You repeat these steps with each application on your prioritized list.

- Creating a completely *custom* set of policies. In this scenario, you have a team of network security experts who have assembled a detailed list of security features and studied the many supplied rule modules. The experts use the **Analysis -> Application Behavior Investigation** tool to thoroughly study the applications for which they will write rules. Then, the experts will craft custom policies by selecting the desired rule modules and rules. With this custom approach, consider conducting a small pilot of a few systems in a test lab and then expanding to a larger and more thorough pilot.

Using Test Mode

CSA policies can execute in *live mode*, where they enforce rules by denying or allowing events, or *test mode*, where they indicate in the event log what the action would have been to the given event. All entries in the event log for rules in test mode begin with the label `TESTMODE:` to make it easy to scan for events relating to rules under test. In general, you start a pilot in test mode and gradually change over to live mode as you examine the performance of each policy. You can use test mode in two different ways:

- Place *all policies for a group* in test mode.

From the **Systems->Groups** menu, you use the supplied **Systems - test mode** group, which is available for Windows, Linux, and Solaris. You attach hosts (both desktops and servers) to each appropriate test mode group. You can make one or more agent kits available for download with the test mode groups. Be sure to include “test mode” in the name of the agent kit.

When the “test mode” phase of the pilot is completed, you can unattach hosts from the test mode groups to place the hosts in live mode.

- Place *a specific rule module* in test mode.

If one of the rule modules within a policy is not behaving as expected, you can place it in test mode while still keeping the remaining rule modules in live mode. To do this, select the **Test Mode** checkbox on any **Configuration -> Rule Modules -> <platform> Rule Modules -> <module name>** page.

**Note**

When running your pilot, explain to participants the difference between test mode and live mode, clearly label whether agent kits are for test mode or live mode, and tell participants which kits to download and use during various phases of the pilot.

Test mode is *not* intended to be used indefinitely because the area under test is completely vulnerable from a security standpoint. Groups and rule modules in test mode should move to live mode in a timely fashion. Once the pilot is over, you need to carefully control which hosts if any are in test mode. You can remove the test mode kits to ensure they do not get downloaded during deployment and periodically monitor the **Systems - test mode** group to ensure that all pilot participants have migrated to live mode agent kits. You want to avoid the situation where a security hole exists after deployment because some groups or rule modules were inadvertently left in test mode.

Disabling Specific Rules

When you examine the event log with the **Events -> Event Log** menu, the description of each event references the *rule number*. If you find a consistent pattern of false positives with the same specific rule number, you can disable that rule if desired. There are two different approaches to disabling rules:

- You can disable the rule *temporarily*. At a later time, you can go back and modify the rule, set up a query with a cached response, or set up an exception rule.
- You can disable the rule *permanently* if the rule protects a resource that you don't need protected as part of your security policy.

The easiest way to disable a rule is by clicking on the rule number at the bottom of the event description in the event log. On the rule page, you click on the Enabled checkbox to uncheck it and disable the rule. Once you generate the rules, this rule will be disabled.

Caching and Resetting Query Responses

Rules can be configured with enforcement actions of allow, deny, terminate, or query the user. In some cases, there are rules that already query the user but do so repeatedly instead of caching the user's response to make it persistent. In other cases, there are rules that are generating a mix of false positives and valid enforcements in the event log and need to be modified so they query the user and cache the user's response for the false positives.

You set up a query and cache the answer with *different* MC menus:

- To set up a query, you display the rule you wish to modify by clicking on the rule number in the event log. You then select **Query User** from the action popup menu.
- To cache the response for a query, select the **Configuration -> Variables -> Query Settings** menu option, and then select the desired query from the page. Then, click on the **Enable “don't ask again” option** checkbox if it is not already checked. When users receive the query and indicate they don't want to be asked this query again, their answer is cached.



Note

One trade-off of setting up a cached query response is that users can answer the query inappropriately and then the inappropriate response becomes persistent. After setting up a cached query response, review the event log to make sure users are responding appropriately to the query. If some users give inappropriate responses, you can reset their agents and then give the users more information about responding to the query.

If a user has responded to a query inappropriately and the response is being cached, you can reset the user's cache by doing the following:

1. Select the **Systems -> Hosts** menu option.
2. Click on the `<hostname>`.
3. Select **User Query Responses** and click on the **Reset Cisco Security Agent** button.

Setting Up Exception Rules

In some cases, you need two or more different rules to completely specify the desired actions to a specific event. For example, you could have one rule that denies all applications from writing to the //blizzard/webdocs directory and another rule that allows the WebGuru application with authenticated user webmaster to write to the //blizzard/webdocs directory. The second rule allowing write access for WebGuru is considered *an exception rule* because it overrides a small part of the overall deny rule for the //blizzard/webdocs/ directory. The MC manipulates the precedence of exception rules so that they are evaluated before the rules that they override.

Although you can create exception rules with the MC rule pages, the easiest way to create exception rules is using the Event Management Wizard from the event log. The wizard tailors its behavior to the event from which you launch it. You can use the wizard to create two general types of exception rules:

- Exception rules that under certain conditions allow an event that was denied
- Exception rules that stop logging similar events

To launch the wizard:

1. Select **Events -> Event Log**.
2. Click on the **Wizard** link at the bottom of the desired event's description.

The wizard asks you questions about the following:

- Whether the exception rule applies to the user/state conditions of the triggering rule or the user/state conditions of the specific event where you launched the wizard. If you want the exception to apply to all users, you typically want the user/state conditions of the triggering rule (the default). If you want to create an exception rule only for the user specified in the event, you need to explicitly select the **specific user state conditions** radio button
- Whether the description of the proposed exception rule looks correct. Keep in mind that if you need to make some small changes to the rule, such as the applications specified, you can do so later. After the wizard finishes, you can still modify the exception rule further before saving it.
- Whether you want to put this new exception rule in a separate exception rule module (the default) or modify the rule module that triggered the event. In most cases, you want to put this in a separate exception rule module so you can preserve the supplied rule modules.

- Whether you want the exception rule based on the application specified in the event or whether you want to base it on a new application class.

After you click Finish in the wizard, the MC displays the new exception rule. At this point, you should do the following:

1. Change the **Description** field to an appropriate name.
2. Examine the details in the **when** box. If necessary, you can change these details to expand or narrow the conditions for the exception.
3. Click the **Save** button.



CHAPTER 3

Installing the Management Center for Cisco Security Agents

Overview

This chapter provides instructions for installing CSA MC. Once you have reviewed the preliminary information outlined in the previous chapter, you are ready to proceed.

It is through CSA MC that you create agent installation kits. The tools for creating agent kits are installed as part of CSA MC.

This section contains the following topics.

- [Licensing Information, page 3-2](#)
- [Installing V5.2 and Migrating Configurations and Hosts from Previous Versions, page 3-3](#)
- [Installation and Migration Overview, page 3-3](#)
- [Local and Remote DB Installation Overview, page 3-6](#)
- [Installing CSA MC with a Local Database, page 3-8](#)
- [Installing CSA MC with a Remote Database, page 3-21](#)
- [Installing CSA MC with a Previous Version's Database \(Same System Installation\), page 3-32](#)
- [Note for installing two CSA MCs on two separate machines, page 3-37](#)

- [Installation Log](#), page 3-38
- [Accessing Management Center for Cisco Security Agents](#), page 3-39
- [Migration Instructions](#), page 3-40
- [Initiating Secure Communications](#), page 3-44
- [Uninstalling Management Center for Cisco Security Agents](#), page 3-49
- [Copying Cisco Trust Agent Installer Files](#), page 3-50

Licensing Information

The Management Center for Cisco Security Agents product CD and product download contains a license key which is automatically imported during the installation and used to operate the MC itself. If you need further license keys, before deploying Cisco Security Agents, you should obtain a license key from Cisco. To receive your license key, you must use the Product Authorization Key (PAK) label affixed to the claim certificate for CSA MC located in the separate licensing envelope.

The information contained in your CSA MC license includes the number of server-agent licenses that have been allotted to you. When you receive your license from Cisco, you should copy it to the system to which you are installing CSA MC (or to a file share accessible from the CSA MC system). Then you can copy the license to the CSA MC directory in the following manner:

After installing CSA MC, to copy the license to the CSA MC directory, click **Maintenance** in the menu bar and select **License Information**. The License Information screen appears. You can browse to the license file by clicking the **Browse** button. Once the license file is located, click the **Upload** button to copy the file into the CSA MC directory.

Installing V5.2 and Migrating Configurations and Hosts from Previous Versions

If you have previous versions (V5.1, V5.0, V4.5.x or V4.0.3) of the product installed, installing Management Center for Cisco Security Agents 5.2 does not upgrade those previous versions. V5.2 configurations coexists with V5.1, but in some cases it requires that V5.0 configurations and V4.x configuration be migrated to V5.1 before then migrating to V5.2.

If you are reusing the same hardware, you must uninstall CSA MC V5.0 and VMS from your Windows 2000 system, and then you can install 5.2 on your newly installed Windows 2003 system. Then you could migrate older V5.0.x configurations and hosts to your 5.2 MC using migration tools that are provided.

The migration procedure is more straightforward if you are not reusing the same hardware. In that case, you could install Management Center for Cisco Security Agents 5.2 on the Windows 2003 system and migrate configurations and hosts from the Management Center for Cisco Security Agents 5.0 or 4.5.x or 4.0.3 on the Windows 2000 system.

And if you are running Management Center for Cisco Security Agents 5.1 on Windows 2003, the migration is quite simple.

All migration scenarios mentioned here are detailed in this chapter.

**Note**

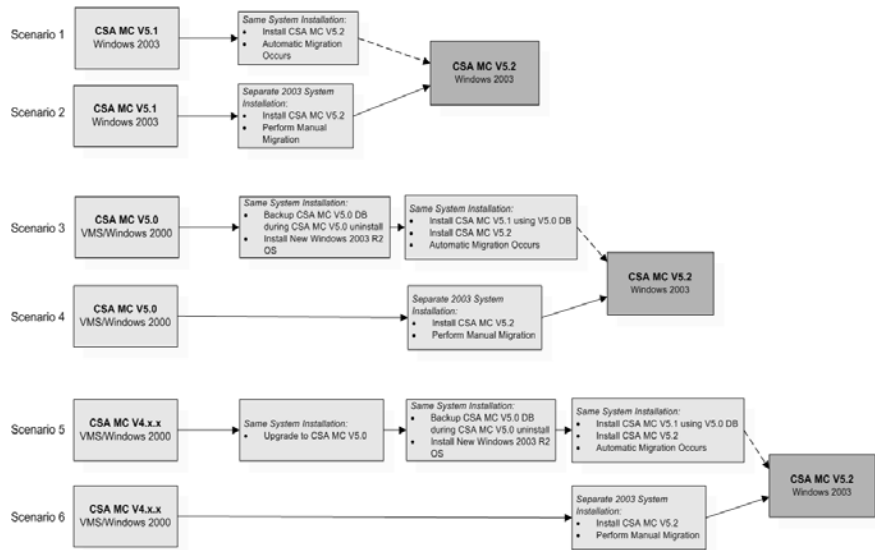
Migrating from versions of the product earlier than version 4.0.3 to version 5.2 is not supported.

Installation and Migration Overview

The following migration to CSA MC V5.2 scenarios are supported. (See [Figure 3-1](#) for a graphical representation of these upgrade path installation scenarios.)

- **Scenario 1 - Migrating V5.1 to V5.2 - Same System:** You can install V5.2 on the same machine as V5.1 and the migration is done automatically.

- **Scenario 2 - Migrating V5.1 to V5.2 - Separate Systems:** You can install V5.2 on a new machine and use the provided migration tools to move V5.1 configurations and hosts to the newly installed V5.2 system.
- **Scenario 3 - Migrating V5.0 to V5.1 to V5.2 - Same System:** You can install V5.2 on the same machine where V5.0 resided once V5.0 and VMS are uninstalled, the database is backed up safely (if local DB) and the system is running a Windows 2003 OS. Then you can use the migration tools provided to access and migrate the backed-up V5.0 database while installing 5.1 and 5.2 MCs.
- **Scenario 4 - Migrating V5.0 to V5.2 - Separate Systems:** You can install V5.2 on a new Windows 2003 system and use the provided migration tools to move V5.0 configurations and hosts to the newly installed V5.2 system.
- **Scenarios 5 and 6 - Migrating V4.5.x or 4.0.3 (4.x) to V5.2 - All:** You can install V5.2 on a new Windows 2003 system and use the provided migration tools to move V4.5.x or 4.0.3 configurations and hosts to the newly installed V5.2 system. You are running CSA MC V4.x on the same system where V5.2 will be installed. You must first upgrade to CSA MC V5.0 before you can migrate to CSA MC V5.2 using one of the previously mentioned scenarios.

Figure 3-1 Supported Migration Paths**Supported Migration Scenarios**

The CSA MC V5.2 installation does not automatically upgrade or overwrite the older installations. Ultimately, the migration process will allow you to import your older configuration items into the newly installed V5.2 system. It will also allow you to migrate hosts to V5.2. After installing V5.2, it is expected that you will spend some time examining how policies and other functionality has changed between versions and you will gradually apply the V5.2 policies to the migrated hosts.

**Caution**

For Scenario 2 in [Figure 3-1](#), you should not uninstall V5.1 until you have migrated all agents to V5.2. Once you install V5.2, you can apply hotfixes to the old V5.1 version, but you cannot install a V5.1 version of the product once the V5.0 version is installed in a one system installation scenario.

If you do apply hotfixes to an old V5.1 version after you install V5.2, you have to manually restart the CSA MC system for both MCs to begin running again.

When you install CSA MC V5.2 on the same system as V5.1, you have multiple versions to select from on the login page. The CSA MC V5.2 installation also creates a new directory structure. Refer to the following:

Directory Paths Per Version

Cisco Systems\CSAMC\CSAMC52

Cisco Systems\CSAMC\CSAMC51

CSCOpX\CSAMC50

Local and Remote DB Installation Overview

You must have local administrator privileges on the system in question to perform the CSA MC installation. Once you've verified system requirements, you can begin the installation.

**Caution**

After you install CSA MC, you should not change the name of the MC system. Changing the system name after the product installation will cause agent/CSA MC communication problems.

New Installation Configuration Options

For a new product install, you have three installation configuration options to consider before launching the CSA MC installation process.

- You can install CSA MC and the database on the same machine. (Select the **Local Database** radio button during the CSA MC installation.)

For a local database configuration, you have the option of installing CSA MC and the included Microsoft SQL Server Express Edition (provided with the product) on the same system if you are planning to deploy no more than 1,000 agents. In this case, the CSA MC installation also installs its own version of Microsoft SQL Server Express Edition on the system.

For a local database configuration, you also have the option of installing Microsoft SQL Server 2005 instead of using the Microsoft SQL Server Express Edition that is provided. Microsoft SQL Server Express Edition has a 4 GB database size limit. In this case, you can have CSA MC and Microsoft SQL Server 2005 on the same system depending on the number of agents you are deploying (see [Scalable Deployments, page 2-3](#)). Note that if you are using SQL Server 2005, it must be licensed separately and it must be installed on the system before you begin the CSA MC installation.

**Note**

If your plan is to use SQL Server 2005, it is recommended that you choose one of the other installation configuration options rather than the local database configuration.

**Note**

Microsoft SQL Server 2005 is the latest SQL Server database release. That is the database version that will be used for this installation section, but you should note that SQL Server 2000 is also supported at this time.

- You can install CSA MC on one machine and install the database on a remote machine. (Select the **Remote Database** radio button during the CSA MC installation. Note that you must install a Cisco Security Agent on this remote database to protect this system. See [Microsoft SQL Server 2005 and 2000 Remote Setup](#), page 3-22.)

Use this configuration option depending on the number of agents you are deploying (see [Scalable Deployments](#), page 2-3). If you are using a separately licensed, managed, and maintained SQL Server 2005 database, SQL Server 2005 must be installed and configured on the remote system before you begin the CSA MC installation.

**Caution**

If you are installing CSA MC and the database to multiple machines, make sure the clocks of each machine are in sync. If all clocks are not in sync, unexpected behavior may occur.

- You can install two CSA MCs on two separate machines and install the database on a remote machine. In this case, both CSA MCs use the same remote database. (Select the **Remote Database** radio button during the CSA MC installation. Note that you must install a Cisco Security Agent on this remote database to protect this system. See [Microsoft SQL Server 2005 and 2000 Remote Setup](#), page 3-22.)

This is the recommended configuration if you are deploying more than 5,000 agents and are using a separately licensed, managed, and maintained SQL Server 2005 database. SQL Server 2005 must be installed and configured on the remote system before you begin the MC installations.

Using this configuration, you can deploy up to 100,000 agents. Having two CSA MCs lets you use one MC for host registration and polling and another MC for editing configurations.

**Caution**

If you are installing two CSA MCs with one of the MCs residing on the machine where the database is installed, you must select the Remote Database radio button during the installation of both MCs. Even though one MC is “local” to the database, for the two MCs configuration to work properly, they must both be configured to communication with the database as though it were remote.

Installing CSA MC with a Local Database

If you are installing both CSA MC and the database to the same machine with the provided Microsoft SQL Server Express database, you should install Microsoft SQL Server Express Edition as part of the CSA MC installation. The CSA MC installation runs the Microsoft SQL Server Express installation program choosing the Microsoft SQL Server Express settings the MC needs. During the MC installation, if you want to install the database on a different system drive from the MC, the install prompts allow you to do this.

It is recommended that you install SQL Server Express via the CSA MC installer. If you install it manually as implied that you might do on [page 3-11](#), you should know that if you take the SQL Server Express defaults, then your subsequent CSA MC installation will fail. (See Caution below)

**Caution**

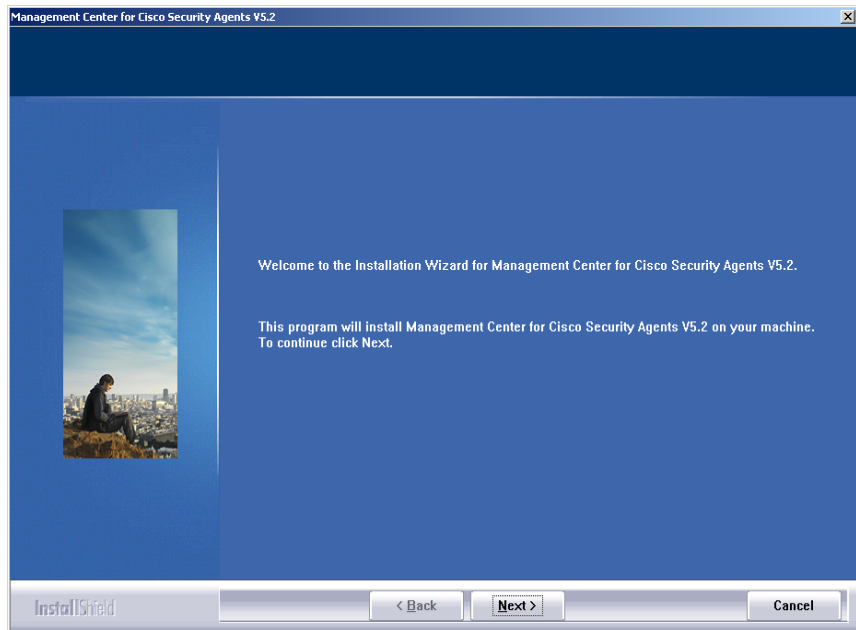
Because Microsoft SQL Server Express is provided on the CD separately, you might be tempted to install it yourself manually. This is not recommended. If you install it yourself, you must select specific non-default settings for the database to work with CSA MC. Those settings are provided in another section here, see [Microsoft SQL Server Express Manual Installation Settings, page 3-20](#). But again, this is not the recommended deployment.

Before beginning, exit any other programs you have running on the system where you are installing CSA MC.

