Installing Management Center for Cisco Security Agents 5.1

Updated: October 13, 2008

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-78-17557

CONTENTS

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, 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.
Italicized text	Used to *emphasize* text.	You must *save* 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. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

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

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from 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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—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.
- 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 to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked 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.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation 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 Technical Support & Documentation Website

The Cisco Technical Support & Documentation 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/techsupport

Access to all tools on the Cisco Technical Support & Documentation 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 Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI 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.

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)—Your 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 operation 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 your network is impaired, but 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.

- 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

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication

identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

http://www.cisco.com/go/iqmagazine

or view the digital edition at this URL:

http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems 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 Systems, 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 for networking professionals to 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

- 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.

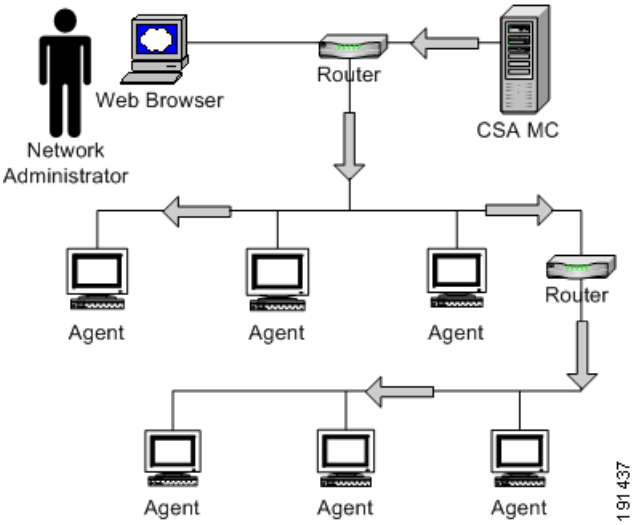
Cisco Security Agent Overview

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 500 agents. If you are planning to deploy CSA MC with more than 500 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	• 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
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 MSDE with Service Pack 4. If the CSA MC installation detects any other database type attached to an existing installation of MSDE, the installation will abort. This database configuration is not supported.
- If MSDE Service Pack 2 or earlier is present on the system, you must uninstall that version of MSDE or upgrade it before proceeding further.

  If you are planning to deploy no more than 500 agents, the shipped version of Microsoft SQL Server Desktop Engine should be adequate. For a larger deployment, you also have the option of installing Microsoft SQL Server 2000 instead of using the Microsoft SQL Server Desktop Engine that is provided. Note that of you are using SQL Server 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	• 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: • 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	25 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	25 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 3.0 WS, ES, or AS
Memory	256 MB minimum
Hard Drive Space	25 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.

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
	Windows 2003	Yes	Yes
Japanese	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes

Language	Operating System	Localized	Qualified
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)
Greek	S	NA	NA
Hebrew	NS	NA	NA
Hungarian	S	S	NA
Italian	L	L(S)	NA

	Professional	Server	Advanced Server
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)
Greek	S	S
Hebrew	NS	NS
Hungarian	S	S
Italian	L	L(S)

	Professional	Home
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)
Polish	T	T	T
Portuguese	S	S	S
Russian	S	S	S
Spanish	L	L(S)	L(S)

	Standard	Web	Enterprise
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.

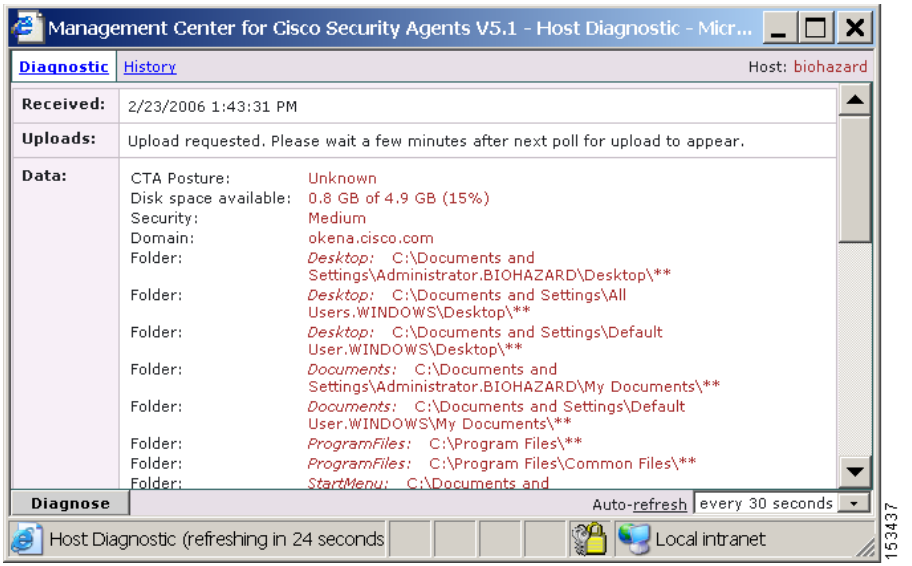
Step 2 Click the link to the host name using the language you want to verify.