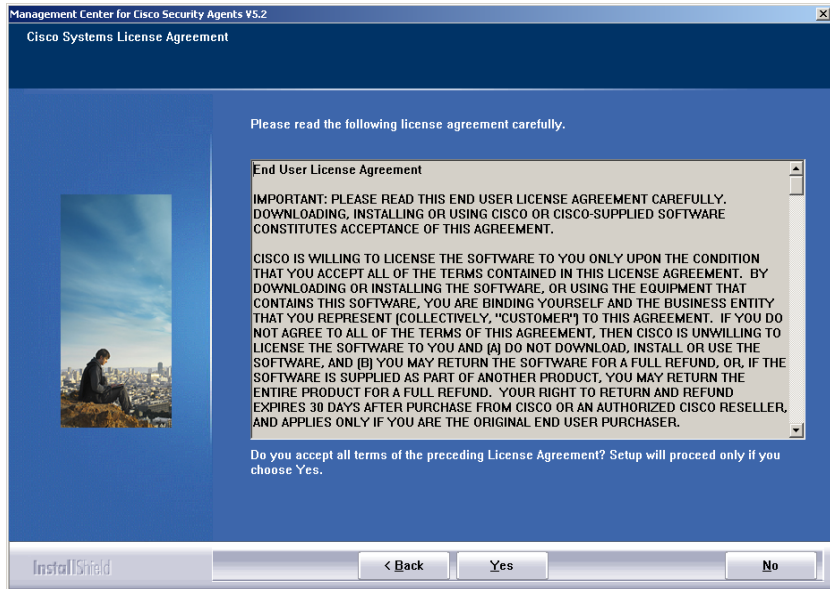
To install the CSA MC, do the following:

- Step 1** Log on as a local Administrator on your Microsoft Server Windows 2003 R2 Standard or Enterprise system.
- Step 2** Put the Management Center for Cisco Security Agents CD into the CDRom drive. The welcome screen appears. Click Next to begin the installation. See [Figure 3-2](#). (If the installation does not start automatically, browse to the setup.exe file on the CD and double click to begin the installation.)

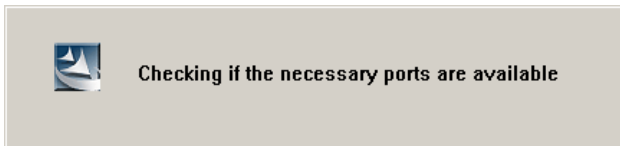
Figure 3-2 CSA MC Installation Welcome Screen



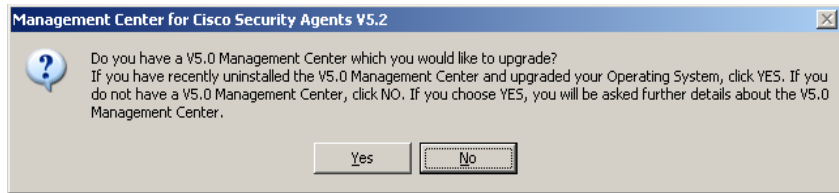
- Step 3** After you click **Next** in the welcome screen, various system checks are performed before the system installation continues.
- Step 4** When the initial system checks are complete, you are prompted to accept the license agreement. Accept the agreement by clicking **Yes**. See [Figure 3-3](#).

Figure 3-3 *CSA MC EULA License Agreement*

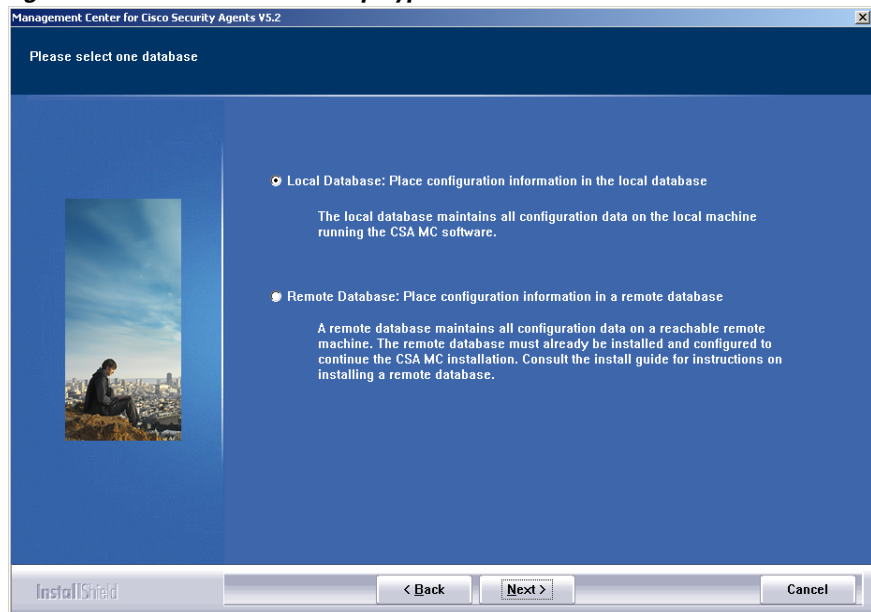
Step 5 The installation check if the needed ports are available.

Figure 3-4 *Installation Port Check*

Step 6 The installation next asks if you are upgrading from a V5.0 Management Center. In this case, click **No** to continue. See [Figure 3-5](#). (If you are upgrading from a V5.0 Management Center, click **Yes** and refer to [Installing CSA MC with a Previous Version's Database \(Same System Installation\)](#), page 3-32.)

Figure 3-5 Upgrade Question Window

Step 7 The install then begins by prompting you to select a database location. In this case, you will keep the default selection of **Local Database** and click the **Next** button. See [Figure 3-6](#).

Figure 3-6 Database Setup Type

Step 8 If installing locally, the installation next checks to see if you have Microsoft SQL Server Express Edition installed. CSA MC uses Microsoft SQL Server Express Edition for its local configuration database. If this software is not detected, you are prompted to install it. See [Figure 3-7](#).

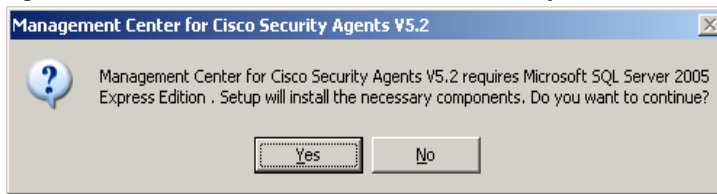


Note For installations exceeding 1,000 agents, it is recommended that you install Microsoft SQL Server 2005 instead of using the Microsoft SQL Server Microsoft SQL Server Express Edition that is provided with the product. Refer to [New Installation Configuration Options, page 3-6](#) for more information. If you are using Microsoft SQL Server 2005, refer to [Microsoft SQL Server 2005 and 2000 Local Installation Notes, page 3-19](#) for details.

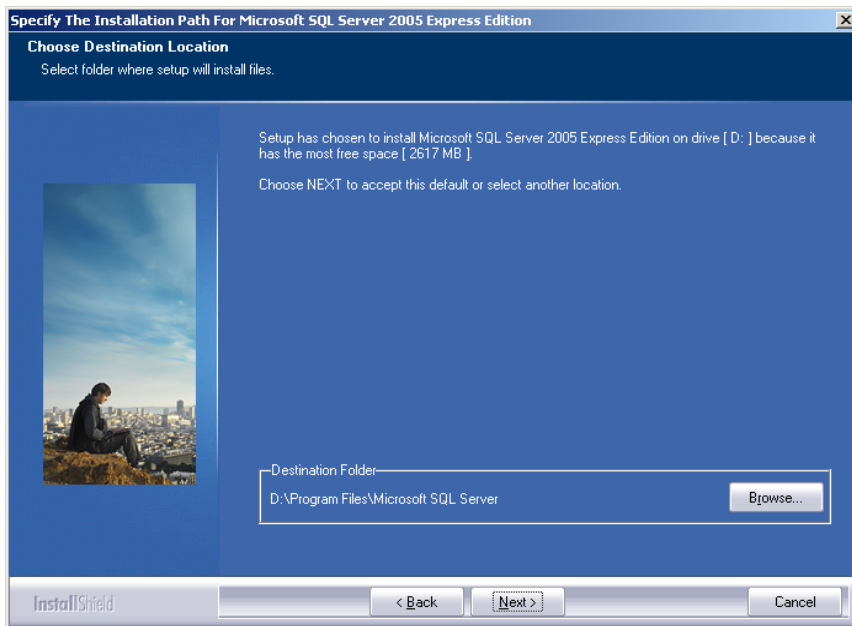
**Caution**

On a system where CSA MC has not previously been installed, the setup program first installs Microsoft SQL Server Express Edition. If the CSA MC installation detects any other database type attached to an existing installation of Microsoft SQL Server Express Edition, the installation will abort. This database configuration is not qualified.

Figure 3-7 *Install Microsoft SQL Server Express Edition Prompt*

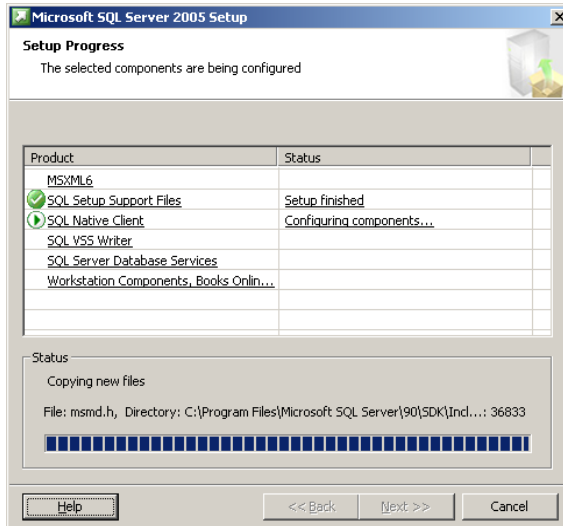


Once you click **Yes**, you proceed through the Microsoft SQL Server Express Edition installation. You are prompted to select an Microsoft SQL Server Express Edition install directory. The Microsoft SQL Server Express Edition installation only takes a few minutes.

Figure 3-8 *SQL Server Installation Directory Selection*

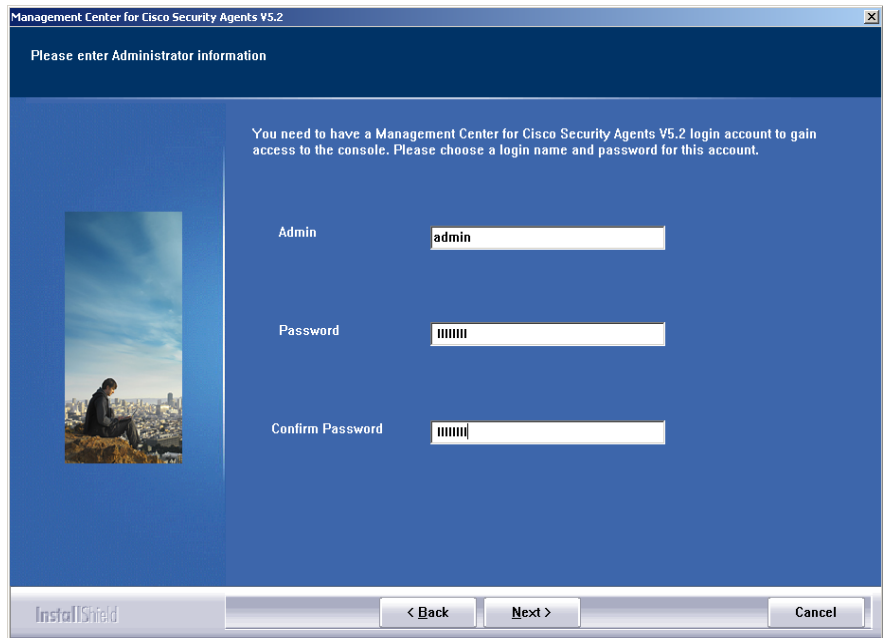
SQL Server Express Edition installs .NET Framework on the system and continues to perform configuration tasks (see [Figure 3-9](#)). The SQL Server Express Edition windows that appear require no user action.

Figure 3-9 SQL Server Express Edition Configuration Status Window

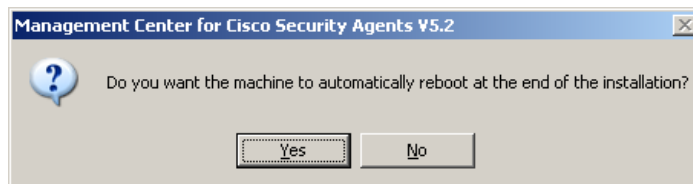
**Note**

When the Microsoft SQL Server Express Edition installation finishes, the CSA MC installation automatically begins again. This time the installation detects the Microsoft SQL Server Express Edition software and proceeds.

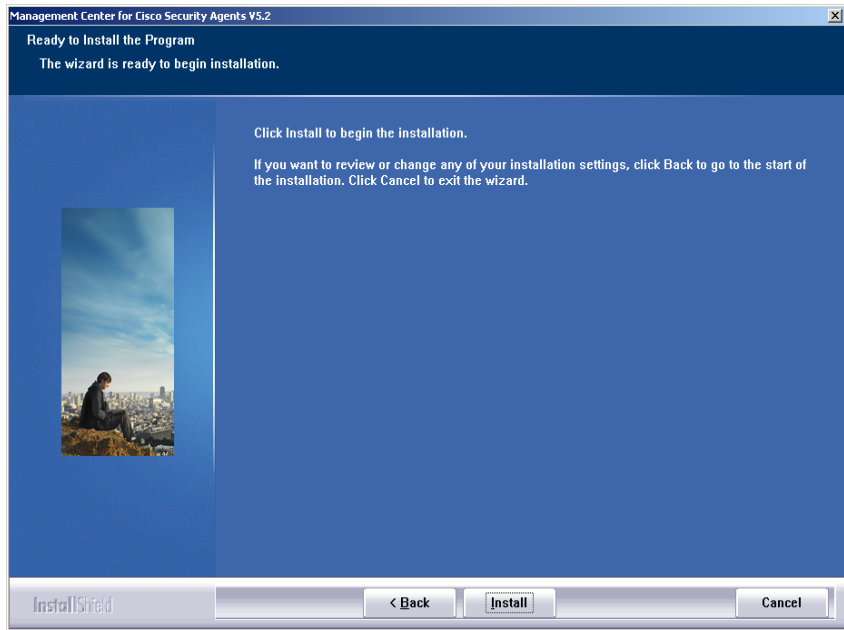
- Step 9** You are prompted to select a CSA MC directory installation path. If you would like to restore a previously backed up CSA MC database, you are prompted to restore that database at this time. Either accept the default installation path or browse to a different path to restore an database backup.
- Step 10** You are next prompted to enter Administrator Name and Password information. This the user name and password you will use to login in to CSA MC. See [Figure 3-10](#). Enter this information and click **Next**.

Figure 3-10 Enter Administrator Name and Password

- Step 11** You are next prompted to select whether or not you want the system to automatically reboot once the installation is complete (see [Figure 3-11](#)). It is required that you reboot the system after the installation is complete whether you select Yes to have it done automatically or you choose to manually reboot at the end.

Figure 3-11 Automatic Reboot Option Prompt

You are next prompted to begin the installation. Click the **Install** button (see [Figure 3-12](#)).

Figure 3-12 *Begin Install*

The install then proceeds copying the necessary files to your system. (See [Figure 3-13](#).) The installation process then continues. (See [Figure 3-14](#).)

Figure 3-13 Copy Files

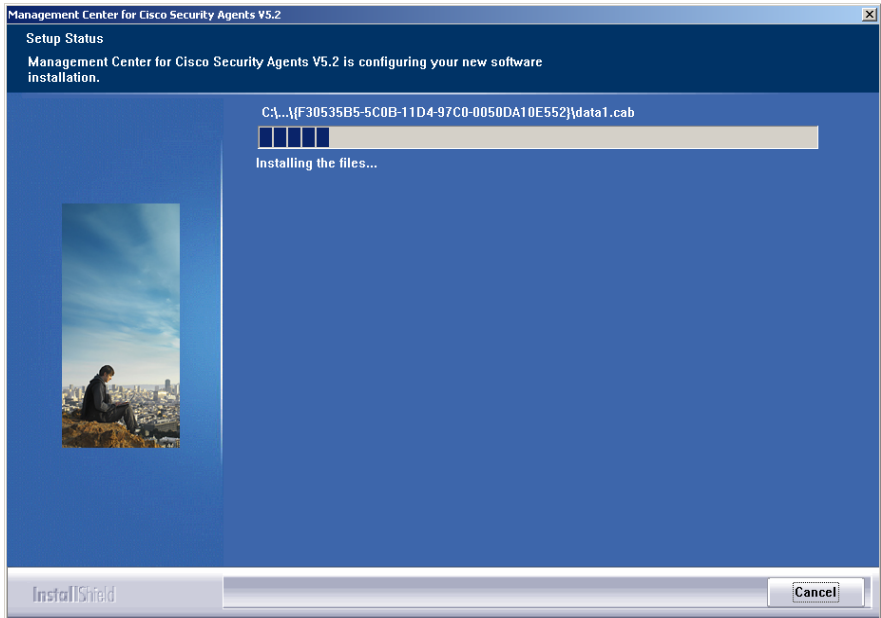
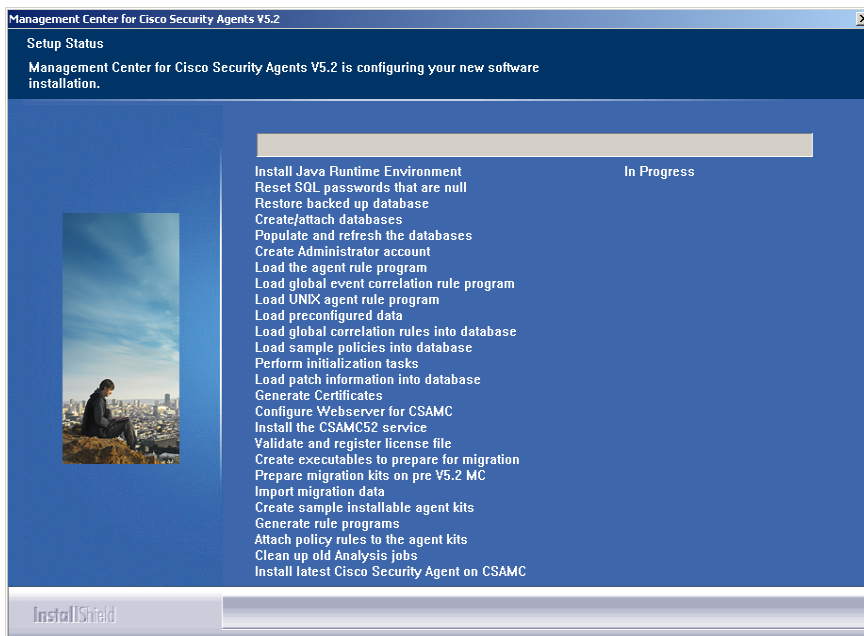


Figure 3-14 Installation Proceeds

**Note**

When the CSA MC installation completes, an agent installation automatically begins. It is recommended that an agent protect the CSA MC system. (You may uninstall the agent separately if you choose, but this is not the recommended configuration.)

If an agent is already installed on a system to which you are installing CSA MC, that agent will automatically be upgraded by the CSA MC agent installation.

When the MC and agent installs are complete, if you selected to have the system reboot automatically, you are prompted that the automatic reboot will occur within 5 minutes. If you selected not to have the system reboot automatically, it is required that you manually reboot the system at this time.

Once the system reboots, should login to the MC and copy the license key file(s) you received from Cisco Systems to your CSA MC. CSA MC ships with and automatically uses a license for the MC and local agent. You must manually import all other licenses through the MC **Maintenance>License** Information window. See the User Guide for license import instructions.

Microsoft SQL Server 2005 and 2000 Local Installation Notes

**Note**

The following instructions are only intended for administrators choosing to install CSA MC and Microsoft SQL Server 2005(or 2000) to the same system. These instructions are not for administrators using CSA MC with a remote database. If you are choosing to use Microsoft SQL Server 2005 as a remote database, information is provided in the section titled [Installing CSA MC with a Remote Database, page 3-21](#). All instructions apply to both Microsoft SQL Server 2005 and 2000 unless otherwise specified.

**Caution**

CSA MC supports Microsoft SQL Server 2005 with Service Pack 0 , Service Pack 1, or Service Pack 2. You should note that if you install a SQL Server 2005 build that is lower than build number 2153 (released after SP1), the service "SQL Server Integration Services" will fail upon system reboot. You can manually start the service or you can upgrade to Microsoft SQL Server 2005 SP1 build number 2153 or higher.

For local database installations exceeding 1,000 agents, it is recommended that you install Microsoft SQL Server 2005 instead of using the Microsoft SQL Server Express Edition that is provided with the product. Microsoft SQL Server Express Edition has a 4 GB limit. SQL Server 2005 must be licensed separately and it must be installed on the local system before you begin the CSA MC installation.