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

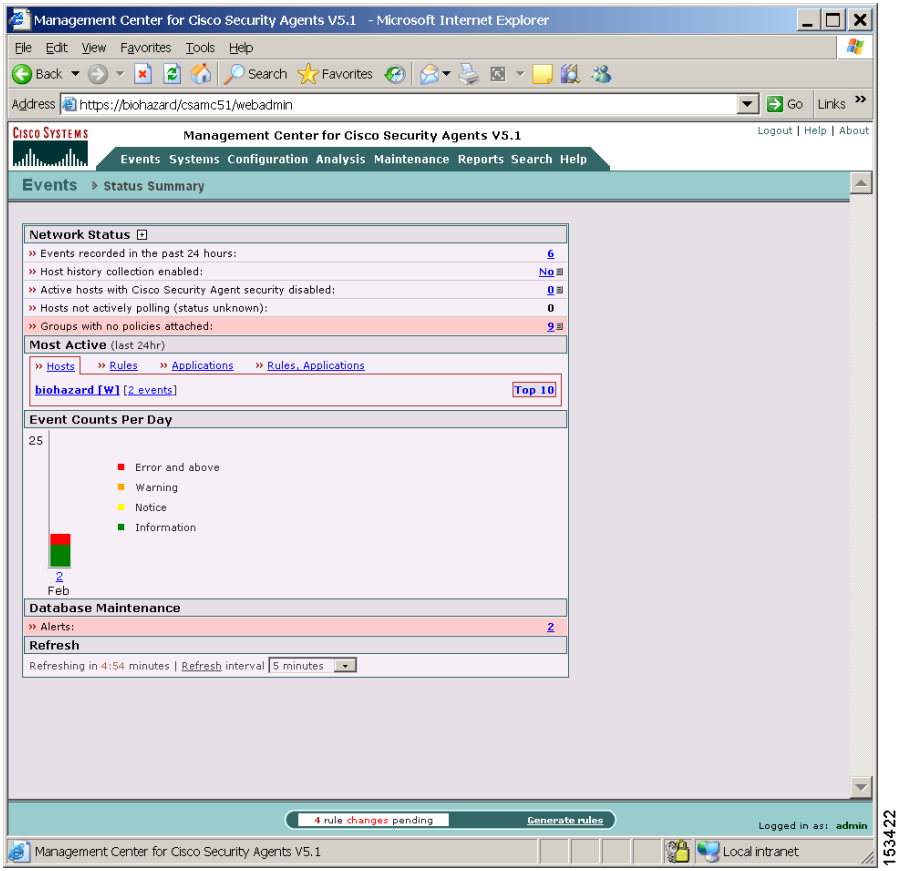


About CSA MC

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

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 is 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 CSAMC 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 500 agents, you should use Microsoft SQL Server 2000 in lieu of MSDE. Only Hardware Configuration 1 supports Microsoft SQL Server 2000 Workgroup or Standard editions with their 2GB RAM limitation.
- The Microsoft SQL Server 2000 should be patched to Service Pack 4. Later service packs for SQL Server are not qualified.

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.

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

The Management Center for Cisco Security Agents product CD and product download contains a license key which is imported automatically 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.

Installation Overview

Caution This Management Center for Cisco Security Agents V5.1 release is intended for new installations. You cannot upgrade to V5.1 from a previous version of the product.

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.

Installation Configuration Options

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 Desktop Engine (provided with the product) on the same system if you are planning to deploy no more than 500 agents. In this case, the CSA MC installation also installs its own version of Microsoft SQL Server Desktop Engine on the system.

  For a local database configuration, you also have the option of installing Microsoft SQL Server 2000 instead of using the Microsoft SQL Server Desktop Engine that is provided. Microsoft SQL Server Desktop Engine has a 2 GB database size limit. In this case, you can have CSA MC and Microsoft SQL Server 2000 on the same system depending on the number of agents you are deploying (see Scalable Deployments, page 2-3). Note that of you are using SQL Server 2000, it must be licensed separately and it must be installed on the system before you begin the CSA MC installation.

  Also note that if your plan is to use SQL Server 2000, it is recommended that you choose one of the other installation configuration options rather than the local database configuration.

- 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 2000 Remote Setup, page 3-17.)

  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 2000 database, SQL Server 2000 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 2000 Remote Setup, page 3-17.)

  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 2000 database. SQL Server 2000 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, you will first install Microsoft SQL Server Desktop Engine (as part of the CSA MC installation) and then install CSA MC.

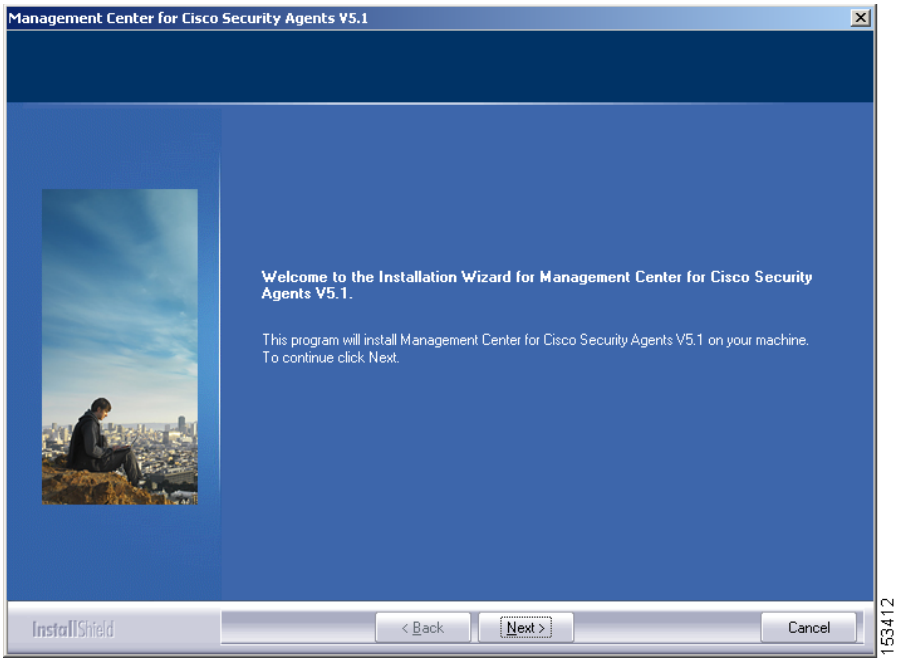
Before beginning, exit any other programs you have running on the system where you are installing CSA MC.

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. See Figure 3-1. (If the installation does not start automatically, browse to the setup.exe file on the CD and double click to begin the installation.)

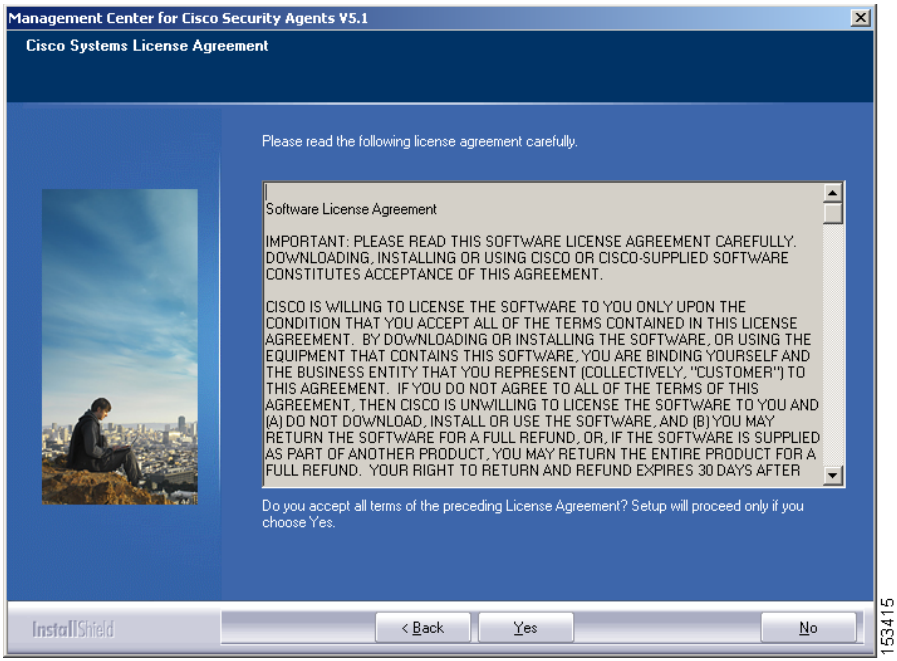
Figure 3-1 CSA MC Installation Welcome Screen



Step 3 After you click **Next** in the welcome screen, various system checks are performed before the system installation continues.

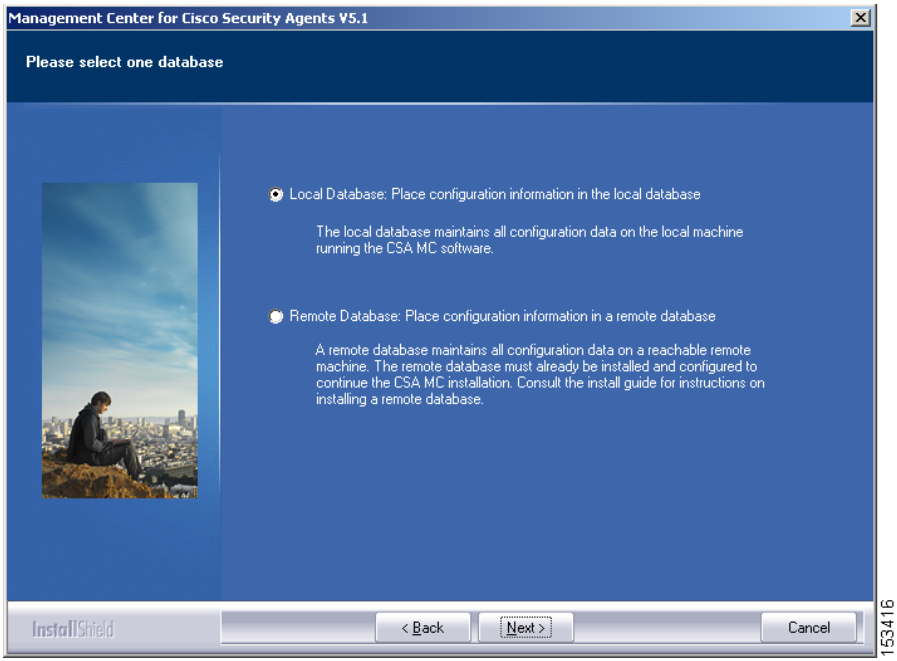
Step 4 When the initial system checks are complete, you are prompted to accept the license agreement. Accept the agreement by clicking **Yes**. See Figure 3-2.

Figure 3-2 CSA MC EULA License Agreement



Step 5 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 3-3.

Figure 3-3 Database Setup Type

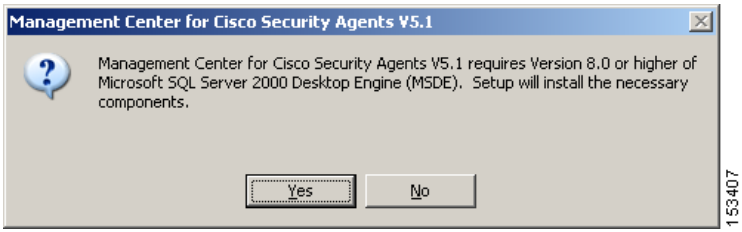


Step 6 If installing locally, the installation next checks to see if you have Microsoft SQL Server Desktop Engine (MSDE) installed. CSA MC uses MSDE for its local configuration database. If this software is not detected, you are prompted to install it. See Figure 3-4.

Note For installations exceeding 500 agents, it is recommended that you install Microsoft SQL Server 2000 instead of using the Microsoft SQL Server Desktop Engine that is provided with the product. Refer to Installation Configuration Options, page 3-3 for more information. If you are using Microsoft SQL Server 2000, refer to Microsoft SQL Server 2000 Local Installation Notes, page 3-15 for details.

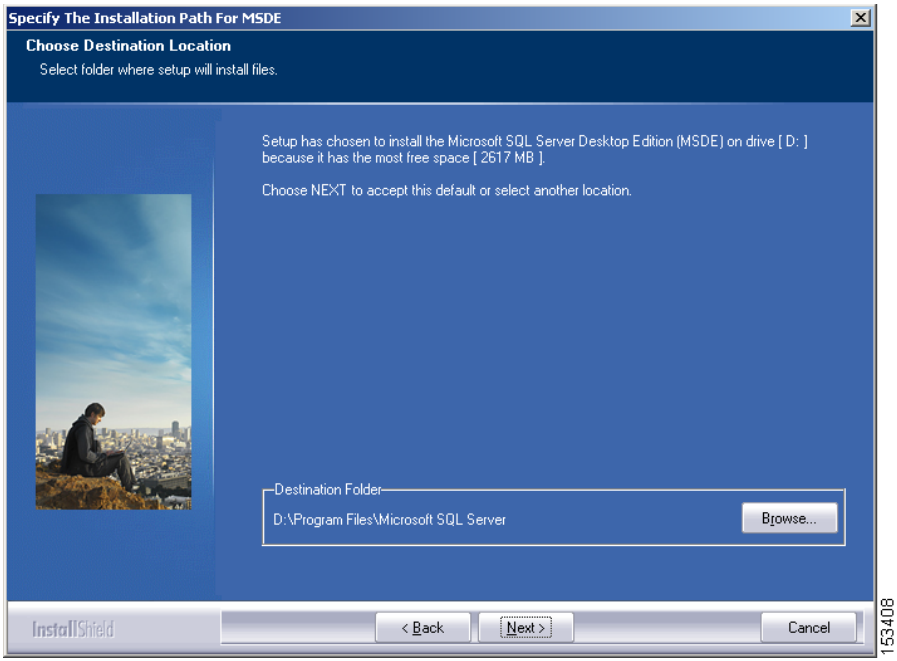
Caution On a system where CSA MC has not previously been installed, the setup program first installs MSDE. If the CSA MC installation detects any other database type attached to an existing installation of MSDE or a version of MSDE or SQL Server 2000 that does not have at least Service Pack 4, the installation will abort. This database configuration is not qualified.

Figure 3-4 Install MSDE Prompt



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

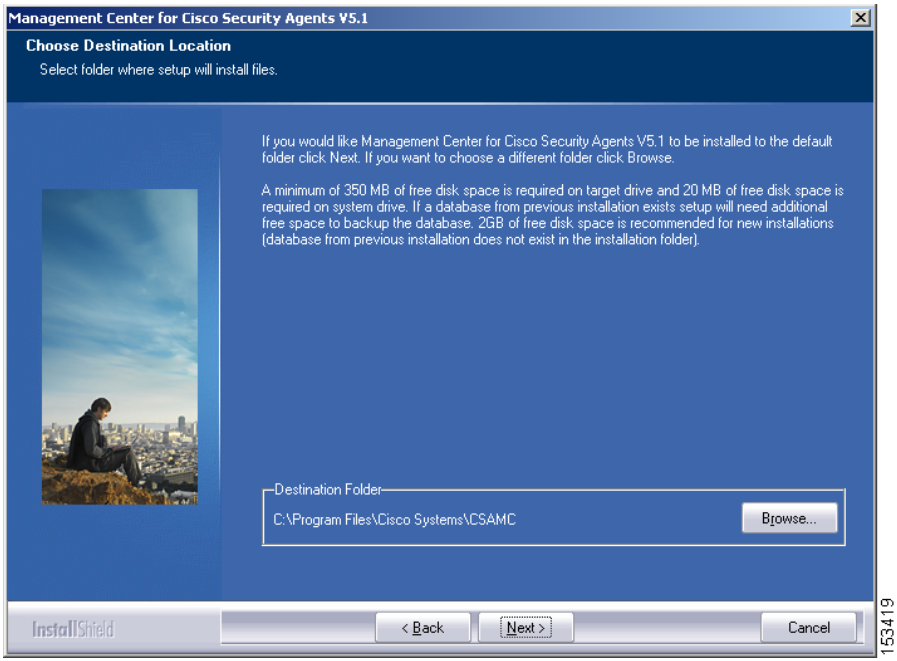
Figure 3-5 MSDE Installation Directory Selection