In order for Microsoft SQL Server 2005 to function properly with CSA MC, you must select certain settings during the installation. Those settings are listed here. (Refer to your Microsoft SQL Server 2005 manual for detailed installation information.)

**Note**

You should not change the default instance name of "MSSQLSERVER" for the SQL Server 2005 database. If you change this, the CSA MC installation will not detect the database.

When installing Microsoft SQL Server 2005, choose the default settings except in the following instances:

- In the **Setup Type** installation window, choose the **Typical** radio button and in the **Destination Folder** section, click the various **Browse** buttons to install SQL Server on the system.
- In the **Services Accounts** installation window, choose the **Use the same account for each service** radio button. In the **Service Settings** section, choose **Use a Domain User Account**. In the edit fields, enter a **Username** and **Password** for the local administrator account.
- (For Microsoft SQL Server 2005 only) In the **Components to Install** screen, select **SQL Server Database Services**.
- (For Microsoft SQL Server 2000 only) In the **Choose Licensing Mode** installation window, select the **Per Seat for** radio button and then increment the **devices** number field to a positive value—at least 1 or 2.

(For Microsoft SQL Server 2005 only) Reboot the system.

(For Microsoft SQL Server 2000 only) Reboot the system and install the most recent service pack for SQL Server 2000. CSA MC has been qualified with Service Pack 4. When installing the service pack, choose the default settings except in the following instances

- When you install the service pack, in the **Installation Folder** screen, you should select a drive that has at least 140 MB of free space. For the service pack installation, choose the default settings in all instances.
- In the **SA Password Warning** installation screen, select the **Ignore the security threat warning, leave the password blank** radio button.
- In the **SQL Server 2000 Service Pack Setup** installation screen, select the **Upgrade Microsoft Search and apply SQL Server 2000 SP4 (required)** checkbox.

Microsoft SQL Server Express Manual Installation Settings

Because Microsoft SQL Server Express is provided on the CD separately, during a local database MC installation, you might be tempted to install Microsoft SQL Server Express yourself manually. This is not recommended. If you install it yourself, you must select specific non-default settings for the database to work with CSA MC. Those settings are provided here. But again, this is not the recommended deployment.

**Caution**

If you are installing both CSA MC and the database to the same machine with the provided Microsoft SQL Server Express database, you should install Microsoft SQL Server Express Edition as part of the CSA MC installation. The CSA MC installation runs the Microsoft SQL Server Express installation program choosing the Microsoft SQL Server Express settings the MC needs. During the MC installation, if you want to install the database on a different system drive from the MC, the install prompts allow you to do this.

During the Microsoft SQL Server Express manual installation, you can simply leave all the default settings except in the following cases:

- **Registration information** dialog - UNCHECK the “Hide advanced configuration options” option.
- **Instance name** dialog - Choose the “Default instance” option.
- **Service Account** - Select “User the built-in system account” and from the drop down menu, select “Local System”.

Installing CSA MC with a Remote Database

If you are installing one or two CSA MCs and their corresponding database to different machines, you must first install and properly configure Microsoft SQL Server 2005 on the remote system according to Microsoft’s instructions. You should restrict access to this database machine as much as possible using any access control systems you already have in place on your network.

**Caution**

It is recommended that all installed CSA MCs and remote databases be placed on a private LAN. If you cannot provide a private LAN, then you should follow Microsoft’s recommendations for securing communication between database servers and application servers.

**Caution**

It is important that the time on the database server system closely match the time on the CSA MC system. Both systems must be in the same time zone and you should make sure both times are set correctly.

**Caution**

You must install a Cisco Security Agent on this remote database. This agent should be in the following groups: Servers-SQL Server, Servers-All types, Systems-Mission Critical, and Systems-Restricted Networking. You should install this agent after the last CSA MC has been installed and rebooted.

Microsoft SQL Server 2005 and 2000 Remote Setup

**Note**

The following section contains overview information for setting up the Microsoft SQL Server 2005 or Microsoft SQL Server 2000 database to work correctly with CSA MC. More detailed SQL Server configuration information should be obtained from your Microsoft documentation. All instructions apply to both Microsoft SQL Server 2005 and 2000 unless otherwise specified.

**Caution**

CSA MC supports Microsoft SQL Server 2005 with Service Pack 0, Service Pack 1, or Service Pack 2. You should note that if you install a SQL Server 2005 build that is lower than build number 2153 (released after SP1), the service "SQL Server Integration Services" will fail upon system reboot. You can manually start the service or you can upgrade to Microsoft SQL Server 2005 SP1 build number 2153 or higher.

In order to enter the requested remote database information during the CSA MC installation, you must first setup the SQL Server database system by doing the following. (Note that these steps may be performed by your database administrators. The procedure is detailed after the bullet list.)

- Create an empty database.
- You must configure a new login ID and password and associate it with a new user ID which has the standard access rights on the CSA MC database, including db_ddladmin, db_datareader, and db_datawriter. Note that the login ID and user ID must be identical. (db_owner privileges are not required.)

- (SQL Server 2005 - only instruction) Right-click on the server name and view Properties. On the left side of the Properties panel, click Permissions. In the table containing the logins and roles, click on the user id that has been created for CSA MC. In the explicit permissions list for the user, for the permission “View Server State”, check the box for “Grant”.
- (SQL Server 2005 - only instruction) Under the created CSA MC database, select Schema. Create a new schema with a name that is identical to the user id and login id. Click the Search button and locate the user. Attach this user to the new schema and click OK. Return to the Users in the database. Double-click the user id and select the newly created schema as the default schema.
- Make sure the default language is set to English. Note that you should not change the language default after CSA MC is installed.
- Make sure that the database is configured to accept SQL Server authentication.
- You also need to create a file group for the database called “analysis” and it must have at least one file attached.

More specifically, use the following procedure as a guideline:

-
- Step 1** Right click your SQL Server. Select the **Security** tab and set "Authentication" to **SQL Server and Windows**. Then click **OK**.
 - Step 2** Stop and start sql server.
 - Step 3** Create new database "CSAMC52".
 - Step 4** Inside the DB properties, click **Data Files** and in the **File Name** box, type "csamcanalysis", and in the **Filegroup** field type "ANALYSIS". Then click **OK**.
 - Step 5** Expand the "security" + and right-click Logins. Then create a new login. Use SQL Server Authentication. Set Defaults -> Database = csamc52 database.



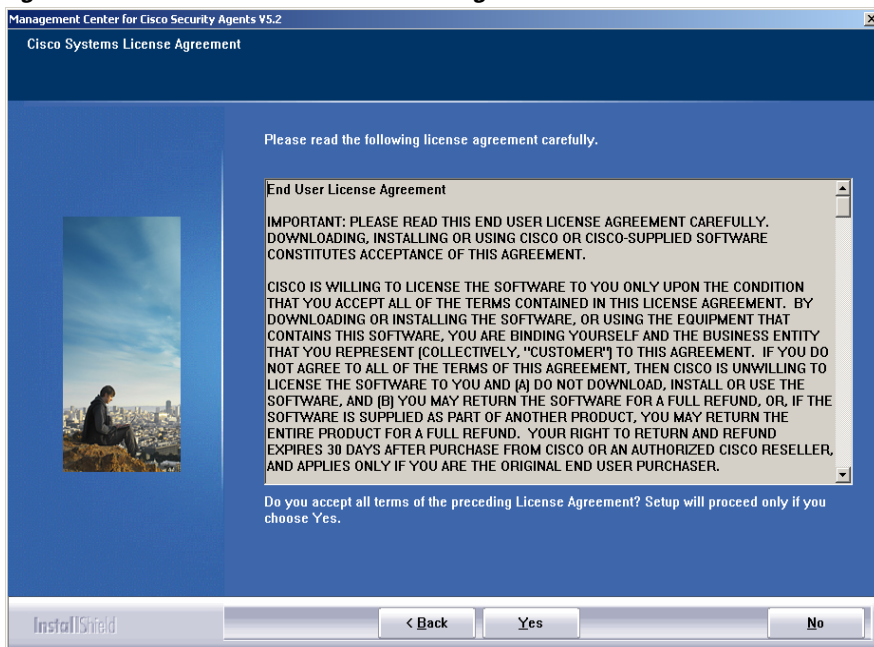
Note Do not click anything under "server roles".

- Step 6** In the "database access" section, permit access to csamc52 and give the role of db_ddladmin, db_datareader and db_datawriter permissions must also be provided. Click **OK**.
- Step 7** Restart the server.

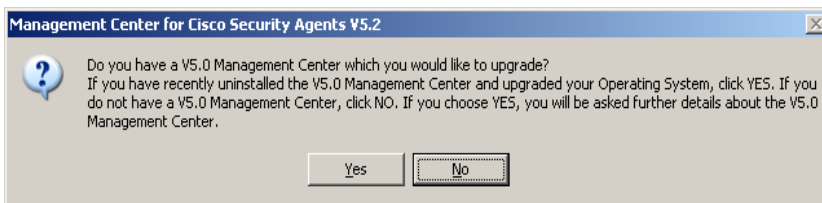
Once this is configured, you can begin the CSA MC installation.

Before beginning, exit any other programs you have running on the system where you are installing CSA MC. To install the CSA MC, do the following:

-
- Step 1** Log on as a local Administrator on your Microsoft Server Windows 2003 R2 Standard or Enterprise system.
 - Step 2** Management Center for Cisco Security Agents CD into the CDROM drive. The welcome screen appears. Click **Next** to begin the installation. (If the installation does not start automatically, browse to the setup.exe file on the CD and double click to begin the installation.)
 - Step 3** The Management Center for Cisco Security Agents appears. After you click **Next** in the welcome screen, various system checks are performed before the system installation continues.
 - Step 4** When the initial system checks are complete, you are prompted to accept the license agreement. Accept the agreement by clicking **Yes**. See [Figure 3-15](#).

Figure 3-15 *CSA MC EULA License Agreement*

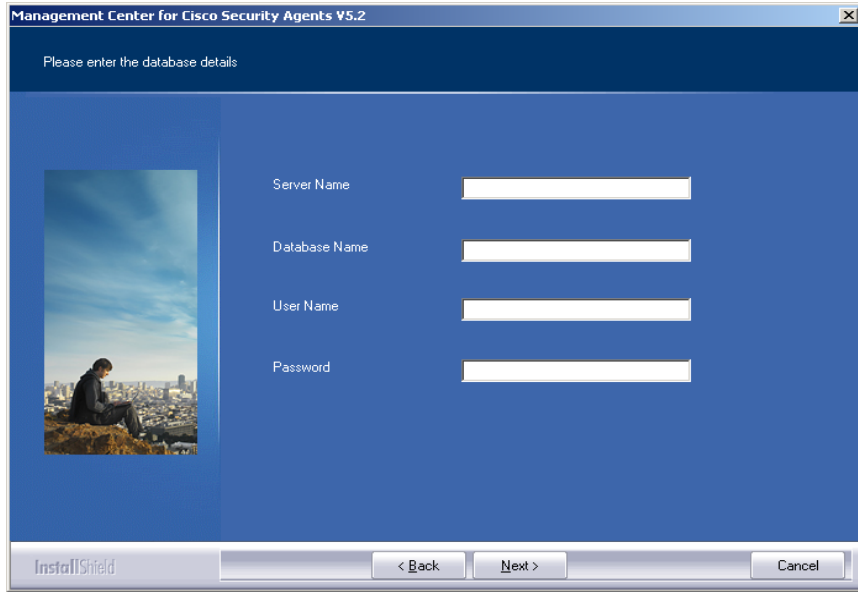
- Step 5** The installation asks if you are upgrading from a V5.0 Management Center. In this case, click **No** to continue. See [Figure 3-16](#). (If you are upgrading from a V5.0 Management Center, click **Yes** and refer to [Installing CSA MC with a Previous Version's Database \(Same System Installation\)](#), page 3-32.)

Figure 3-16 *Upgrade Question Window*

- Step 6** The install begins by prompting you to choose a database setup type. In this case, you will select the **Remote Database** radio button and click the **Next** button. When you select the Remote Database radio button, you are next prompted to enter the following information for the remote SQL Server database (see [Figure 3-17](#)):

- Name of the server
- Name of the database
- Login ID
- Password

Figure 3-17 Remote Database Information



Management Center for Cisco Security Agents V5.2

Please enter the database details

Server Name

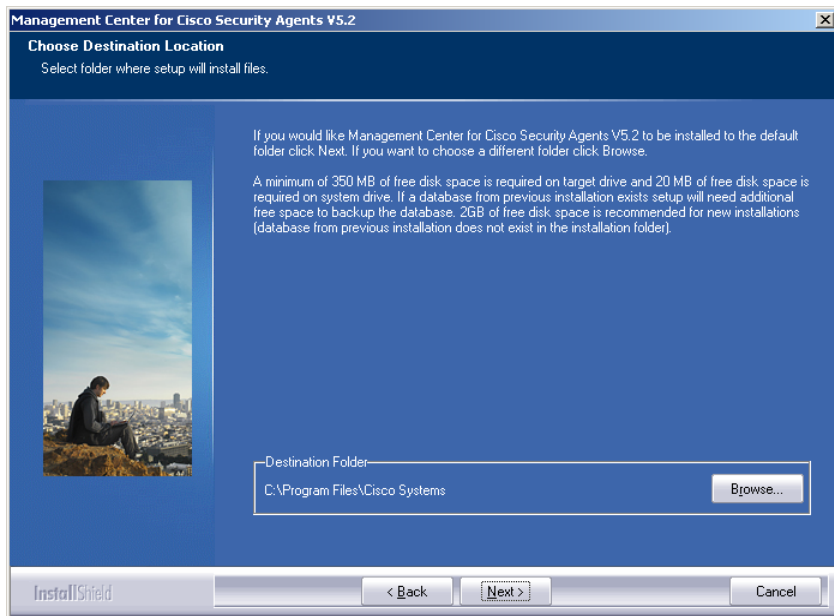
Database Name

User Name

Password

InstallShield < Back Next > Cancel

- Step 7** Once you enter the database information and click **Next**, the installation attempts to locate the database and verify that it is configured appropriately. If the database is not setup correctly, you are prompted with this information and the installation will not continue. Otherwise, the installation proceeds.
- Step 8** You are next prompted to select a CSA MC directory installation path. Either accept the default installation path or browse to a different path.

Figure 3-18 *Installation Directory*

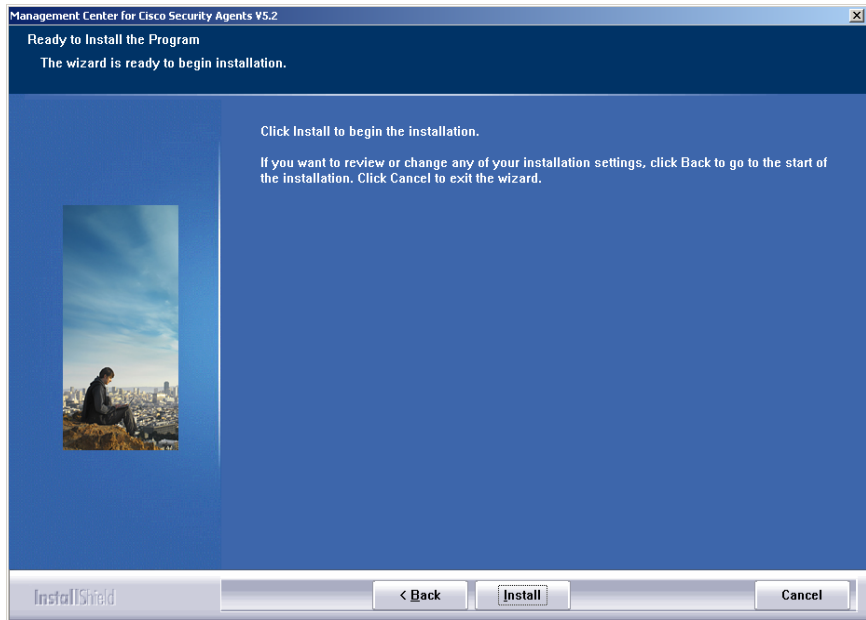
- Step 9** You are next prompted to enter Administrator Name and Password information. This the user name and password you will use to login in to CSA MC. See [Figure 3-19](#). Enter this information and click **Next**.

Figure 3-19 Enter Administrator Name and Password

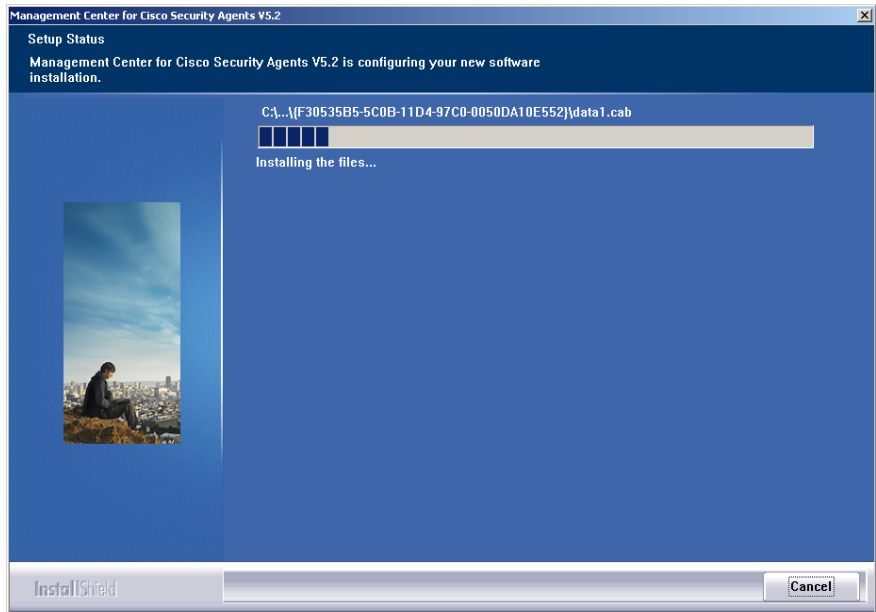
You are next prompted to select whether or not you want the system to automatically reboot once the installation is complete (see [Figure 3-20](#)). It is recommended that you reboot the system after the installation is complete whether you select **Yes** to have it done automatically or you choose to manually reboot at the end.

Figure 3-20 Automatic Reboot Option Prompt

You are next prompted to begin the installation. Click the **Install** button. (See [Figure 3-21](#).)

Figure 3-21 *Begin Install*

The install then proceeds copying the necessary files to your system (see [Figure 3-22](#)).

Figure 3-22 Copy Files

Once the copying is complete, the installation begins configuration and setup tasks. See [Figure 3-23](#).

Figure 3-23 *Installation Proceeds***Note**

When the CSA MC installation completes, an agent installation automatically begins. It is recommended that an agent protect the CSA MC system and this is done automatically for you. (You may uninstall the agent separately if you choose, but this is not the recommended configuration.)

When the MC and agent installs are complete, if you selected to have the system reboot automatically, you are prompted that the automatic reboot will occur within 5 minutes. If you selected not to have the system reboot automatically, it is recommended that you manually reboot the system at this time.

Once the system reboots, should login to the MC and copy the license key file(s) you received from Cisco Systems to your CSA MC. CSA MC ships with and automatically uses a license for the MC and local agent. You must manually import all other licenses through the MC **Maintenance>License** Information window. See the User Guide for license import instructions.

Installing CSA MC with a Previous Version's Database (Same System Installation)

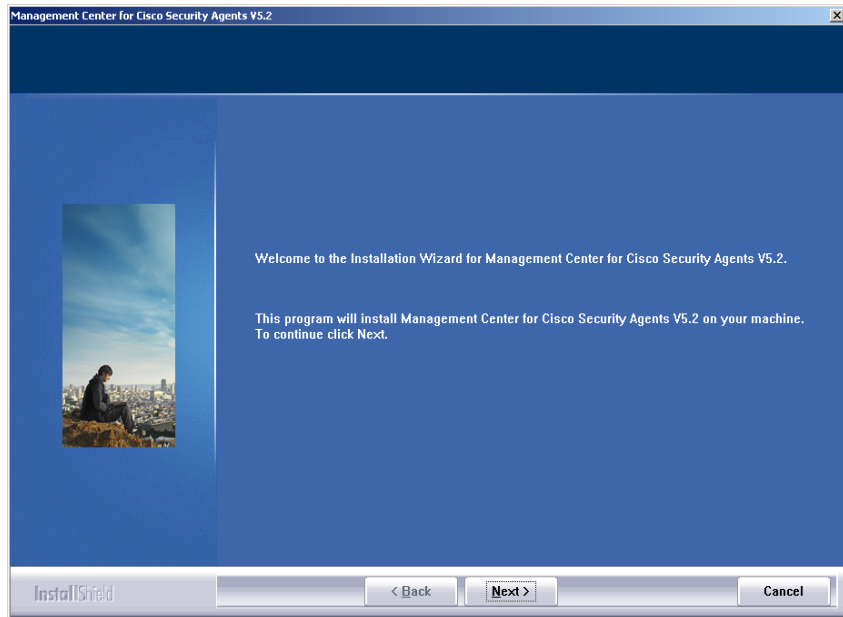
This section addresses the procedure for backing up and importing a 5.0 database as part of CSA MC V5.2. same system installation. (Scenarios 3 and 5 in [Figure 3-1](#)).