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

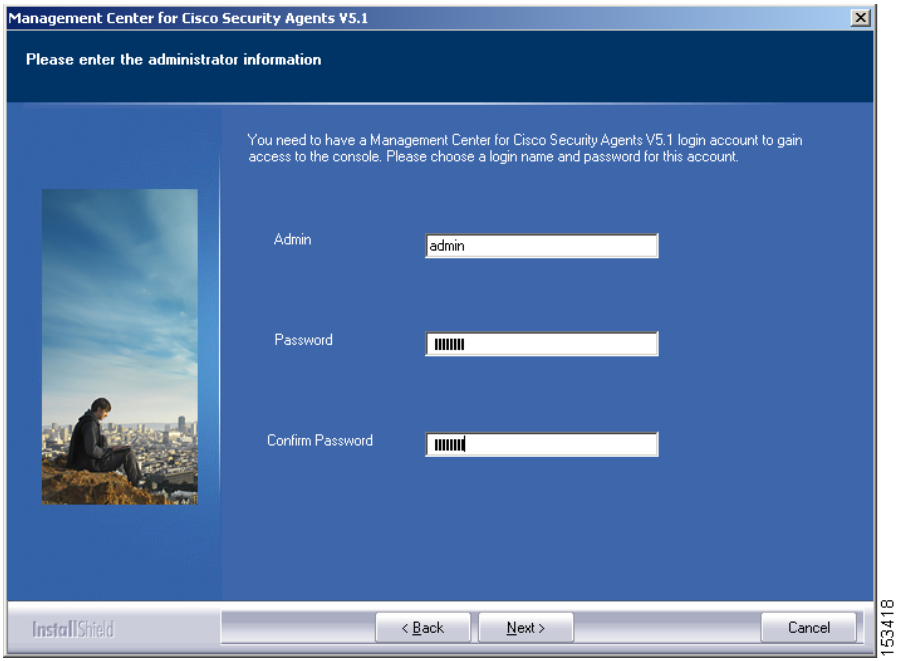
Step 7 You are prompted to select a CSA MC directory installation path. If you would like to restore a previously backed up CSA MC database, you are prompted to restore that database at this time. Either accept the default installation path or browse to a different path to restore an database backup.

Figure 3-6 Directory Prompt



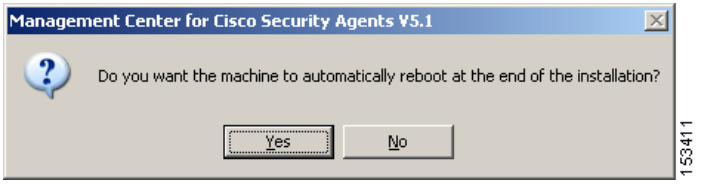
Step 8 You are next prompted to enter Administrator Name and Password information. This the user name and password you will use to login in to CSA MC. See Figure 3-7. Enter this information and click **Next**.

Figure 3-7 Enter Administrator Name and Password



Step 9 You are next prompted to select whether or not you want the system to automatically reboot once the installation is complete (see Figure 3-8). 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 3-8 Automatic Reboot Option Prompt



You are next prompted to begin the installation (see Figure 3-9). The install then proceeds copying the necessary files to your system (see Figure 3-10).

Figure 3-9 Installation Prompt

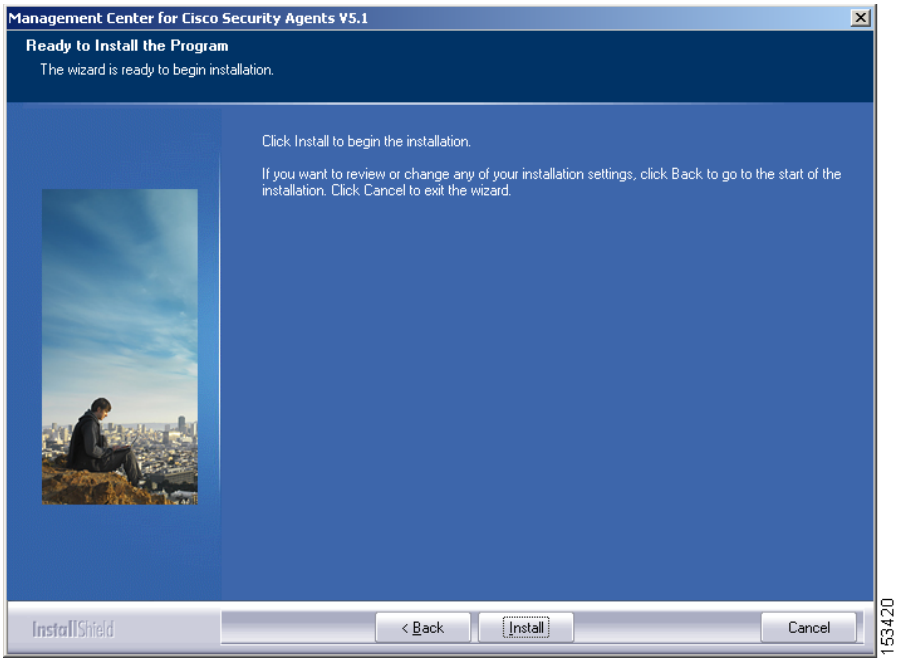
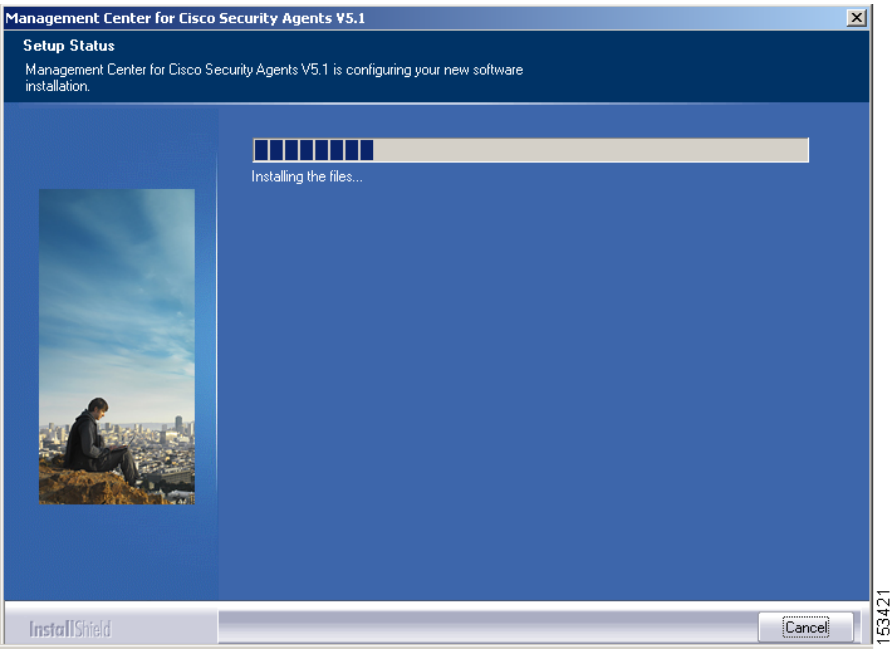
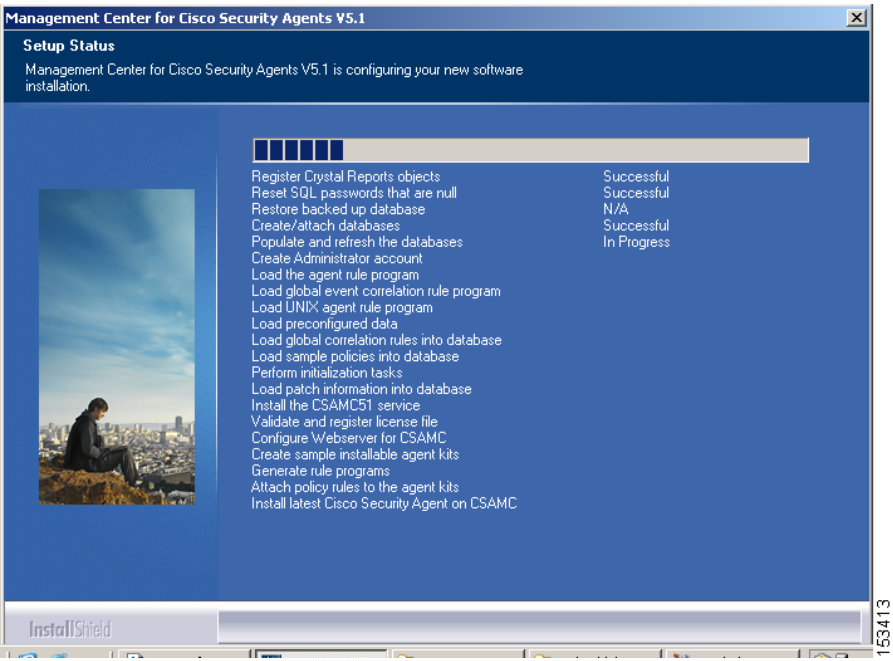


Figure 3-10 Copy Files



Once all the files are copied, the installation performs some preliminary system setup tasks (see Figure 3-11).

Figure 3-11 Installation Progress



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 2000 Local Installation Notes

Note The following instructions are only intended for administrators choosing to install CSA MC and Microsoft SQL Server 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 2000 as a remote database, information is provided in the section titled Installing CSA MC with a Remote Database, page 3-16.

For local database installations exceeding 500 agents, it is recommended that you install Microsoft SQL Server 2000 instead of using the Microsoft SQL Server Desktop Engine that is provided with the product. Microsoft SQL Server Desktop Engine has a 2 GB limit. SQL Server 2000 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 2000 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 2000 manual for detailed installation information.)

Note You should not change the default instance name of "MSSQLSERVER" for the SQL Server 2000 database. If you change this, the CSA MC installation will not detect the database.

When installing Microsoft SQL Server 2000, 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.
- 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.

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.

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 2000 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. Additionally, 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 2000, 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 2000 Remote Setup

Note The following section contains overview information for setting up the Microsoft SQL Server 2000 database to work correctly with CSA MC. More detailed SQL Server configuration information should be obtained from your Microsoft documentation.

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.)
- 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 "CSAMC51".

Step 4 Inside the DB properties, click **Data Files** and in the **File Name** box, type "csamcalanysis", 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 = csamc51 database.

Note Do not click anything under "server roles".

Step 6 In the "database access" section, permit access to csamc51 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:

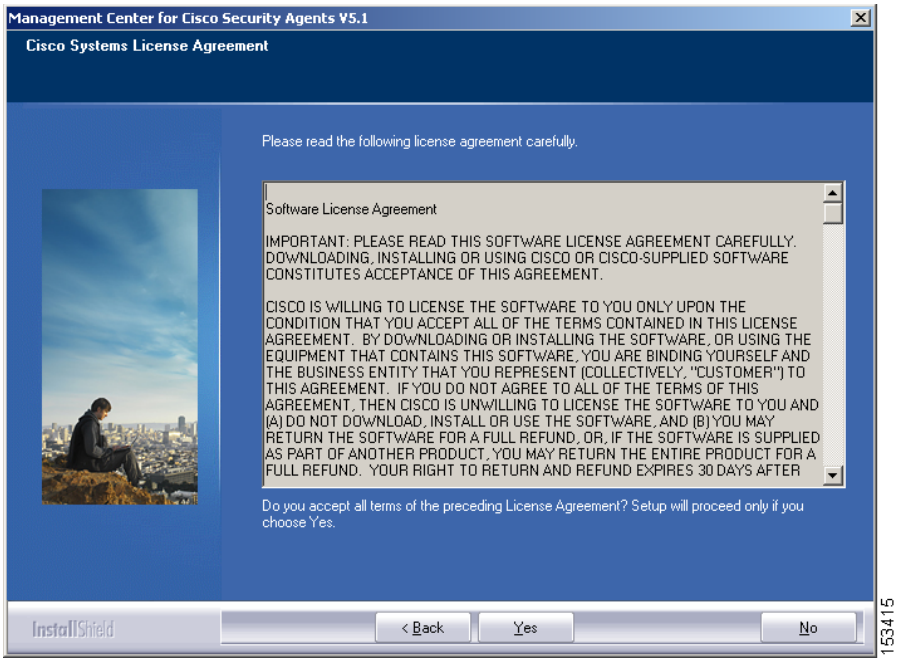
Step 1 Log on as a local Administrator on your Microsoft Server Windows 2003 R2 Standard or Enterprise system.

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 3-12.