In order to perform this type of migration you must install a V5.1 MC along with the V5.2 MC. You must use V5.1 to migrate your V5.0 hosts and data to the V5.2 product schema. V5.1 is provided as an interim tool for bringing all your data into V5.2 correctly. The V5.2 installation installs both MCs, first 5.1 and then 5.2, with one reboot at the end.

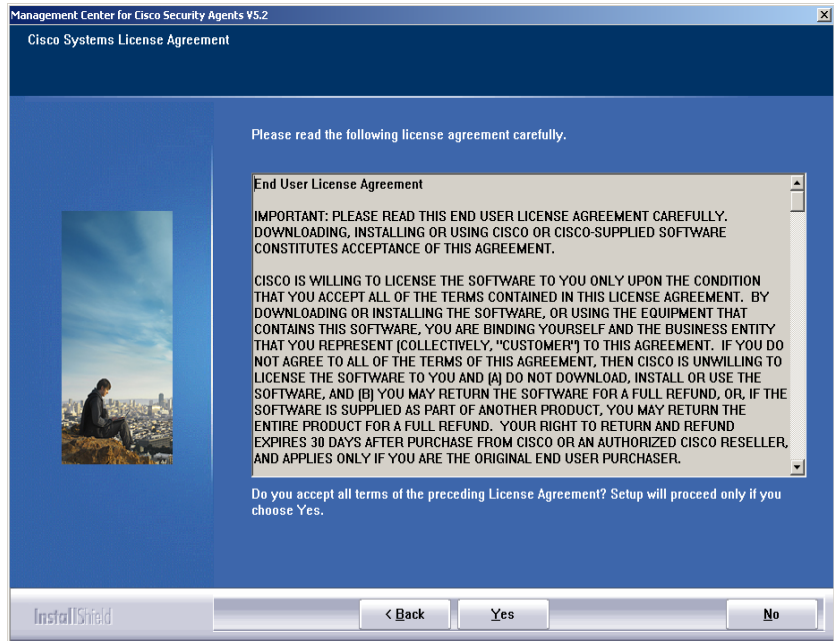


Note If you are migrating from CSA MC V4.x in a same system installation scenario, you must first upgrade to CSA MC V5.0. Refer to the CSA MC V5.0 Installation Guide for that procedure. Once you've completed that upgrade, you can use the following procedure.

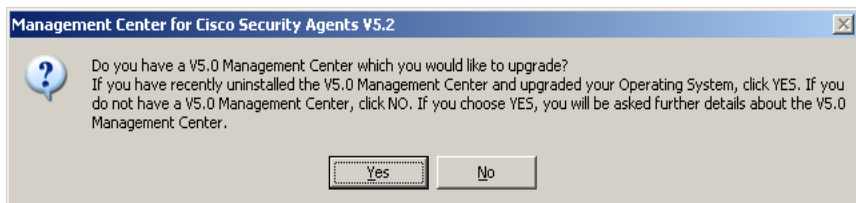
-
- Step 1** Uninstall CSA MCV5.0 per the instructions in your CSA MC V5.0 Installation Guide. (If V5.0 uses a local database, during the CSA MC V5.0 uninstall procedure, when prompted, make sure to select to backup the database. When the uninstall completes, move the backed-up database to a different, network accessible system.)
 - Step 2** Re-install that same system with the Windows 2003 R2 operating system.
Install CSA MC V5.2 as follows:
 - Step 3** Log on as a local Administrator on your Microsoft Server Windows 2003 R2 Standard or Enterprise system.
 - Step 4** Place the Management Center for Cisco Security Agents CD into the CDROM drive. The welcome screen appears. Click Next to begin the installation. See [Figure 3-24](#). (If the installation does not start automatically, browse to the setup.exe file on the CD and double click to begin the installation.)

Figure 3-24 *CSA MC Installation Welcome Screen*

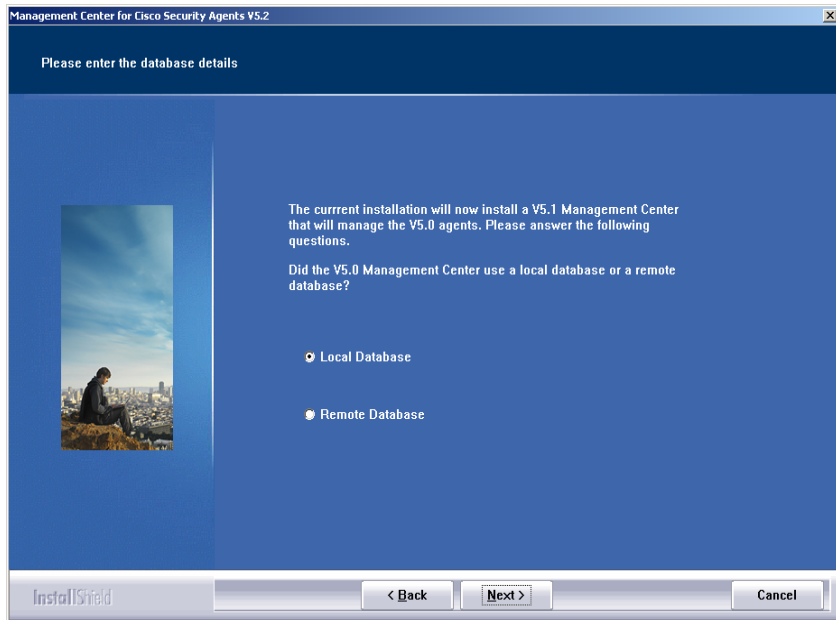
- Step 5** After you click **Next** in the welcome screen, various system checks are performed before the system installation continues.
- Step 6** When the initial system checks are complete, you are prompted to accept the license agreement. Accept the agreement by clicking **Yes**. See [Figure 3-25](#).

Figure 3-25 CSA MC EULA License Agreement

Step 7 The installation asks if you are upgrading from a V5.0 Management Center. In this case, click **Yes** to continue. See [Figure 3-26](#).

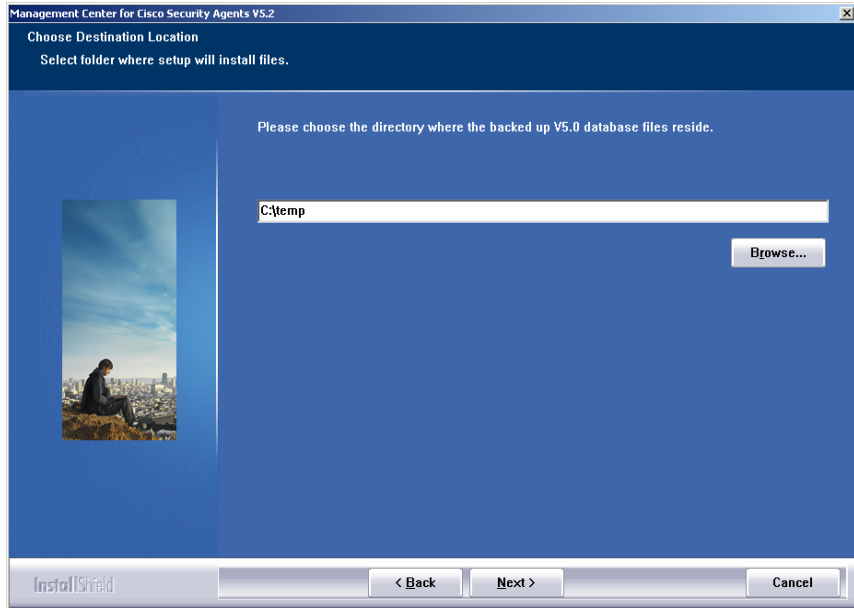
Figure 3-26 Upgrade Question Window

Step 8 Select whether your V5.0 installation used a local or a remote database. See [Figure 3-27](#).

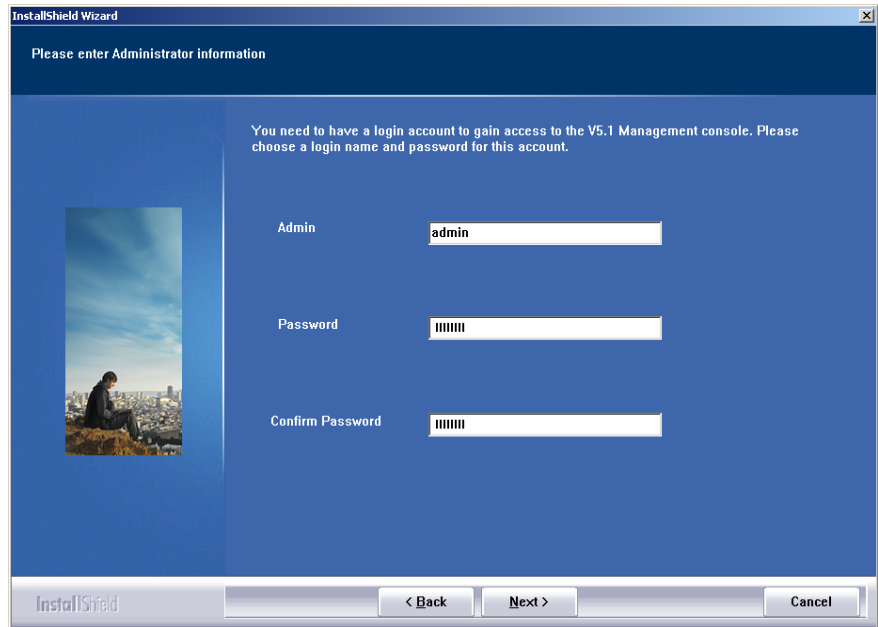
Figure 3-27 *Select V5.0 Database Type*

Step 9 If you select Local Database, you are next asked to browse to the location of the backed-up V5.0 database. Once you've located the database, click **Next** to continue. See [Figure 3-28](#).

If you select Remote Database, you are asked to enter data for accessing the remote database. This remote database entry screen is the same as [Figure 3-17](#).

Figure 3-28 Browse to Backed-up V5.0 Database

- Step 10** Once the V5.0 local or remote database is located, the installation will proceed to install CSA MC V5.1.
- Step 11** You must create a user name and password to login into the CSA MC V5.1. See [Figure 3-29](#). (You will later create another user and password for CSA MC V5.2).

Figure 3-29 Username and Password Creation for V5.1

The screenshot shows the 'InstallShield Wizard' window with the title 'Please enter Administrator information'. The main text reads: 'You need to have a login account to gain access to the V5.1 Management console. Please choose a login name and password for this account.' On the left, there is a small image of a person sitting on a hill overlooking a city. On the right, there are three input fields: 'Admin' with the value 'admin', 'Password' with masked characters '|||||||', and 'Confirm Password' with masked characters '|||||||'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

From here, you can continue by following the procedures detailed in [Installing CSA MC with a Local Database, page 3-8](#) or [Installing CSA MC with a Remote Database, page 3-21](#) depending on how you are installing the product. As stated earlier, the installation will proceed by first installing V5.1 and then directly begin the V5.2 installation with one reboot at the end of the procedure. For both V5.1. and V5.2 installations, you must select a database type and setup usernames and passwords as explained in the procedures referenced above.

Note for installing two CSA MCs on two separate machines

If you are installing two CSA MCs using one remote database, repeat the steps detailed in this section, entering the same remote database information for the second MC.

**Caution**

When installing two CSA MCs, the first MC you install automatically becomes the polling and logging MC. The second MC acts as the configuration MC. During the installation process, the CSA MCs know the order in which the MCs were installed and direct polling, logging, and management tasks to the appropriate MC.

**Caution**

In a distributed MC environment, when installing, upgrading, or uninstalling any MC in the distributed configuration, the service must be stopped on the other MCs and restarted later.

Installation Log

The installation of CSA MC produces a log file. This log file, called "CSAMC-Install.log" and located in the \CSAMC52\log directory, provides a detailed list of installation tasks that were performed. If there is a problem with the installation, this text file should provide information on what task failed during the install.

**Note**

The installation of the agent produces a similar file called "CSAgent-Install.log" and is located in the Cisco Systems\CSAgent\log directory on agent host systems.

Accessing Management Center for Cisco Security Agents

When the installation has completed and you've rebooted the system, a Management Center for Cisco Security Agents [version number] shortcut icon is placed on your desktop. Double-clicking this icon launches the MC in your default browser.

Local Access

To access CSA MC locally on the system hosting the CSA MC software:

- Double-click the shortcut icon added to your desktop during the installation. This launches the management console login screen in your default browser.

**Note**

See [Initiating Secure Communications, page 3-44](#) if you cannot connect to CSA MC.

Remote Access

To access CSA MC from a remote location,

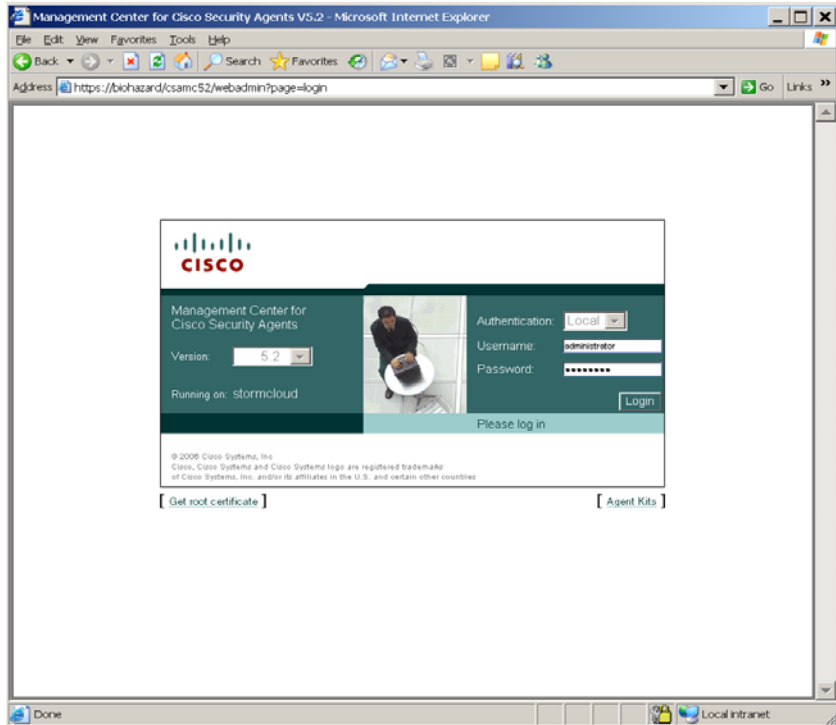
- Launch a browser application on the remote host and enter the following:
`http://<management center system hostname>.<domain>`
in the Address or Location field (depending on the browser you're using) to access the Login view.

For example, enter `http://stormcenter.cisco.com`

**Note**

In this example, CSA MC is installed on a host system with the name `stormcenter`.

Figure 3-30 CSA MC Login Window



Migration Instructions

The following section contains information for migrating to CSA MC V5.2 from a previous version installed on the same system as CSA MC V5.2 and for a previous version installed on a separate machine. Both scenarios are covered here.



Note

If you install 5.2 on the same system where you have 5.1 installed, the majority of this migration is done automatically.

If you intend to migrate 5.1 Solaris agents, please read [Solaris and Linux Agent Migration, page 3-43](#) before starting your upgrade.

To migrate to V5.2, do the following:

-
- Step 1** Install the Management Center for Cisco Security Agents V5.2. See previous sections for instructions.
- If you're installing CSA MC V5.2 on the same machine running CSA MC V5.1, an xml file containing V5.1 configuration items and several .dat files containing host information are automatically generated by the installation and ready for importing once the install is complete.
 - If you're installing CSA MC V5.2 on a different machine from the system running V5.x or V4.x, after installing V5.2, you must copy and manually run an executable file on the V5.x or V4.x machine to create the xml and dat files needed for importing V5.x or V4.x configurations and host information to V5.2.
- Step 2** If you have installed V5.2 on the same machine as V5.1, you can skip to the end of Step 6. Otherwise, once you've installed CSA MC V5.2 and rebooted the system, navigate to the CSCOPx\CSAMC52\migration directory. Copy the appropriate file (named `prepare_<version>_migration.exe` depending on the version you're migrating from, for example `prepare_50_migration.exe`) to your V5.x or V4.x system. (You can copy it to any place on the system.)
- Step 3** On your V5.x or V4.x system, disable agent security and run the `prepare_<version>_migration.exe` file that you copied from the V5.2 system. (You must disable security in order to run the executable file and create the import xml data.) This launches a command prompt which displays the progress of the migration.
- Step 4** When the `prepare_<version>_migration.exe` file is finished, on the V5.x or V4.x system, navigate to the Cisco Systems\CSAMC\CSAMC51\migration\export or CSCOPx\CSAMC50\migration\export directory (again, directory name depends on the version you're migrating from) and locate several newly created files. Your configuration data is now in a file named `migration_data_export.xml`. Your host data (hosts and distinct host groupings) are now in several files, depending on how many distinct host groupings existed, named `migration_host_data<number>.dat`.
- Using the data that is now wrapped up in these files allows you to import your existing policy configurations and your current host groupings, thereby preserving the policy tuning and host group configurations for your new V5.2 installation.

- Step 5** Next you copy the `migration_data_export.xml` and all the `migration_host_data<number>.dat` files from the V5.x or V4.x system to your V5.2 system. These files must exist together in the same directory on the V5.2 system (although the directory name and location does not matter).
- Step 6** Then from the V5.2 system, run the `webmgr import` utility from a command prompt to pull the data into the new MC. You cannot use the CSA MC UI Import utility to do this. That utility does not allow you to import the .dat files that are associated with the .xml file as one grouping.

From a command prompt window on the V5.2 system, `cd` to the `Cisco Systems\CSAMC\CSAMC52\bin` directory and run the following:

```
%system%Cisco Systems\CSAMC\CSAMC52\bin>webmgr import  
%path_to_xml_file%\migration_data_export.xml
```

Because the host .dat files are associated with the .xml file, this command imports both the configuration and host data with the `migration_data_export.xml` file.

- Step 7** You must generate rules once the import is complete. If you do not generate rules at this point, you cannot upgrade agent host software as described in the next section.

**Note**

CSA MC V5.2 ships with policies that contain new V5.2 functionality. This new functionality does not match all V5.x or V4.x configurations. CSA MC configuration item names are labeled with the release version number to distinguish them from older (or newer) configuration items or items created by administrators. When you import your older configuration, new V5.2 items are not overwritten. You will likely have items from both versions in your CSA MC V5.2. If the import process finds that two items have the exact same contents and the only difference is the V5.2 appended name field, the older item is not imported and the newer V5.2 item is used in its place.

- Step 8** To upgrade migrated V5.x or V4.x agents to V5.2, schedule V5.2 software updates for older agents. You schedule this upgrade from the V5.x or V4.x system. (Running the `prepare_<version>_migration.exe` file placed a V5.2 software update on the V5.x or V4.x machine.)

Once the older agents receive the scheduled software update, they will point to and register with the new CSA MC V5.2. The update contains the appropriate new certificates to allow this to occur. Once hosts register with V5.2, they will be associated with the correct groups based on the host migration that you performed earlier.

**Note**

Agent kits are configuration items that do not migrate to the new version. Because host migration does not relate to agent kits, old agents kits are not considered to be necessary migration items.

Also, configuration items that are not used (not attached to anything) do not migrate to the new version.

**Caution**

When upgrading V5.x or V4.x agents to software version 5.2, the upgrade program disables the system network interfaces to ensure a secure upgrade process. The agent service is also stopped to allow the update to occur. Once the update is complete, the agent service is restarted and the network interfaces are enabled. (Note, that secure upgrades are not supported for Windows NT systems.)