Figure 3-12 CSA MC EULA License Agreement

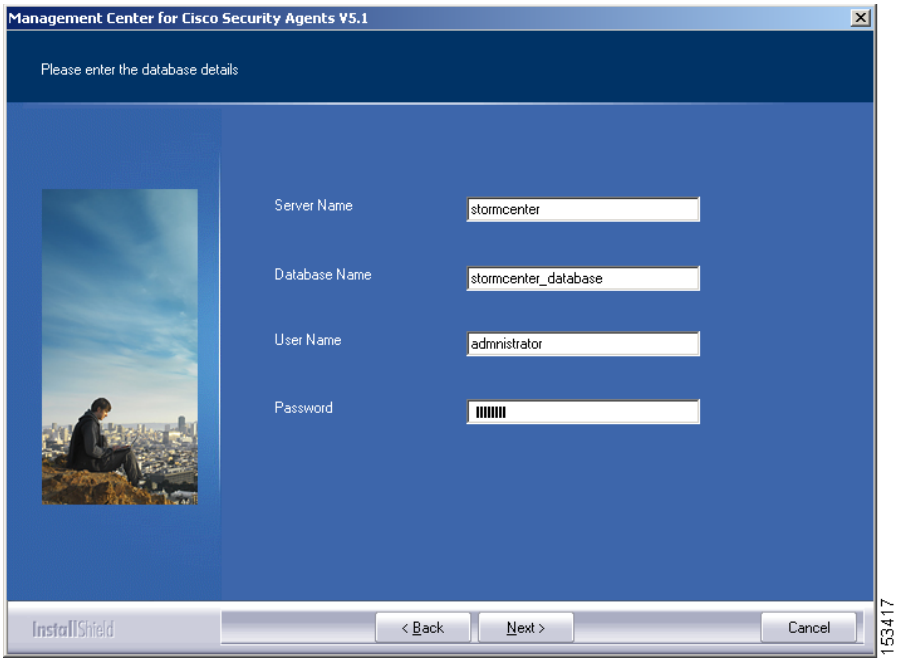


Step 5 The install begins by prompting you to choose a database setup type. In this case, you will select the **Remote Database** radio button and click the **Next** button.

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 3-13):

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

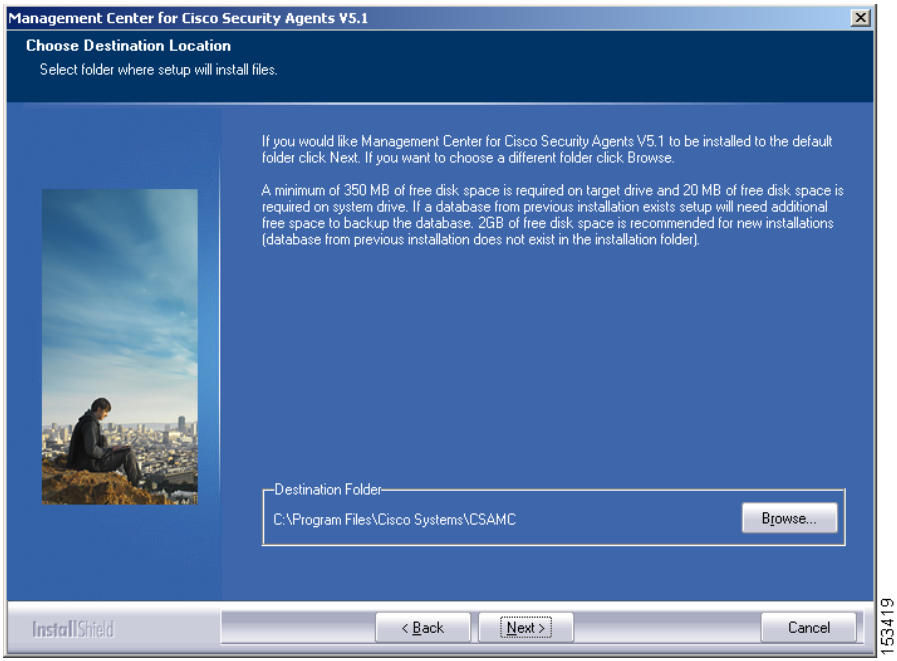
Figure 3-13 Remote Database Information



Step 6 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.

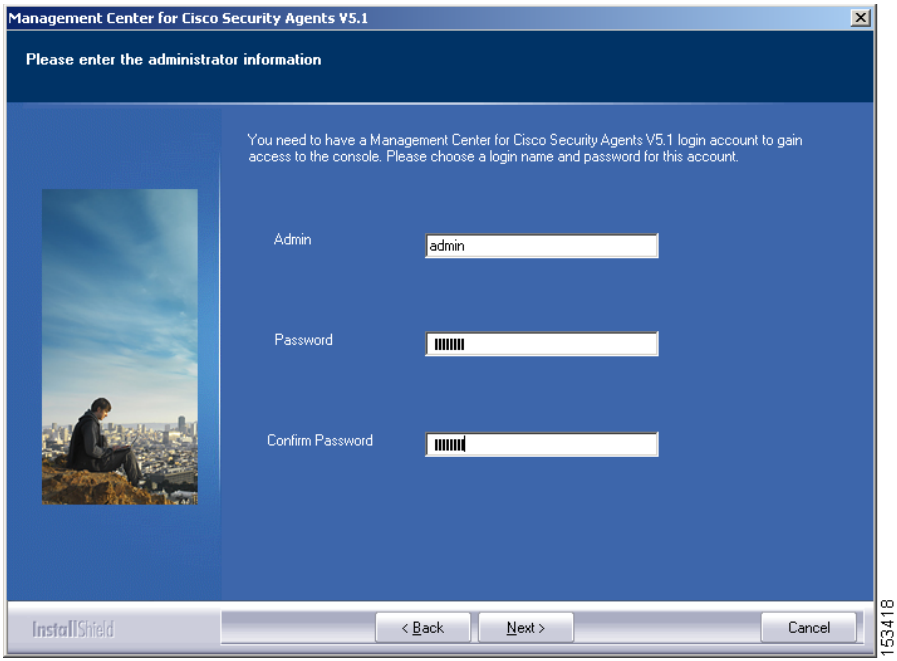
Step 7 You are next prompted to select a CSA MC directory installation path. Either accept the default installation path or browse to a different path. See Figure 3-14.

Figure 3-14 Directory Prompt



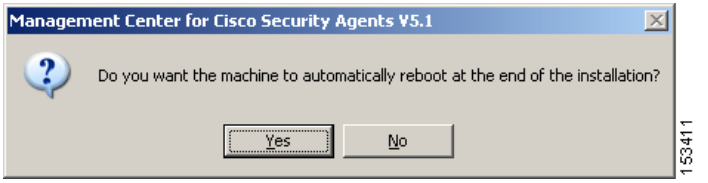
Step 8 You are next prompted to enter Administrator Name and Password information. This the user name and password you will use to login in to CSA MC. See Figure 3-15. Enter this information and click **Next**.

Figure 3-15 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 3-16). 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 3-16 Automatic Reboot Option Prompt



You are next prompted to begin the installation (see Figure 3-17). The install then proceeds copying the necessary files to your system (see Figure 3-18).

Figure 3-17 Installation Prompt

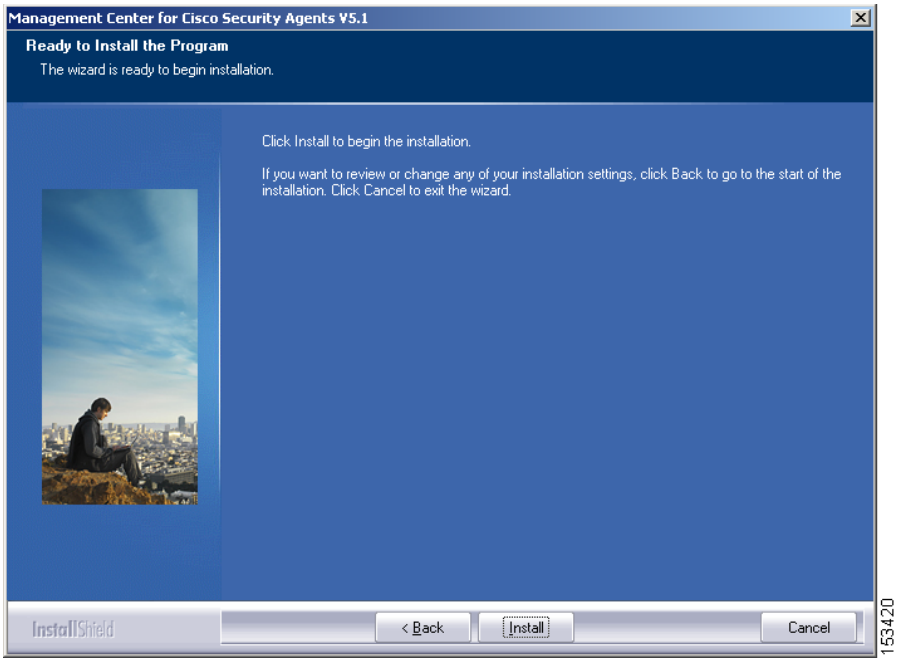
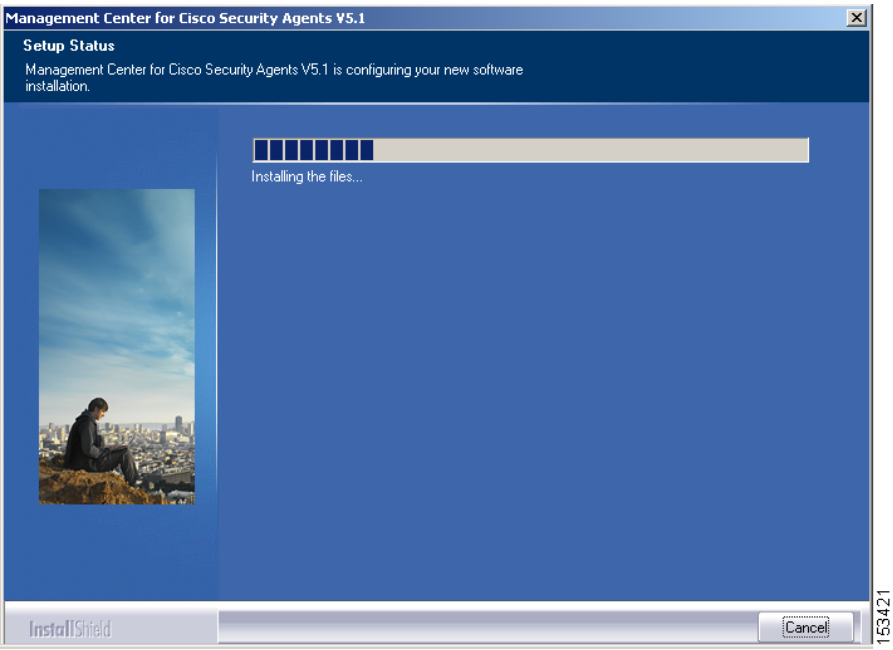


Figure 3-18 Copy Files



Once all the files are copied, the installation performs some preliminary system setup tasks.

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.

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 \CSAMC51\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 3-27 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:

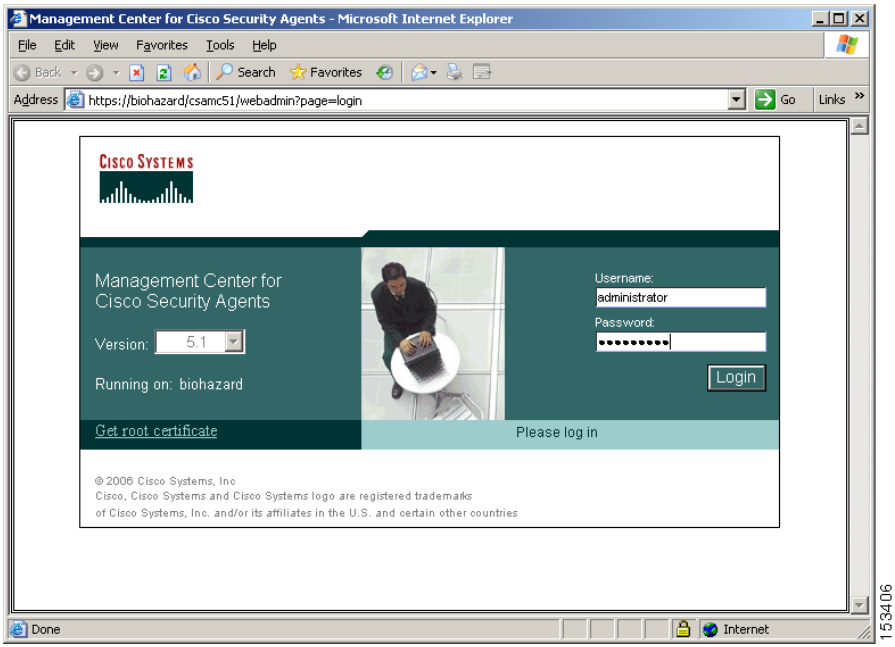
  `http://<management center system hostname>.<domain>`

  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 3-19 CSA MC Login Window



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.