Once you have migrated all old agents to the newer version, you can uninstall the old version of CSA MC. See [Uninstalling Management Center for Cisco Security Agents, page 3-49](#).

Solaris and Linux Agent Migration

**Caution**

Solaris agent versions 4.0.3.736 and any 4.5 or 4.5.1 can be upgraded to version 5.2. Earlier Solaris agents cannot be upgraded.

Only Linux agent version 4.5.1.638 and above can be upgraded to version 5.2. Earlier Linux agents cannot be upgraded.

You should note that the Solaris host migration process is a bit different than Windows and Linux migration.

Once scheduled, Solaris software upgrades must be launched manually by accessing the **csactl** command line tool on the Solaris systems and typing in the software update command. When the update is complete, network connectivity is disabled and remains disabled until the system automatically reboots within 5 minutes. This reboot *cannot* be stopped. Therefore, once you launch the Solaris software update, you must understand that the system will reboot when the update completes.

Upgrade Note

Newer versions of policies are not automatically attached to the auto-enrollment groups during upgrade. If you want to update the mandatory policies, you can use the CSA MC Compare tool to synchronize the existing auto-enrollment groups with the new updated auto-enrollment groups added by the upgrade.

Initiating Secure Communications

CSA MC uses SSL to secure all communications between the CSA MC user interface (locally and remotely) and the Management Center for Cisco Security Agents server system itself. This way, all configuration data travels over secure channels irrespective of the location of the CSA MC host system.

During installation, CSA MC generates private and public keys to be used for secure communications between any system accessing the CSA MC user interface and the CSA MC itself.

When your browser connects to the server, it receives the server's certificate. You are then prompted to accept this certificate. It is recommended that you import it into your local certificate database so that you are not prompted to accept the certificate each time you login. The following sections show the process of importing certificates into Internet Explorer and Netscape Web browsers.

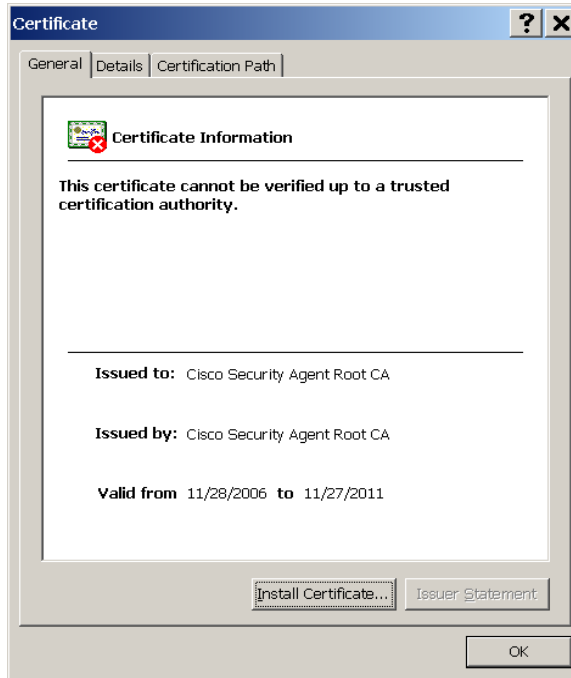
Internet Explorer: Importing the Root Certificate



Note

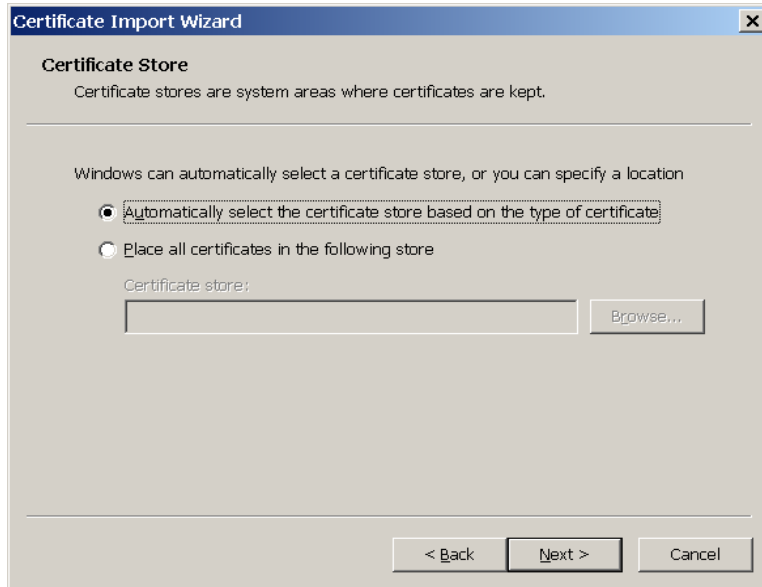
If you are using Internet Explorer 7.0, you see an “Invalid Certificate” screen when you first attempt to open a CSA MC browser window. See the end of this section for further information.

-
- Step 1** You import the certificate from the CSA MC login window. Click the **Get root certificate** link. See [Figure 3-30](#).
 - Step 2** Select the **Open** (this file from its current location) button and click **OK**.
 - Step 3** The certificate information box appears (see [Figure 3-31](#)). It contains information on the system the certificate is issued to and it displays expiration dates. Click the **Install Certificate** button to start the Certificate Manager Import Wizard.

Figure 3-31 Certificate Information

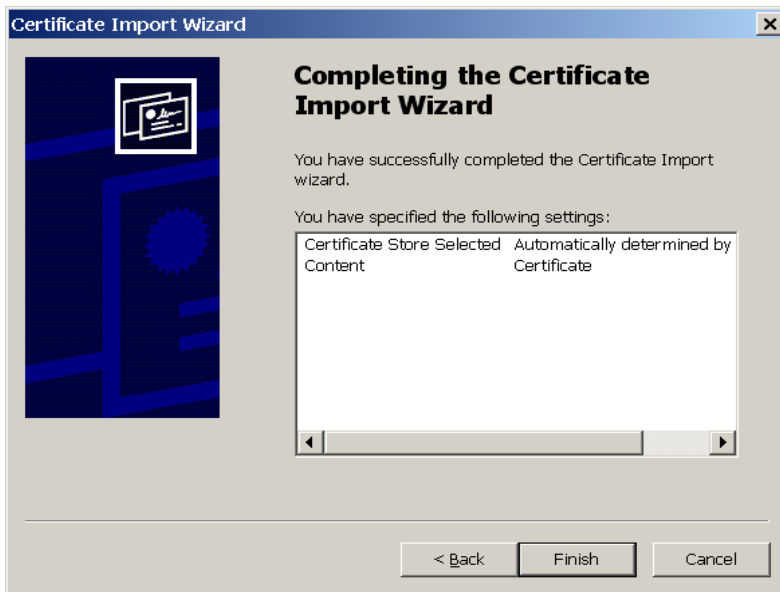
- Step 4** The first Certificate Manager Import page contains an overview of certificate information. Click **Next** to continue.
- Step 5** From the Select a Certificate Store page, make sure the **Automatically select the certificate store based on the type of certificate** radio button is selected. Click **Next**.

Figure 3-32 Certificate Wizard



- Step 6** You've now imported your certificate for the server. Click the **Finish** button (Figure 3-33) to continue.

Figure 3-33 Certificate Wizard Finish Page



- Step 7** Now, you must save the certificate. Click the **Yes** button in the Root Certificate Store box.
- Step 8** You are next prompted with a confirmation box informing you that your certificate was created successfully.



Note You must perform this certificate import process the first time you login to CSA MC from any remote machine. Once the certificate import is complete, you can access the login page directly for all management sessions. To access the login page remotely, enter the URL in the following format.

```
http://<management center system hostname>.<domain>
```

For example, enter `http://stormcenter.cisco.com`

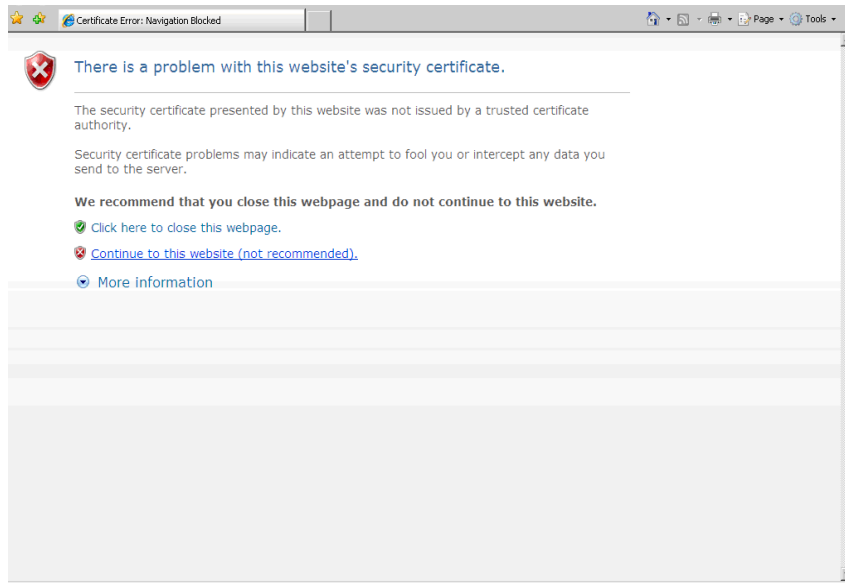
**Caution**

If you have not obtained a valid license from Cisco, when you login to CSA MC, you'll receive a warning informing you that your license is not valid. Refer back to [page 3-2](#) for further licensing information.

Internet Explorer 7.0: Importing the Root Certificate

If you are using Internet Explorer 7.0, you see an “Invalid Certificate” screen when you first attempt to open a CSA MC browser window. When that screen appears, click the **Continue to this website (not recommended)** link, see [Figure 3-34](#). Then you can continue by following instructions in [Internet Explorer: Importing the Root Certificate, page 3-44](#).

You will only see this screen the first time you access the CSA MC browser in IE 7.0. Once you follow the instructions and import the root certificate, the screen should not appear again.

Figure 3-34 *Internet Explorer 7.0 Certificate Screen*

Uninstalling Management Center for Cisco Security Agents

Uninstall the CSA MC software as follows:

- Step 1** Click the uninstall CSA MC option on the system from **Start>All Programs>Cisco Systems>Uninstall Management Center for Cisco Security Agents**. This launches the uninstall program.

You must respond to uninstall confirmation and database back-up prompts during the uninstall process. The CSA MC uninstall also removes the Cisco Security Agent on the MC system.



Note Uninstalling CSA MC does not uninstall the Microsoft SQL Server Desktop Engine (database). You must uninstall this separately from the **Control Panel>Add/Remove Programs** window if you are completely removing the product from your system.

**Caution**

If you are upgrading to a new version of CSA MC, or if you are reinstalling the product on the same system, and you want to preserve your current configuration, you should select to **Backup the Database** during the uninstall when you are prompted to do so. If you do not backup the database, the uninstall removes all program files and configurations. (Note that this only applies to local database installations. CSA MC does not provide a backup mechanism for remote databases.)

Copying Cisco Trust Agent Installer Files

Cisco Trust Agent (CTA) is an optional application you may install as part of an agent kit. The goal of bundling CTA in an agent kit is to facilitate the distribution of CTA. CTA is a separate application from CSA and has its own security objectives.

If you intend to distribute CTA through an agent kit, copy your CTA installer files to the system running CSA MC.

**Note**

Distribution of CTA through agent kits is only supported for Windows versions of CTA.

To copy the CTA installer files, follow this procedure:

Step 1

Obtain the desired CTA installer files from Cisco Systems.

**Caution**

If you are intending to install CTA version 2.1 or later, you must extract an .msi installer file from the initial CtaAdminEx-xxx-xxx**.exe file you receive. If you copy the .exe file itself to CSA MC, the CTA installation will fail. Simply

double-click the CtaAdminEx-xxx-xxx**.exe file and agree to the EULA (license) to extract the ctasetup-xxx-xxx.msi file. It is this msi file that you copy to the CSA MC system.



Note It is the user's responsibility to verify that they have obtained the correct CTA installer files.

Step 2 Copy the CTA installer files to the **%Program Files%\CSAMC52\bin\webserver\htdocs\cta_kits** directory.

The default Cisco Security Agent policies protect this directory. When you copy the files into the directory, CSA prompts you to determine if you want to allow the action. Select the **Yes** radio button and click **Apply**. Repeat this step for every file you copy into this directory.



Note Refer to the Agent Kits section of the User Guide for information on installing the CTA files you have just copied.



CHAPTER 4

Quick Start Configuration

Overview

This chapter provides the basic setup information you need to start using the Management Center for Cisco Security Agents to configure some preliminary groups and build agent kits. The goal of this chapter is to help you quickly configure and distribute Cisco Security Agent kits to hosts and have those hosts successfully register with CSA MC. Once this is accomplished you can configure some policies and distribute them to installed and registered Cisco Security Agents.

For detailed configuration information, you should refer to the User Guide.

This section contains the following topics.

- [Access Management Center for Cisco Security Agents, page 4-2](#)
- [Administrator Roles in CSA MC, page 4-3](#)
- [Administrator Authentication, page 4-3](#)
- [Cisco Security Agent Policies, page 4-4](#)
- [Configure a Group, page 4-5](#)
- [Build an Agent Kit, page 4-7](#)
- [The Cisco Security Agent, page 4-11](#)
- [View Registered Hosts, page 4-12](#)

- [Configure a Rule Module, page 4-12](#)
- [Configure a Policy, page 4-18](#)
- [Attach a Rule Module to a Policy, page 4-19](#)
- [Attach a Policy to a Group, page 4-19](#)
- [Generate Rule Programs, page 4-20](#)

Access Management Center for Cisco Security Agents

Local Access

- To access CSA MC locally on the system hosting CSA MC software, double-click the CSA MC desktop icon created during the installation.

Remote Access

- To access CSA MC from a remote location, launch a browser application and enter

```
http://<system hostname>.<domain>
```

For example, enter `http://stormcenter.cisco.com`

- Enter the administrator name and password created during the CSA MC installation.



Caution

If you have not obtained a valid license from Cisco, when you login to CSA MC, you'll receive a warning informing you that your license is not valid. Any newly deployed agents will not be able to register with the unlicensed CSA MC. Refer back to [Chapter 3, "Installing the Management Center for Cisco Security Agents"](#) for further licensing information.

Administrator Roles in CSA MC

Administrators can have different levels of CSA MC database access privileges. The initial administrator created by the CSA MC installation automatically has configure privileges. When you create new administrators on the system, you can give them one of the following roles.

CSA MC Administrator Roles:

- **Configure**—This provides full read and write access to the CSA MC database.
- **Deploy**—This provides full read and partial write access to the CSA MC database. Administrators can manage hosts and groups, attach policies, create kits, schedule software updates, and perform all monitoring actions.
- **Monitor**—This provides administrators with read access to the entire CSA MC database. Administrators can also create reports, alerts, and event sets.

See the *Management Center for Cisco Security Agents User Guide* for Administrator configuration details.

Administrator Authentication

CSA MC allows administrators logging into the system to be authenticated either through the local configuration database or via LDAP authentication. If you intend to use LDAP authentication, LDAP server information must be entered in CSA MC. See the *Management Center for Cisco Security Agents User Guide* for Administrator LDAP authentication details.

Cisco Security Agent Policies

CSA MC default Cisco Security Agent kits, groups, policies, and configuration variables are designed to provide a high level of security coverage for desktops and servers. These default Cisco Security Agent kits, groups, policies, rule modules and configuration variables cannot anticipate all possible local security policy requirements specified by your organization's management, nor can they anticipate all local combinations of application usage patterns. Cisco recommends deploying agents using the default configurations and then monitoring for possible tuning to your environment.

If you are using shipped policies, you can also use shipped, pre-built agent kits. Therefore, if you're not creating your own configurations, you can simply refer to [Chapter 3](#) and [Chapter 10](#) in the User Guide for information on deploying kits to end users and viewing the event log.



Note

Each pre-configured rule module, policy, and group page has data in the expandable +**Detailed** description field explaining the item in question. Read the information in these fields to learn about the items described and to determine if the item in question meets your needs for usage.

As a jumping off point for creating your own configurations, the following sections in this manual take you through the step by step process of configuring some of the basic elements you need to initiate server/agent communications and to begin the distribution of your own policies.

Configure a Group

Host groups reduce the administrative burden of managing a large number of agents. Grouping hosts together also lets you apply the same policy to a number of hosts.

A group is the only element required to build Cisco Security Agent kits. When hosts register with CSA MC, they are automatically put into their assigned group or groups. Once hosts are registered you can edit their grouping at any time.

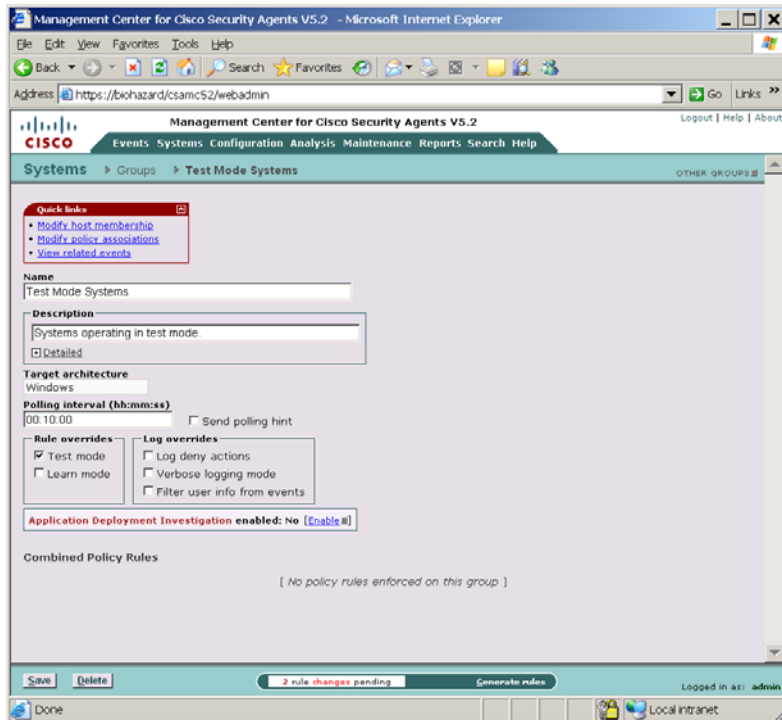
**Note**

Management Center for Cisco Security Agents ships with preconfigured groups you can use if they meet your initial needs. If you use a preconfigured group, you do not have to create your own group as detailed in the following pages.

To configure a group, do the following.

-
- Step 1** Move the mouse over **Systems** in the menu bar of CSA MC and select **Groups** from the drop-down menu that appears. The Groups list view appears.
- Step 2** Click the **New** button to create a new group entry. You are prompted to select whether this is a Windows, Linux, or Solaris group. For this example, click the Windows button. This takes you to the Group configuration page.
- Step 3** In the available group configuration fields, enter the following information:
- **Name**—This is a unique name for this group of hosts. Names are case insensitive, must start with an alphabetic character, can be up to 64 characters long and can include alphanumeric characters, spaces, and underscores.
 - **Description**—This is an optional line of text that is displayed in the list view and helps you to identify this particular group.

Figure 4-1 Group Configuration View



Step 4 Cisco suggests that you select the **Test Mode** checkbox (available from the **Rule overrides** section) for this group. In Test Mode, the policy we will later apply to this group will not be active. In other words, the agent will not deny any action even if an associated policy says it should be denied. Instead, the agent will allow the action but log an event letting you know the action would have been denied.

Using Test Mode helps you to understand the impact of deploying a policy on a host before enforcing it. If examining the logs shows you that the policy is working as intended on a group, you can then remove the Test Mode designation. For detailed information on **Polling intervals**, **Test Mode**, **Verbose Logging Mode**, **Log deny actions** and **Filter user from events** refer to the User Guide.

Step 5 Click the **Save** button to enter and save your group in the CSA MC database.

Build an Agent Kit

**Note**

The Management Center for Cisco Security Agents ships with preconfigured agent kits you can use to download and install agents if they meet your initial needs (accessible from **System>Agent kits** in the menu bar). There are prebuilt kits for desktops, servers, and others. These kits place hosts in the corresponding groups and enforce the associated policies of each group. (If you use a preconfigured agent kit, you do not have to build your own kit as detailed in the following pages.)

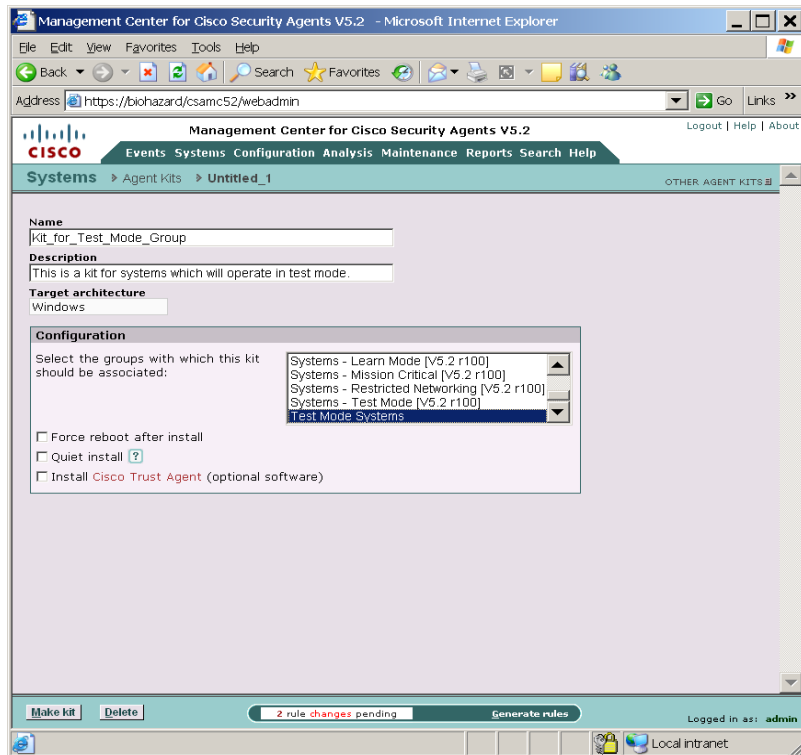
Once you have a group configured, you can build a Cisco Security Agent kit. Hosts on your network will download this kit and use it to install an agent on their system. A group designation is the only information this kit will initially contain for hosts that download and install it.

When an agent is installed on a host, the agent automatically and transparently registers itself with CSA MC. It now appears in the CSA MC database as part of the groups designated in the kit, and will enforce policies that are applied to those groups.

To create a Cisco Security Agent kit, do the following.

-
- Step 1** Move the mouse over **Systems** in the menu bar and select **Agent Kits** from the drop-down menu that appears. The agent kit list view displays the preconfigured agent kits.
 - Step 2** Click the **New** button to create a new agent kit. You are prompted to select whether this is a Windows, Linux, or Solaris agent kit. For this example, click the Windows button. This takes you to the Agent kit configuration page.
 - Step 3** In the configuration view (see [Figure 4-2](#)), enter a **Name** for the kit. This is a unique name (Agent kit names are an exception. Spaces are not valid name characters for agents kits as they are for other name fields).
 - Step 4** Enter a **Description**. This is an optional line of text that is displayed in the agent kit list view.
 - Step 5** From the available list box, select the groups you are associating with this kit. (The names of the groups you configured in the previous section should appear here.)
 - Step 6** You have the option of forcing systems to reboot after the agent installation completes. If you select the **Force reboot after install** checkbox, when the install finishes, a message appears to the end user warning that the system will automatically reboot in 5 minutes. This reboot cannot be stopped by the end user. Keep in mind, if you are selecting to force a reboot, the installation must also be "Quiet". (See the User Guide for details.)
 - Step 7** Click the **Make Kit** button in the bottom frame. See [Figure 4-2](#).

Figure 4-2 Create Agent Kit



Once you click the Make Kit button and generate rules, CSA MC produces a kit for distribution (see Figure 4-3). You may distribute the kit download URL, via email for example, to the host systems the kit is designated for. They access the URL to download and then install the kit. This is the recommended method of agent kit distribution.

But you may also point users to a URL for the CSA MC system. This URL will allow them to see all kits that are available. That URL is:

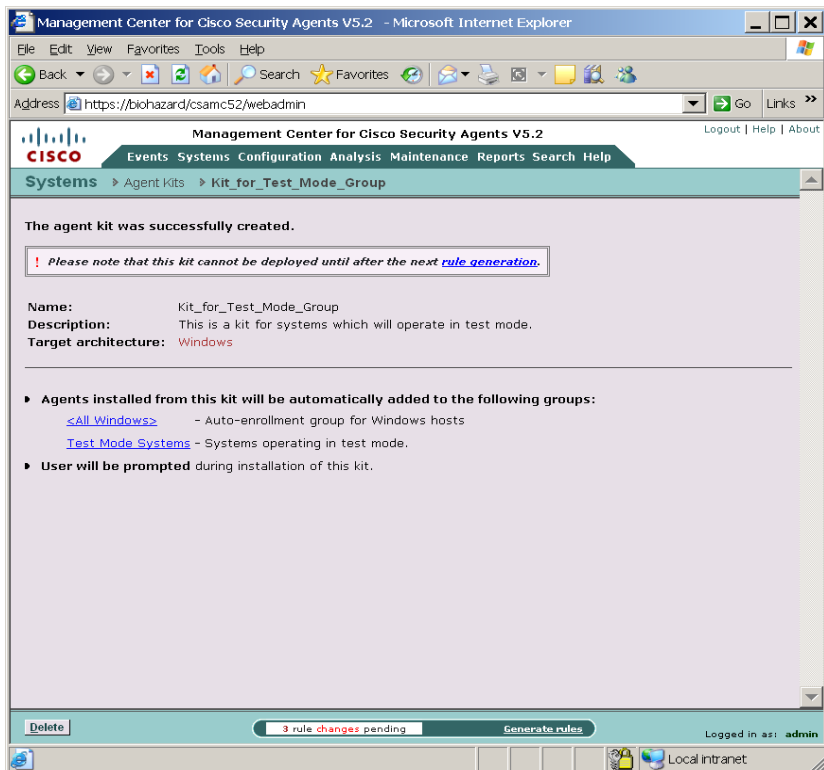
```
https://<system name>/csamc52/kits
```

If you are pointing users to the “kits” URL and you have multiple agent kits listed here, be sure to tell users which kits to download.



Note Note that the Registration Control feature also applies to the `https://<system name>/csamc52/kits` URL. If the Registration Control feature (see the User Guide for details on the feature) prevents your IP address from registering.

Figure 4-3 Agent Kit Created



The Cisco Security Agent

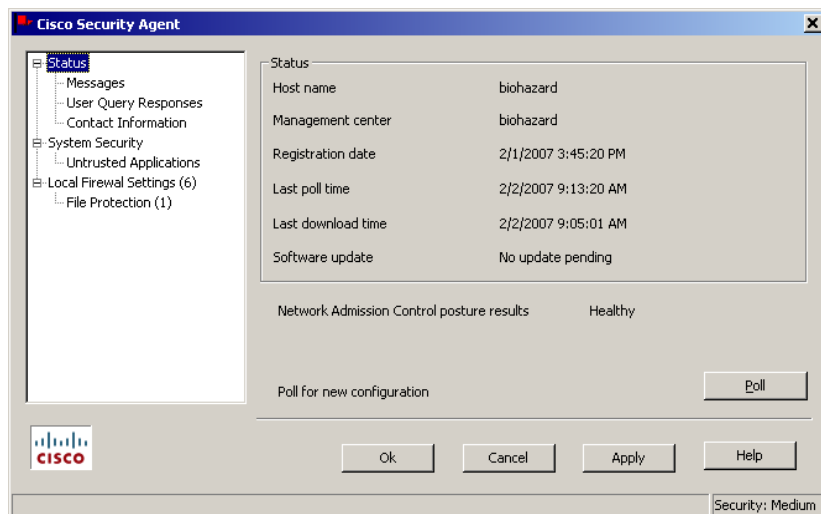
- Users must have administrator privileges on their systems to install the Cisco Security Agent software.
- The Cisco Security Agent installs on supported Windows, Linux, and Solaris platforms. (Note that on Solaris systems there is no agent user interface. See Appendix A in the User Guide for information on the Solaris agent utility.)

Once users successfully download and install Cisco Security Agents, they can optionally perform a reboot for full agent functionality.

When the system restarts, the agent service starts immediately and the flag icon appears in the system tray (if end user systems are configured to have an agent UI). At this time, the agent automatically and transparently registers with CSA MC. Agents are immediately enforcing rules.

To open the agent user interface, end users can double-click on the flag icon in their system tray. The user interface opens on their desktop.

Figure 4-4 Agent Status



Note

For detailed information on installing both the Windows and UNIX agents, refer to Appendix A in this manual or in the User Guide.

View Registered Hosts

From CSA MC, you can see which hosts have successfully registered by accessing **Hosts** from the **Systems** link in the menu bar. This takes you to the **Hosts list** page. On the right side of this page is a column that displays varying types of information on each host. Use the pull-down menu for this column to filter your host list based on the status in question.

To search for specific hosts based on more status data, use the **Search** option in CSA MC. Search for Hosts using available status information such as:

- Active hosts—A host is active if it polls into CSA MC at regular intervals.
- Not active hosts—A host is inactive if it has missed a certain number polling intervals or if it has not polled into the server for at least one hour.

You can also view registered hosts by accessing the Groups page. From the groups list view, click the link for the group you created in the previous sections. Now click the **Modify host membership** link. All hosts who installed the kit created using this group should appear here as part of the group. (You might want to click the Refresh button on your browser to ensure you are viewing updated information.)

Configure a Rule Module

This section provides brief instructions for configuring and distributing a policy to Cisco Security Agents. For a full discussion of rule modules and policies, you should refer to the User Guide. In the meantime, use the following instructions to distribute a fairly simple policy to the agents that are currently installed on end user systems.

When you configure a policy, you are combining rule modules under a common name. Those rule modules are then attached to a policy. That policy is attached to a group of hosts and it uses the rules that comprise the policy to control the actions that are allowed and denied on those hosts.

For this example, we will configure a rule module containing file access control rule that protects systems from a known email virus. In this example, a VBS file (badfile.vbs) is detected, correlated across systems, and quarantined by CSA MC.

This quarantine list updates automatically (dynamically) as logged quarantined files are received. You can use a file access control rule to permanently quarantine a known virus as shown in this example.

**Note**

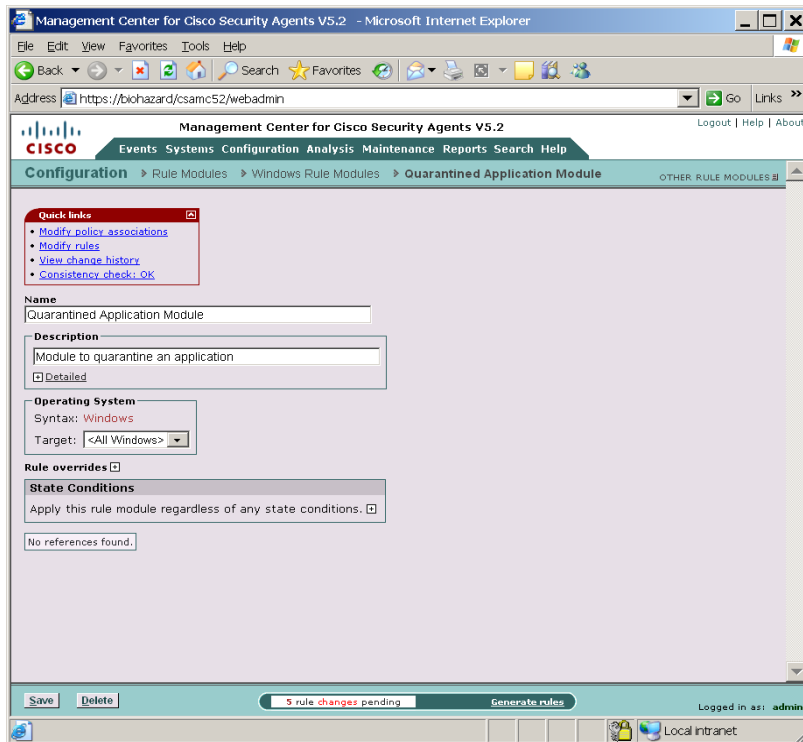
Cisco recommends that you do not edit the preconfigured policies shipped with the Management Center for Cisco Security Agents, but instead add new policies to groups for any changes you might want.

To configure this file quarantine rule module, do the following.

-
- Step 1** Move the mouse over **Configuration** in the menu bar and select **Rule Modules [Windows]** from the drop-down list that appears. The Windows Rule Module list view appears.
 - Step 2** Click the **New** button to create a new module. This takes you to the Rule Module configuration page. See [Figure 4-5](#).
 - Step 3** In the configuration view, enter the **Name** *Quarantined Application Module*. Note that names are case insensitive, must start with an alphabetic character, can be up to 64 characters long. Spaces are also allowed in names.
 - Step 4** Enter a **Description** of your module. We'll enter *Module to quarantine an application*.
 - Step 5** Click the **Save** button. (We will not use State Sets in this example.)

Now we add our file access rule to this module.

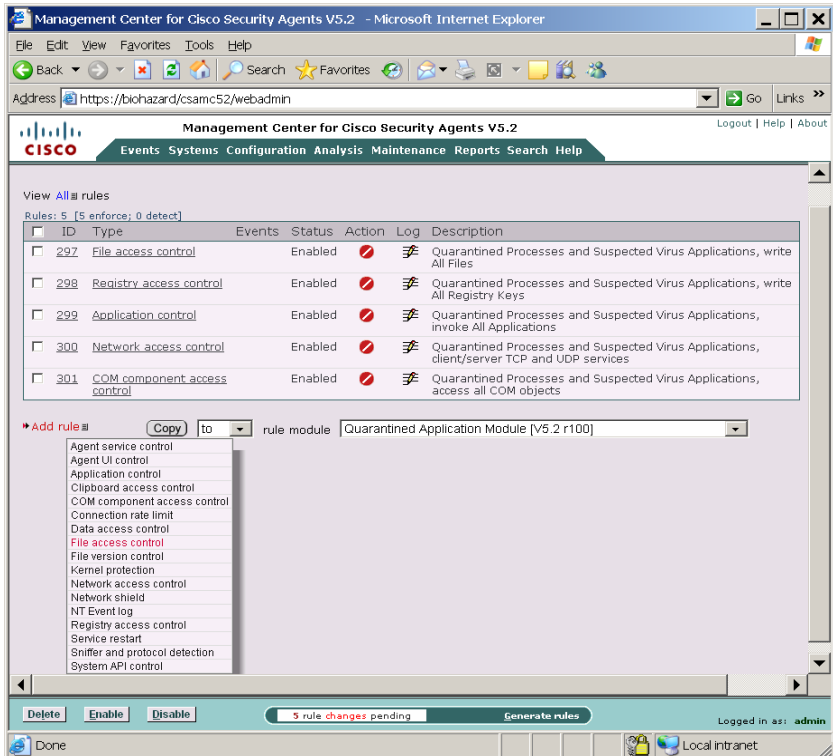
Figure 4-5 Rule Module Creation View



Create a File Access Control Rule

- Step 1** From the Rule Module configuration page (Figure 4-5), click the **Modify rules** link at the top of the page. You are now on the Rules page.
- Step 2** In the Rule page, click the **Add rule** link. A drop down list of available rule types appears.
- Step 3** Click the **File access control** rule from the drop down list (see Figure 4-6). This takes you to the configuration page for this rule.

Figure 4-6 Add Rules to Module



Step 4 In the File access control rule configuration view (see Figure 4-7), enter the following information:

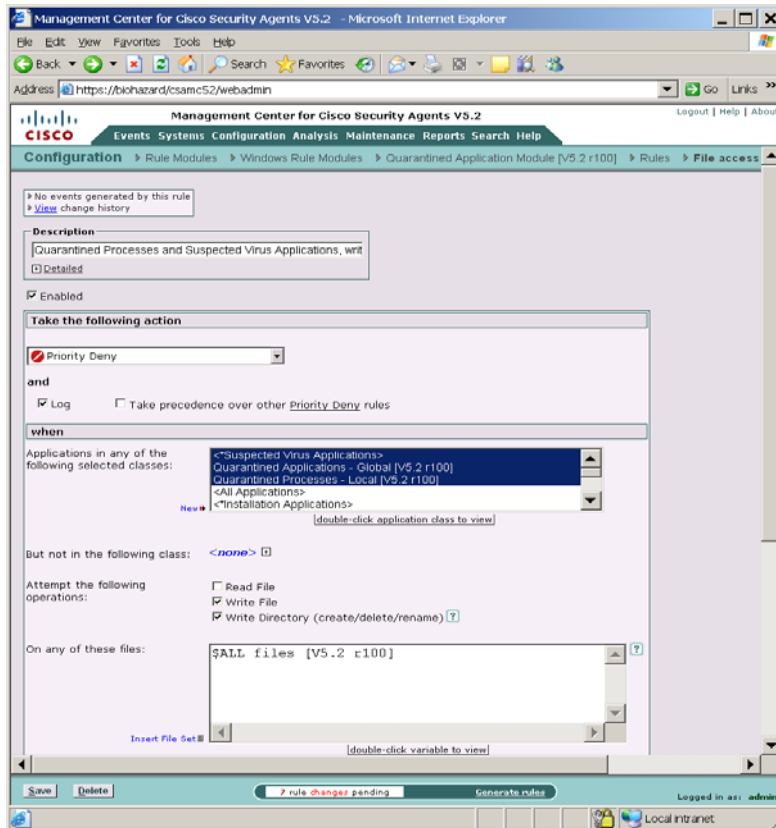
- **Description**—Quarantined and Suspected Virus Applications, write All Files
- **Enabled**—(This is selected by default. Don't change this setting for this example.)

Step 5 Select **Priority Deny** from the action pulldown list.

By selecting Priority Deny here, we are stopping the quarantined applications we're going to specify later from performing a selected operation on the files we will indicate. By default, when you create a deny rule, all other actions are allowed unless specifically denied by other rules. See the User Guide for information on allow/deny specifics.

- Step 6** Select the **Log** checkbox.
This means that the system action in question is logged and sent to the server. Generally, you will want to turn logging on for all deny rules so you can monitor event activity.
- Step 7** Select a preconfigured Application class from the available list to indicate the applications whose access to files we want exercise control over. For this rule, we'll select **Quarantined applications**. Note that when you click Save, selected application classes move to the top of the list.
- Step 8** Select the and **Write File** and **Write Directory** checkboxes to indicate the actions we are denying.
- Step 9** Now we'll enter the system files we are protecting with this rule. In the files field, enter \$All files available from the **Insert File Set** option.
- Step 10** Click the **Save** button.
Next, we will create a policy to attach our rule module to.

Figure 4-7 File Access Control Rule



Configure a Policy

Generally, when you configure a policy, you are combining multiple rule modules under a common name. That policy name is then attached to a group of hosts and it uses the rules that comprise the policy to control the actions that are allowed and denied on those hosts. You can have several different types of rules in a rule module and consequently within one policy.

The policy level is the common ground by which host groups acquire the rules that make up their security policy. You can attach rule modules of differing architectures to the same policy. This way, you can configure a task-specific, self-contained, inclusive policies across all supported architectures (Windows, Solaris, Linux) for software that is supported on all platforms.

**Note**

Management Center for Cisco Security Agents ships with preconfigured policies you can use if they meet your initial needs. If you use a preconfigured policy, you do not have to create your own policy as detailed in the following pages.

To configure a policy, do the following.

-
- Step 1** Move the mouse over **Configuration** in the menu bar of CSA MC and select **Policies** from the drop-down menu that appears. The policy list view appears.
 - Step 2** Click the **New** button to create a new policy entry. This takes you to the policy configuration page.
 - Step 3** In the available policy configuration fields, enter the following information:
 - **Name**—This is a unique name for this policy grouping of rule modules. Names are case insensitive, must start with an alphabetic character, can be up to 64 characters long and can include alphanumeric characters, spaces, and underscores. For this exercise, enter the name *Quarantined Applications*.
 - **Description**—This is an optional line of text that is displayed in the list view and helps you to identify this particular policy.
 - Step 4** Click the **Save** button.

Attach a Rule Module to a Policy

To apply our configured email quarantine rule module to the policy we've created, do the following.

-
- Step 1** From Policy edit view, click the **Modify rule module associations** link. This takes you to a view containing a swap box list of available modules.
 - Step 2** Select the **Quarantined Application Module** from the list box on the left and click the **Add** button to move it to the right side box.

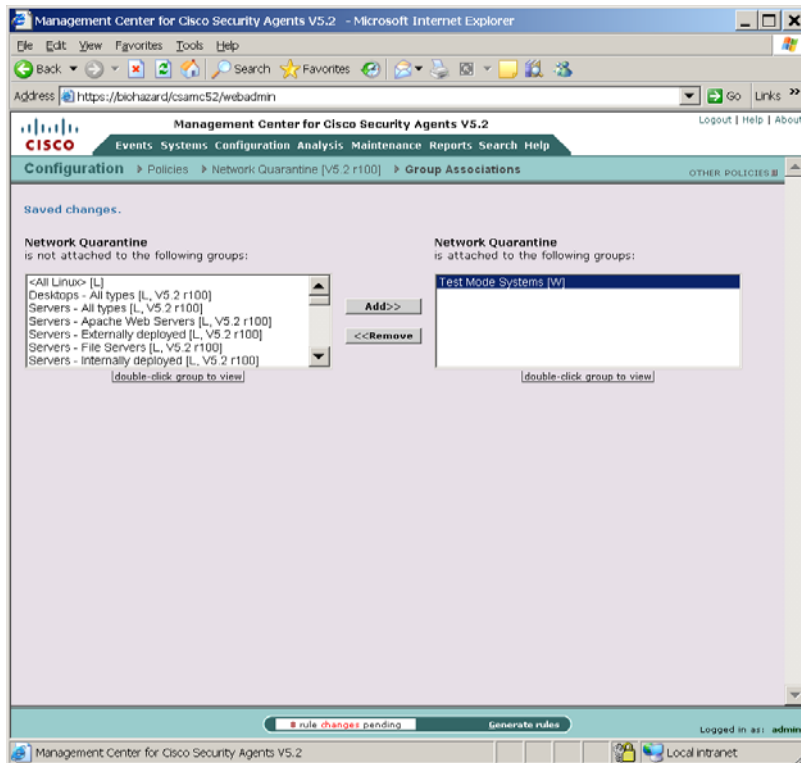
The rule module is now attached to this policy.

Attach a Policy to a Group

To apply our configured email quarantine policy to a particular group of host systems, we must attach this policy to that group.

-
- Step 1** Move the mouse over **Systems** in the menu bar and select **Groups** from the drop-down menu that appears.
 - Step 2** From the group list view, click the link for the group you want to attach the policy to. This brings you to that group's edit view.
 - Step 3** From the edit view, click the **Modify policy associations** link. This takes you to a view containing a swap box list of available policies (see [Figure 4-8](#)).
 - Step 4** Select the appropriate policy from the list box on the left and click the **Add** button to move it to the right side box.
 - Step 5** The policy is now attached to this group.

Figure 4-8 Attach Policy to Group



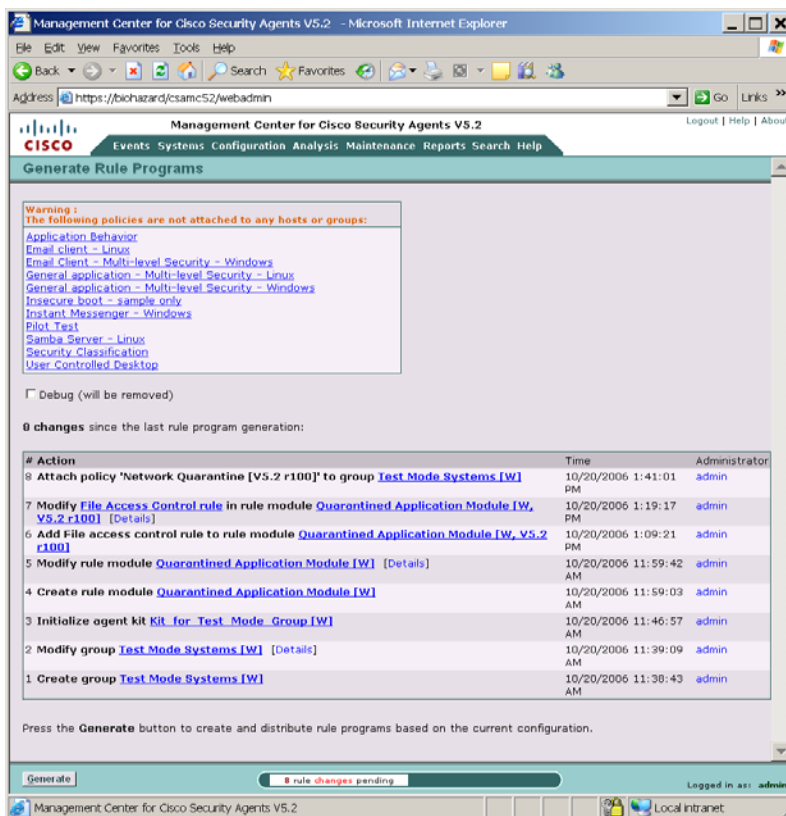
Generate Rule Programs

Now that we've configured our policy and attached it to a group, we'll next distribute the policy to the agents that are part of the group. We do this by first generating our rule programs.

Click **Generate rules** in the bottom frame of CSA MC. All pending database changes ready for distribution appear (see [Figure 4-9](#)).

If everything looks okay, you can click the **Generate** button that now appears in the bottom frame. This distributes your policy to the agents.

Figure 4-9 Generate Rule Programs



You can ensure that agents have received this policy by clicking **Hosts** (accessible from **Systems** in the menu bar) and viewing the individual host status views. Click the Refresh button on your browser and look at the host Configuration version data in the host view to make sure it's up-to-date.



Note

Hosts poll into CSA MC to retrieve policies. You can shorten or lengthen this polling time in the Group configuration page. You can also send a hint message to tell hosts to poll in before their set polling interval. See the User Guide for details.

Now your agents are installed and protecting end user systems using the macro policy we've configured.

Refer to the User Guide to read about the configuration tasks described here in more detail.



APPENDIX **A**

Cisco Security Agent Installation and Overview

Overview

This chapter describes the Cisco Security Agent and provides information on the agent user interface. It also includes installation information for Windows, Linux, and Solaris agents. (This information, with additional details, also appears in a similarly titled Appendix A in the User Guide.)

Once the agent is installed, there is no configuration necessary on the part of the end user in order to run the agent software. Optionally, as the administrator, you can ask users to enter individualized contact information into the fields provided. If required, the agent user interface makes it easy for the user to enter this data and send it to CSA MC.

This section contains the following topics.

- [Downloading and Installing, page A-2](#)
- [The Cisco Security Agent User Interface, page A-4](#)
- [Installing the Solaris Agent, page A-6](#)
- [Installing the Linux Agent, page A-8](#)

Downloading and Installing

Once you build an agent kit on CSA MC, you deliver the generated URL, via email for example, to end users so that they can download and install the Cisco Security Agent. They access the URL to download and then install the kit. This is the recommended method of agent kit distribution. But you may also point users to a URL for the CSA MC system. This URL will allow them to see all kits that are available. That URL is:

```
https://<system name>/csamc52/kits
```

If you are pointing users to the “kits” URL and you have multiple agent kits listed here, be sure to tell users which kits to download.

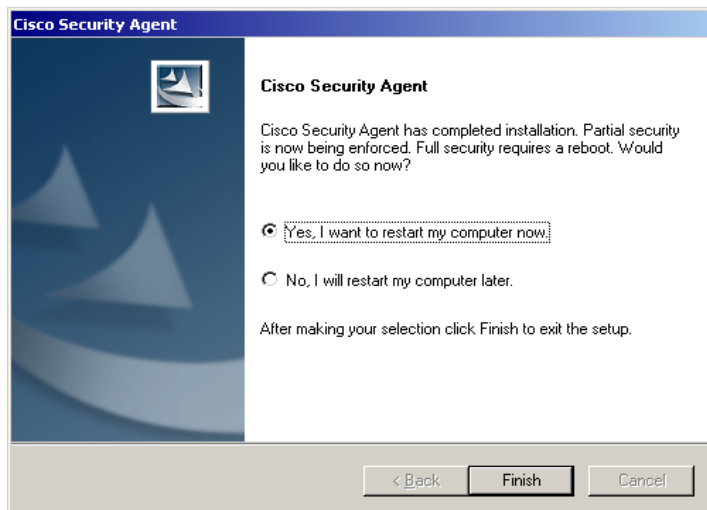
**Note**

Note that the Registration Control feature also applies to the <system name>/csamc52/kits URL. If the Registration Control feature (see the User Guide for details on the feature) prevents your IP address from registering, it also prevents you from viewing the agent kits URL.

**Note**

Cisco Security Agent systems must be able to communicate with the Management Center for Cisco Security Agents over HTTPS.

Once users install agents on their systems, they can optionally perform a reboot (if Force reboot is not selected). See [Figure A-1](#). Whether a system is rebooted or not, the agent service starts immediately and the system is protected. (Note that Windows NT4 systems must be rebooted after an agent installation.)

Figure A-1 *Optional Agent Reboot*

If a system is not rebooted following the agent installation, the following functionality is not immediately available. (This functionality becomes available the next time the system is rebooted.)

Windows agents

- Network Shield rules are not applied until the system is rebooted.
- Network access control rules only apply to new socket connections. Network server services should be stopped and restarted for full network access control security without a system reboot.
- Data access control rules are not applied until the web server service is restarted.

Solaris and Linux agents, when no reboot occurs after install, the following caveats exist

- Network access control rules only apply to new socket connections. Network server services should be stopped and restarted for full network access control security without a system reboot.
- Buffer overflow protection is only enforced for new processes.
- File access control rules only apply to newly opened files.
- Data access control rules are not applied until the web server service is restarted.

After installation, the agent automatically and transparently registers with CSA MC. You can see which hosts have successfully registered by clicking the **Hosts** link available from the **Systems** category in the menu bar. This displays the hosts list view. All registered host system names appear here.

The Cisco Security Agent User Interface

**Note**

The Cisco Security Agent user interface does not run on Solaris systems.

**Note**

If the **Agent UI control rule** is not present (available on Windows and Linux only) for the system group, no agent UI appears on the end user system.

To open the Cisco Security Agent user interface on Windows and Linux systems, users can double-click on the flag icon in their system trays. The user interface opens on their desktop.

As the administrator, you decide which agent UI options to provide to the end user. These options are controlled by the Agent UI control rule. Available options are as follows:

- **Allow user to reset agent UI default settings**—Selecting this checkbox in the Agent UI control rule causes the end user to have a product reset option available from the Start>Programs>Cisco Security Agent menu. Selecting the "Reset Cisco Security Agent" option puts all agent settings back to their original states and clears almost all other user-configured settings. This does not clear configured Firewall Settings or File Protection settings. But if these features are enabled, they are disabled as this is the default factory setting. The information entered into the edit boxes for these features is not lost.
- **Allow user interaction**—Selecting this checkbox in the Agent UI control rule causes the end user to have a visible and accessible agent UI, including a red flag in the system tray.
- **Allow user access to agent configuration and contact information**—Selecting this checkbox in the Agent UI control rule provides Status, Messages, and Contact Information features, including the ability to manually poll the MC. It also provides the User Query Responses window.

- **Allow user to modify agent security settings**—Selecting this checkbox in the Agent UI control rule provides System Security and Untrusted Applications features.
- **Allow user to modify agent personal firewall settings**—Selecting this checkbox in the Agent UI control rule provides Local Firewall Settings and File Protection features.

The options available to the user in the agent UI depend upon the features selected in the Agent UI control rule governing the agent in question. All possible agent features are described in Appendix A of the User Guide.

Uninstall Windows Cisco Security Agent

To uninstall the Cisco Security Agent, do the following:

From the **Start** menu, go to **Programs>Cisco Security Agent>Uninstall Cisco Security Agent**. Reboot the system when the uninstall is finished.



Note You can also uninstall the agent from the Start>Settings>Control Panel>Add/Remove Programs dialog.

Installing the Solaris Agent

This section details the commands you enter and the subsequent output that is displayed when you install the Cisco Security Agent on Solaris systems.



Note

See the similarly titled Appendix A in the User Guide for information on a Solaris agent utility which allows you to manually poll to CSA MC and perform other tasks.

When you download the Cisco Security Agent kit from CSA MC, do the following to unpack and install it. (Note that you can put the downloaded tar file in any temp directory. Do not put it in the opt directory, for example, as you may then experience problems with the installation.)

Step 1 You must be super user on the system to install the agent package.

```
$ su
```

Step 2 Untar the agent kit.

```
# tar xf
CSA-Test_Mode_Server_V5.2.0.265-sol-setup-f734064be5a448b88e2a2786
7059113c.tar
```

Step 3 Install the agent package. (Use the command listed below when you install. This command forces the installation to use a package administration file to check the system for the required OS software agent dependencies. If the required dependencies are not present, such as the "SUNWlibCx" library, the install aborts.)

```
# pkgadd -a CSCOcsa/reloc/cfg/admin -d .
```

```
[Output:]
```

```
The following packages are available:
```

```
1 CSCOcsa CSAagent
(sun4u) 5.2.0.15
```

Step 4 Select the correct package or press enter to unpack all current packages.

```
Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

```
[Output:]
```

```
Processing package instance <CSCOcsa> from </space/user>
```

The install now displays the Cisco copyright and prompts you to continue the installation.

Step 5 Answer yes (y) to continue the installation.

This package contains scripts which will be executed with super-user permission during the process of installing this package.

```
Do you want to continue with the installation of <CSCOcsa>
[y,n,?] y
[Output:]
Installing CSAagent as <CSCOcsa>
```

The installation continues to copy and install files. When the install is complete, the following is displayed:

```
[Output:]
The agent installed cleanly, but has not yet been started.
The command: /etc/init.d/ciscosec start
will start the agent. The agent will also start
automatically upon reboot. A reboot is recommended to
ensure complete system protection.
The following packages are available:
  1 CSCOcsa CSAagent
    (sun4u) 5.2.0.15
```

Step 6 Quit (q) when installation is finished.

```
Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]: q
```

Step 7 Optionally, reboot the system by entering the following.

```
# shutdown -y -i6 -g0
```

**Caution**

If a system is not rebooted following the agent installation, the following functionality is not immediately available: Buffer overflow protection is only enforced for new processes, network access control rules only apply to new socket connections, file access control rules only apply to newly opened files, and data access control rules are not applied until the web server service is restarted. (This functionality becomes available the next time the system is rebooted.)

The agent installs into the following directory:

```
/opt/CSCOcsa
```

Some files are put into additional directories such as

```
/kernel/strmod/sparcv9,usr/lib/csa,/etc/init.d and /etc/rc?.d.
```

**Caution**

If you are upgrading the Solaris agent and you encounter the following error, "There is already an instance of the package and you cannot install due to administrator rules", you must edit the file `/var/sadm/install/admin/default`. Change "instance=unique" to "instance=overwrite" and then proceed with the upgrade.

Uninstall Solaris Agent

To uninstall the Cisco Security Agent, enter the following command:

```
# pkgrm CSCOcsa
```

**Note**

If an agent is running a policy which contains an Agent self protection rule, the agent cannot be uninstalled unless this rule is disabled. (Administrators can generally do this through a remote management session if the default policies applied to the CSA MC/VMS system are not changed to restrict this access.) See **Agent self protection** in the User Guide for details on this rule type.

A shipped UNIX policy allows secured management applications to stop the agent service. For example, after having logged in by selecting Command Line Login in the options menu of the login screen, all login applications are considered secure management applications. You can now run the `pkgrm` command to uninstall the agent.

Installing the Linux Agent

This section details the commands you enter and the subsequent output that is displayed when you install the Cisco Security Agent on Linux systems.

When you download the Cisco Security Agent kit from CSA MC, do the following to unpack and install it.

Step 1 Move the tar file downloaded from CSA MC to a temporary directory, e.g.

```
$ mv  
CSA-Server_v5.2.0.218-lin-setup-1a969c667ddb0a2d2a8da3e7959  
a30b2.tar /tmp
```

Step 2 Untar the file.

```
$ cd /tmp
$ tar xvf
CSA-Server_V5.2.0.218-lin-setup-1a969c667ddb0a2d2a8da3e7959
a30b2.tar
```

Step 3 cd to CSCCOcsa directory where the rpm package is located.

```
$ cd /tmp/CSCCOcsa
```

Step 4 Run script install_rpm.sh as root.

```
# sh ./install_rpm.sh
```

The package will be installed to `/opt/CSCCOcsa`, with some files being put into directories such as `/lib/modules/CSCCOcsa`, `/lib/csa`, `/etc/init.d` and `/etc/rc?.d`.



Note

CSAagent rpm packages are not relocatable.



Caution

If a system is not rebooted following the agent installation, the following functionality is not immediately available: Buffer overflow protection is only enforced for new processes, network access control rules only apply to new socket connections, file access control rules only apply to newly opened files, and data access control rules are not applied until the web server service is restarted. (This functionality becomes available the next time the system is rebooted.)



Note

Linux Agent UI: For gnome desktop environments, the install script will only modify the default session config file for launching the agent UI automatically every time a user starts a gnome desktop session. But if a user already has their own session file (`~/.gnome2/session`), the default session file (`/usr/share/gnome/default.session`) will not be effective. Therefore, the agent UI will not automatically start when the user logs in. In such a case, the user must add the agent UI (`/opt/CSCCOcsa/bin/ciscosecui`) manually (using "gnome-session-properties" utility) to make the agent UI auto-start.

**Caution**

On Linux systems, if you upgrade the kernel version or boot a different kernel version than the initial version where the agent was installed, you must uninstall and reinstall the agent.

Uninstall Linux Agent

To uninstall the Cisco Security Agent, do the following.

- Step 1** You must know the version number of the currently installed agent. Keep in mind that upgrades may have been installed since the first installation. When you know the version, run the following, using the correct version number.

```
# rpm -qf /opt/CSCOcsa/bin/ciscosecd  
CSAgent-5.2-218
```

- Step 2** Remove that rpm with rpm -ev, e.g.

```
# rpm -ev CSAgent-5.2-218
```

**Caution**

If an agent is running a policy which contains an Agent self protection rule, the agent cannot be uninstalled unless this rule is disabled. (Administrators can generally do this through a remote management session if the default policies applied to the CSA MC system are not changed to restrict this access.) See **Agent self protection** in the User Guide for details on this rule type.

You can uninstall the linux agent regardless of policies if you login using single user mode.



APPENDIX **B**

Third Party Copyright Notices

Cisco Security Agent utilizes third party software from various sources. Portions of this software are copyrighted by their respective owners as indicated in the copyright notices below.

OPENSSL [version 0.9.7L]

Copyright (c) 1998-2006 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====
 This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

SSLEAY license [version SSLeay 0.8.0]

Copyright © 1995-1998 Eric Young (ey@cryptsoft.com)
 All rights reserved.

This package is an SSL implementation written by Eric Young (ey@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
"This product includes cryptographic software written by Eric Young (ey@cryptsoft.com)"
The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related ;-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

**Apache [version 2.0.59],
Xerces 2.7 and AxisCpp 1.6**

Copyright © 2000-2005 The Apache Software Foundation. All rights reserved.

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

**TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND
DISTRIBUTION**

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a

whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. **Grant of Copyright License.** Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. **Grant of Patent License.** Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or

contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

- (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

- (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

- (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

- (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License,

without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. **Trademarks.** This License does not grant permission to use the tradenames, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. **Disclaimer of Warranty.** Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. **Limitation of Liability.** In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. **Accepting Warranty or Additional Liability.** While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

TCL license

This software is copyrighted by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and other parties. The following terms apply to all files associated with the software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute, and license this software and its documentation for any purpose, provided that the existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this software may be copyrighted by their authors and need not follow the licensing terms described here, provided that the new terms are clearly indicated on the first page of each file where they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the U.S. Government, the Government shall have only "Restricted Rights" in the software and related documentation as defined in the Federal Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you are acquiring the software on behalf of the Department of Defense, the software shall be classified as "Commercial Computer Software" and the Government shall have only "Restricted Rights" as defined in Clause 252.227-7013 (c) (1) of DFARs. Notwithstanding the

foregoing, the authors grant the U.S. Government and others acting in its behalf permission to use and distribute the software in accordance with the terms specified in this license.

Perl

Copyright 1987-2005, Larry Wall

Perl may be copied only under the terms of either the Artistic License or the GNU General Public License, which may be found in the Perl 5 source kit.

Complete documentation for Perl, including FAQ lists, should be found on this system using ``man perl'` or ``perldoc perl'`. If you have access to the Internet, point your browser at <http://www.perl.org/>, the Perl Home Page.

libpcap

Copyright (c) 1993, 1994, 1995, 1996, 1997, 1998, The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University of California, nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER

IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

CMU-SNMP Libraries

This product contains software developed by Carnegie Mellon University. Copyright 1998 by Carnegie Mellon University. All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Open Market FastCGI

This FastCGI application library source and object code (the "Software") and its documentation (the "Documentation") are copyrighted by Open Market, Inc ("Open Market"). The following terms apply to all files associated with the Software and Documentation unless explicitly disclaimed in individual files.

Open Market permits you to use, copy, modify, distribute, and license this Software and the Documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this Software and Documentation may be copyrighted by their authors and need not follow the

licensing terms described here. If modifications to this Software and Documentation have new licensing terms, the new terms must be clearly indicated on the first page of each file where they apply.

OPEN MARKET MAKES NO EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE SOFTWARE OR THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL OPEN MARKET BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY DAMAGES ARISING FROM OR RELATING TO THIS SOFTWARE OR THE DOCUMENTATION, INCLUDING, WITHOUT LIMITATION, ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OR SIMILAR DAMAGES, INCLUDING LOST PROFITS OR LOST DATA, EVEN IF OPEN MARKET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS". OPEN MARKET HAS NO LIABILITY IN CONTRACT, TORT, NEGLIGENCE OR OTHERWISE ARISING OUT OF THIS SOFTWARE OR THE DOCUMENTATION.

CGIC License

CGIC, copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004 by Thomas Boutell and Boutell.Com, Inc.. Permission is granted to use CGIC in any application, commercial or noncommercial, at no cost. HOWEVER, this copyright paragraph must appear on a "credits" page accessible in the public online and offline documentation of the program. Modified versions of the CGIC library should not be distributed without the attachment of a clear statement regarding the author of the modifications, and this notice may in no case be removed. Modifications may also be submitted to the author for inclusion in the main CGIC distribution.

Mozilla 1.xx (libcurl)

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2007, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT SQL SERVER 2005 EXPRESS EDITION

MICROSOFT SQL SERVER 2005 EXPRESS EDITION WITH ADVANCED SERVICES

MICROSOFT SQL SERVER 2005 EXPRESS TOOLKIT

MICROSOFT SQL SERVER 2005 MANAGEMENT STUDIO EXPRESS

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply.

BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE.

If you comply with these license terms, you have the rights below.

1. **INSTALLATION AND USE RIGHTS.**

- a. Installation and Use. You may install and use any number of copies of the software on your devices.
 - b. Included Microsoft Programs. The software contains other Microsoft programs. These license terms apply to your use of those programs.
2. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.
- a. Distributable Code. You are permitted to distribute the software in programs you develop if you comply with the terms below.
 - i. Right to Use and Distribute. The software is "Distributable Code."
 - Distributable Code. You may copy and distribute the object code form of the software. You may not modify the software, and your programs must include a complete copy of the software, including set-up.
 - Third Party Distribution. You may permit distributors of your programs to copy and distribute the Distributable Code as part of those programs.
 - ii. Distribution Requirements. For any Distributable Code you distribute, you must
 - add significant primary functionality to it in your programs;
 - require distributors and external end users to agree to terms that protect it at least as much as this agreement;
 - display your valid copyright notice on your programs;
 - indemnify, defend, and hold harmless Microsoft from any claims, including attorneys' fees, related to the distribution or use of your programs; and
 - if the software is Microsoft SQL Server 2005 Management Studio Express or Microsoft SQL Server 2005 Express Toolkit, distribute it with either:
 - Microsoft SQL Server 2005 Express Edition or
 - Microsoft SQL Server 2005 Express Edition with Advanced Services.
 - iii. Distribution Restrictions. You may not
 - alter any copyright, trademark or patent notice in the Distributable Code;
 - use Microsoft's trademarks in your programs' names or in a way that suggests your programs come from or are endorsed by Microsoft;
 - distribute Distributable Code to run on a platform other than the Windows platform;

- include Distributable Code in malicious, deceptive or unlawful programs; or
 - modify or distribute the source code of any Distributable Code so that any part of it becomes subject to an Excluded License. An Excluded License is one that requires, as a condition of use, modification or distribution, that
 - the code be disclosed or distributed in source code form; or
 - others have the right to modify it.
3. **INTERNET-BASED SERVICES.** Microsoft provides Internet-based services with the software. It may change or cancel them at any time.
 4. **SCOPE OF LICENSE.** The software is licensed, not sold. This agreement only gives you some rights to use the software. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. You may not
 - disclose the results of any benchmark tests of the software to any third party without Microsoft's prior written approval;
 - work around any technical limitations in the software;
 - reverse engineer, decompile or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;
 - make more copies of the software than specified in this agreement or allowed by applicable law, despite this limitation;
 - publish the software for others to copy; or
 - rent, lease or lend the software.
 5. **BACKUP COPY.** You may make one backup copy of the software. You may use it only to reinstall the software.
 6. **DOCUMENTATION.** Any person that has valid access to your computer or internal network may copy and use the documentation for your internal, reference purposes.

7. **TRANSFER TO A THIRD PARTY.** The first user of the software may transfer it and this agreement directly to a third party. Before the transfer, that party must agree that this agreement applies to the transfer and use of the software. The first user must uninstall the software before transferring it separately from the device. The first user may not retain any copies.
8. **EXPORT RESTRICTIONS.** The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.
9. **SUPPORT SERVICES.** Because this software is "as is," we may not provide support services for it.
10. **ENTIRE AGREEMENT.** This agreement, and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the software and support services.
11. **APPLICABLE LAW.**
 - a. **United States.** If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.
 - b. **Outside the United States.** If you acquired the software in any other country, the laws of that country apply.
12. **LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.
13. **DISCLAIMER OF WARRANTY. THE SOFTWARE IS LICENSED "AS-IS." YOU BEAR THE RISK OF USING IT. MICROSOFT GIVES NO EXPRESS WARRANTIES, GUARANTEES OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS,**

MICROSOFT EXCLUDES THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

14. LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. \$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.

This limitation applies to

- anything related to the software, services, content (including code) on third party Internet sites, or third party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

.Net Framework 2.0

End-User License Agreement

MICROSOFT SOFTWARE SUPPLEMENTAL LICENSE TERMS

MICROSOFT .NET FRAMEWORK 2.0

Microsoft Corporation (or based on where you live, one of its affiliates) licenses this supplement to you. If you are licensed to use Microsoft Windows operating system software (the "software"), you may use this supplement. You may not use it if you do not have a license for the software. You may use a copy of this supplement with each validly licensed copy of the software.

The following license terms describe additional use terms for this supplement. These terms and the license terms for the software apply to your use of this supplement. If there is a conflict, these supplemental license terms apply.

By using this supplement, you accept these terms. If you do not accept them, do not use this supplement. If you comply with these license terms, you have the rights below.

1. **SUPPORT SERVICES FOR SUPPLEMENT.** Microsoft provides support services for this supplement as described at www.support.microsoft.com/common/international.aspx.
2. **MICROSOFT .NET FRAMEWORK BENCHMARK TESTING.** This supplement includes the .NET Framework component of the Windows operating systems (".NET Component"). You may conduct internal benchmark testing of the .NET Component. You may disclose the results of any benchmark test of the .NET Component, provided that you comply with the following terms: (1) you must disclose all the information necessary for replication of the tests, including complete and accurate details of your benchmark testing methodology, the test scripts/cases, tuning parameters applied, hardware and software platforms tested, the name and version number of any third party testing tool used to conduct the testing, and complete source code for the benchmark suite/harness that is developed by or for you and used to test both the .NET Component and the competing implementation(s); (2) you must disclose the date (s) that you conducted the benchmark tests, along with specific version information for all Microsoft software products tested, including the .NET Component; (3) your benchmark testing was performed using all performance tuning and best practice guidance set forth in the product documentation and/or on Microsoft's support web sites, and uses the latest updates, patches and fixes available for the .NET Component and the relevant Microsoft operating system; (4) it shall be sufficient if you make the disclosures provided for above at a publicly available location such as a website, so long as every public disclosure of the results of your benchmark test expressly identifies the public site containing all required disclosures; and (5) nothing in this provision shall be deemed to waive any other right that you may have to conduct benchmark testing. The foregoing obligations shall not apply to your disclosure of the results of any customized benchmark test of the .NET Component, whereby such disclosure is made under confidentiality in conjunction with a bid request by a prospective customer, such customer's application(s) are specifically tested and the results are only disclosed to such specific customer. Notwithstanding any other agreement you may have with Microsoft, if you disclose such benchmark test results, Microsoft shall have

the right to disclose the results of benchmark tests it conducts of your products that compete with the .NET Component, provided it complies with the same conditions above.

MarshallSoft Computing SMTP/POP3 Email Engine

License for Use and Distribution

MarshallSoft Computing, Inc. grants the registered user of SEE4C the right to use one copy of the SEE4C DLL's on a single computer in the development of any software product. The user may not use the library on more than one computer at the same time.

However, the registered DLLs (SEE16.DLL and SEE32.DLL) may be distributed without royalty with the user's compiled application, provided that the value of the keycode is not revealed.

The "student" (\$73.50) registered DLL's may not be distributed under any circumstances, nor may they be used for any commercial purpose.

The "professional" (\$105) registered DLL's may be distributed (without royalty) in object form only, as part of the user's compiled application. The registered DLL's may NOT be distributed as part of any software development system (compiler or interpreter) without our express written permission.

When you register, you will be sent a "key code" which enables access to the registered DLL's. You may NOT distribute or make known this key code.

Registered DLLs do NOT expire. Registered users may download free updates for a period of one year from the date of purchase.

[END]

Jasper Reports version 1.2.0

jTDS version 1.2

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License.

Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an

executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

- b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.
- c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

- a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
 - b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.
8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.
10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.
11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING

THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

iText version 1.3.1

MOZILLA PUBLIC LICENSE Version 1.1

1. Definitions.

1.0.1. "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

- 1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.
- 1.5. "Executable" means Covered Code in any form other than Source Code.
- 1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.
- 1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.
- 1.8. "License" means this document.
- 1.8.1. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.
- 1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:
- A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.
 - B. Any new file that contains any part of the Original Code or previous Modifications.
- 1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.
- 1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.
- 1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant. The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

b) under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

(c) the licenses granted in this Section 2.1(a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant. Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) the licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

(d) Notwithstanding Section 2.2(b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License. The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code. Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made

available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications. You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims. If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs. If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations. Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices. You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must

also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions. You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works. You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they

affect. Such description must be included in the LEGAL file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6.1. New Versions.

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works.

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS,

MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8. TERMINATION.

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declaratory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

(a) such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

(b) any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10. U.S. GOVERNMENT END USERS.

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. MISCELLANEOUS.

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. MULTIPLE-LICENSED CODE.

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the NPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

EXHIBIT A -Mozilla Public License.

``The contents of this file are subject to the Mozilla Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.mozilla.org/MPL/>

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____.
 Portions created by _____ are Copyright (C) _____
 _____. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the _____ license (the "[____] License"), in which case the provisions of [_____] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [____] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting the provisions above and replace them with the notice and other provisions required by the [____] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [____] License."

[NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]

Java Runtime Environment JRE 1.5.0.06

Sun Microsystems, Inc. Binary Code License Agreement for the JAVA SE RUNTIME ENVIRONMENT (JRE) VERSION 6 SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACCEPT THE TERMS OF THE AGREEMENT.

INDICATE ACCEPTANCE BY SELECTING THE "ACCEPT" BUTTON AT THE BOTTOM OF THE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS, SELECT THE "DECLINE" BUTTON AT THE BOTTOM OF THE AGREEMENT AND THE DOWNLOAD OR INSTALL PROCESS WILL NOT CONTINUE.

1. DEFINITIONS. "Software" means the identified above in binary form, any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Sun, and any user manuals, programming guides and other documentation

provided to you by Sun under this Agreement. "Programs" mean Java applets and applications intended to run on the Java Platform, Standard Edition (Java SE) on Java-enabled general purpose desktop computers and servers.

2. LICENSE TO USE. Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of the Supplemental License Terms, Sun grants you a non-exclusive, non-transferable, limited license without license fees to reproduce and use internally Software complete and unmodified for the sole purpose of running Programs. Additional licenses for developers and/or publishers are granted in the Supplemental License Terms.

3. RESTRICTIONS. Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that Licensed Software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun Microsystems, Inc. disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.

4. LIMITED WARRANTY. Sun warrants to you that for a period of ninety (90) days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software. Any implied warranties on the Software are limited to 90 days. Some states do not allow limitations on duration of an implied warranty, so the above may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.

5. DISCLAIMER OF WARRANTY. UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

6. LIMITATION OF LIABILITY. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

7. TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon Termination, you must destroy all copies of Software.

8. EXPORT REGULATIONS. All Software and technical data delivered under this Agreement are subject to US export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you.

9. TRADEMARKS AND LOGOS. You acknowledge and agree as between you and Sun that Sun owns the SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations ("Sun Marks"), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at <http://www.sun.com/policies/trademarks>. Any use you make of the Sun Marks inures to Sun's benefit.

10. U.S. GOVERNMENT RESTRICTED RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government primecontractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is

in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

11. **GOVERNING LAW.** Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

12. **SEVERABILITY.** If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

13. **INTEGRATION.** This Agreement is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

A. **Software Internal Use and Development License Grant.** Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software "README" file incorporated herein by reference, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified for the purpose of designing, developing, and testing your Programs.

B. **License to Distribute Software.** Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README file, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i)

you distribute the Software complete and unmodified and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software, (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

C. Java Technology Restrictions. You may not create, modify, or change the behavior of, or authorize your licensees to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation.

D. Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

E. Third Party Code. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party open-source/freeware license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions in paragraphs 5 and 6 of the Binary Code License Agreement shall apply to all Software in this distribution.

F. Termination for Infringement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right.

G. Installation and Auto-Update. The Software's installation and auto-update processes transmit a limited amount of data to Sun (or its service provider) about those specific processes to help Sun understand and optimize them. Sun does not associate the data with personally identifiable information. You can find more information about the data Sun collects at <http://java.com/data/>.

For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.



INDEX

-
- A**
- Active hosts [4-12](#)
 - Add rule [4-14](#)
 - Administrator
 - local or LDAP authentication [4-3](#)
 - roles [4-3](#)
 - Agent
 - kits [4-7](#)
 - optional reboot after install [A-3](#)
 - registration [4-7](#)
 - user interface [A-4](#)
 - Agent (Linux)
 - installing [A-8](#)
 - Agent (Solaris)
 - installing [A-6](#)
 - migrating from V4.x [3-43](#)
 - Agent installation automatic [3-31](#)
 - Agent kit [4-7](#)
 - make [4-8](#)
 - preconfigured sample [4-5, 4-7, 4-18](#)
 - Agent migration [3-42](#)
 - Agent-server size ratio [2-4](#)
 - Application class [4-16](#)
 - Attach policy to group [4-19](#)
 - Attach rule module to policy [4-19](#)
-
- B**
- Browser requirements [1-9](#)
 - Build an agent kit [4-7](#)
-
- C**
- Certificate import [3-44, 3-48](#)
 - Cisco Security Agent on remote database [3-22](#)
 - Cisco Trust Agent (CTA) [3-50](#)
 - installation files [3-50](#)
 - Cluster support [1-11](#)
 - Content engine [2-5](#)
 - CSA MC [1-3](#)
 - about [1-2](#)
 - browser requirements [1-9](#)
 - environment requirements [1-9](#)
 - login locally [3-39](#)
 - login remotely [3-39](#)
 - Policies [4-4](#)
 - system requirements [1-3](#)

D

- Deployment overview [1-2](#)
- Detailed description [4-4](#)
- Distributed configuration [3-38](#)
- DNS environments [1-9](#)

F

- File access control rule [4-14](#)
- FireFox
 - version support [1-10](#)
- Force reboot after install [4-8](#)

G

- Generate rules [4-20](#)
- Generating configurations [4-20](#)
- Group
 - configure [4-5, 4-18](#)
 - Polling intervals [4-6](#)
 - preconfigured sample [4-5, 4-18](#)
 - Test Mode [4-6](#)
 - Verbose logging mode [4-6](#)
- Groups
 - No user interaction [A-4](#)

H

- Hosts
 - about [4-5](#)
 - active [4-12](#)
 - not active [4-12](#)
 - search [4-12](#)
 - view [4-12](#)
- HTTPS [1-8, A-2](#)

I

- Import migration data [3-42](#)
- Import Root Certificate [3-44](#)
- Inactive hosts [4-12](#)
- Install
 - agent [A-2](#)
 - certificate (IE) [3-44](#)
 - Microsoft SQL Server [3-11](#)
- Installation Log [3-38](#)
- Installation options [3-6](#)
- Install CSA MC [3-39](#)
 - installation options [3-6](#)
 - license information [3-2](#)
 - local database [3-8](#)
 - remote database [3-21](#)
- Internationalization support [1-11](#)
 - Windows 2000 [1-13](#)
 - Windows 2003 [1-15](#)

Windows XP [1-14](#)
 Internet Explorer
 version support [1-9](#)

L

Licensing import information [3-18, 3-31](#)
 Licensing information [3-2](#)
 Local database install [3-6](#)
 Log
 installation [3-38](#)
 Login
 locally [3-39](#)
 remotely [3-39](#)

M

Make kit [4-8](#)
 Migrate to CSA MC, new version [3-40](#)
 migration_data_export.xml [3-41](#)

N

Not active hosts [4-12](#)
 No user interaction [A-4](#)

O

Operating system changes, agent [1-9](#)

Operating systems sample [2-2](#)
 Overview of product [1-1](#)

P

Pilot
 recommendations [2-2](#)
 Pilot Program
 size of pilot [2-2](#)
 time frame of pilot [2-3](#)
 Policies
 pre-configured modules [4-4](#)
 Policy
 add rule [4-14](#)
 attach to group [4-19](#)
 configure [4-12](#)
 distribute to agents [4-20](#)
 exception rules [2-13](#)
 file access control [4-14](#)
 modify policy associations [4-19](#)
 modify rules [4-14](#)
 query responses [2-12](#)
 rule modules [4-13](#)
 Test Mode as a tool [2-10](#)
 tuning and troubleshooting [2-7](#)
 Polling interval recommendation [2-5](#)
 Polling intervals [4-6](#)
 prepare__migration.exe [3-41](#)
 Product overview [1-1](#)

Q

Quick start setup [4-1](#)

R

Reboot optional

agent [A-2, A-3](#)

Registered hosts

view [4-12](#)

Remote access [3-39, 4-2](#)

Remote database install [3-7](#)

Requirements

agent [1-5](#)

cluster support [1-11](#)

DNS and WINS [1-9](#)

port availability [1-10](#)

server [1-3](#)

time and date settings [1-10](#)

web browsers [1-9](#)

Resolution

screen requirements [1-4](#)

Root certificate import [3-44, 3-48](#)

Rule configuration version [4-21](#)

S

Scalability

hardware sizing [2-3](#)

server configurations [2-3](#)

Scalable deployment [2-3](#)

configuration recommendations [2-5](#)

content engines [2-5](#)

hardware sizing [2-3](#)

polling interval [2-5](#)

software considerations [2-5](#)

three servers [2-3](#)

Secure communications [3-44](#)

Single server [2-3](#)

Software updates

Force reboot [4-8](#)

Solaris agent install directory [A-7](#)

Solaris host migration [3-43](#)

Solaris requirements

agent [1-7](#)

SQL Server 2000 install [3-20](#)

SQL Server 2005 and 2000 install [3-19](#)

SQL Server 2005 and 2000 setup [3-22](#)

SQL Server express installation [3-8, 3-20](#)

SSL [3-44](#)

System requirements [1-3](#)

T

Terminal services [1-5](#)

Test Mode [4-6](#)

Three servers, multi-tiered [2-3](#)

Time settings

remote db and CSA MC system [3-21](#)

Two servers [2-3](#)

U

Uninstall CSA MC [3-49](#)

UNIX agent install directory [A-7](#)

Upgrade naming conventions [3-42](#)

V

Verbose logging mode [4-6](#)

Version labels [3-42](#)

W

Web-based user interface [1-2, 1-17](#)

Web browser

requirements [1-9](#)

Windows Cluster support [1-11](#)

Windows requirements

agent [1-5](#)

WINS environments [1-9](#)