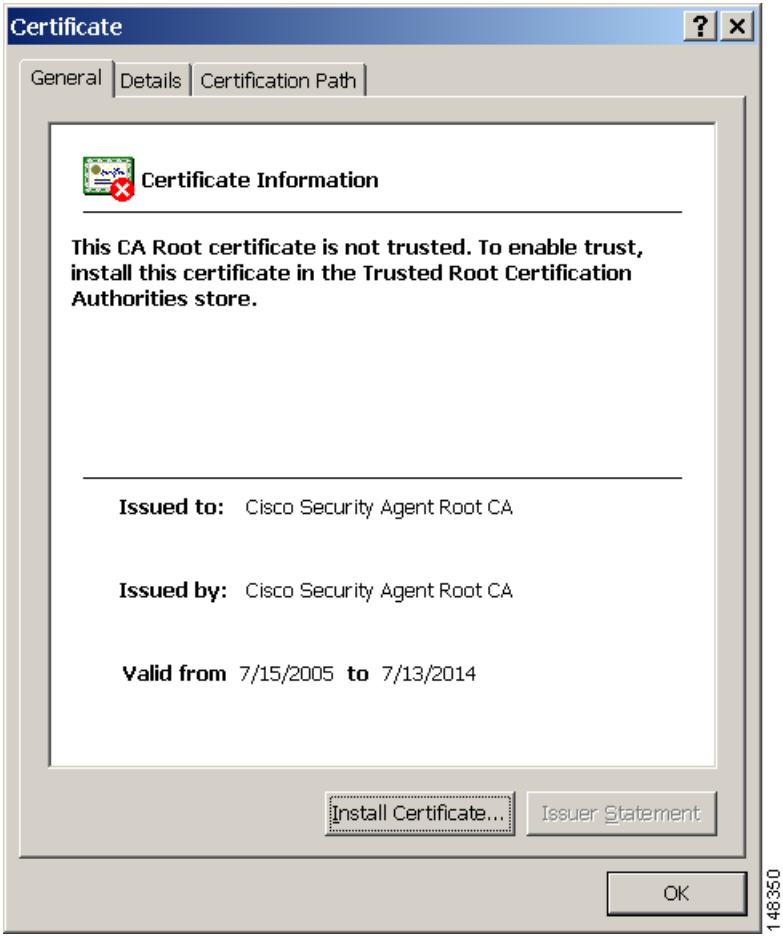
Internet Explorer: Importing the Root Certificate

Step 1 You import the certificate from the CSA MC login window. Click the **Get root certificate** link. See Figure 3-19.

Step 2 Select the **Open** (this file from its current location) button and click **OK**.

Step 3 The certificate information box appears (see Figure 3-20). 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.

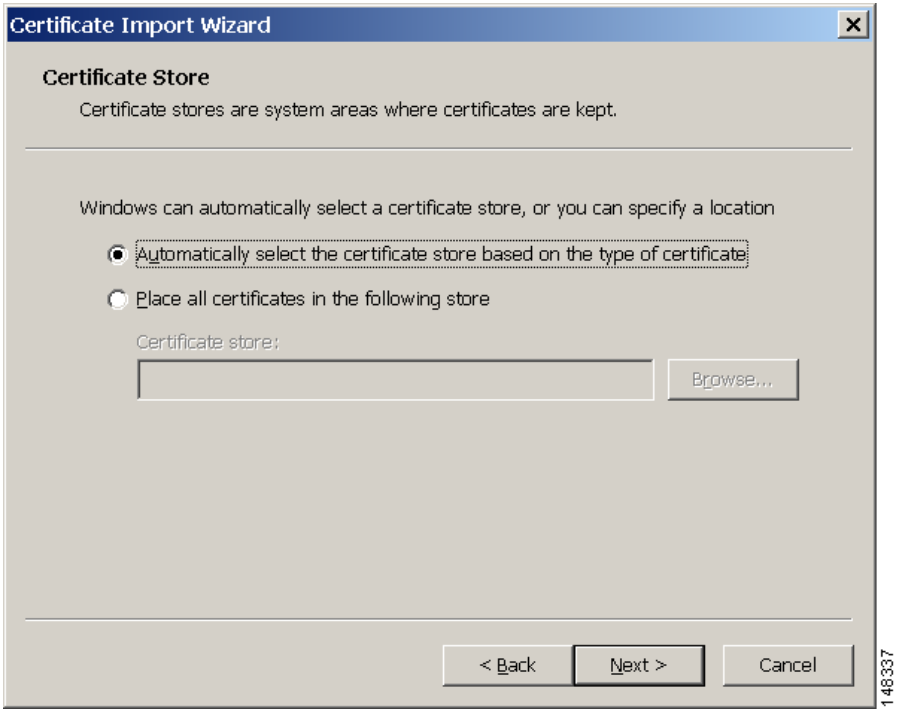
Figure 3-20 Certificate Information



Step 4 The first Certificate Manager Import page contains an overview of certificate information. Click **Next** to continue.

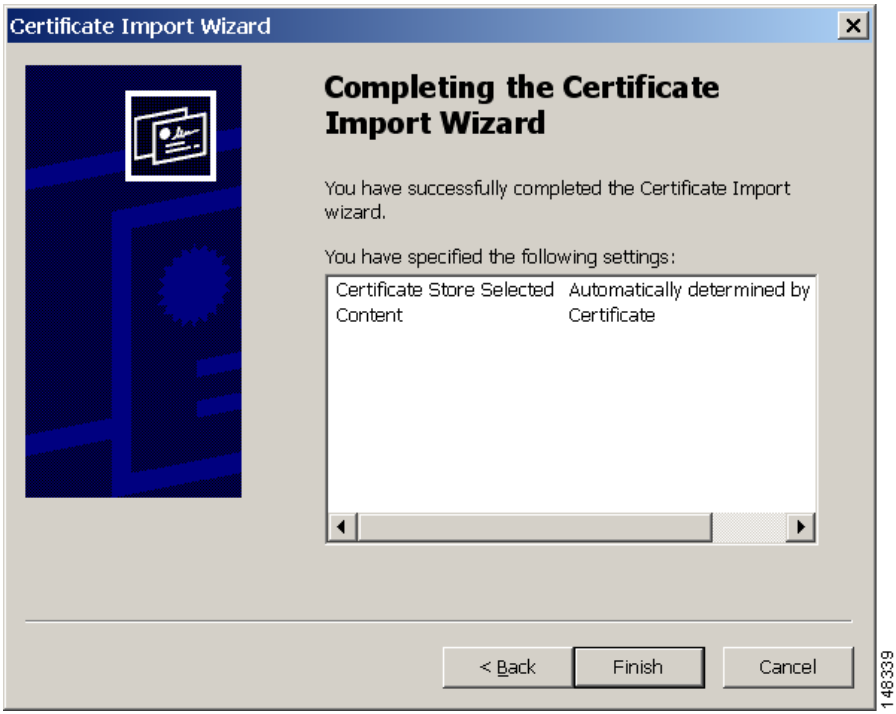
Step 5 From the Select a Certificate Store page, make sure the **Automatically select the certificate store based on the type of certificate** radio button is selected. Click **Next**.

Figure 3-21 Certificate Wizard



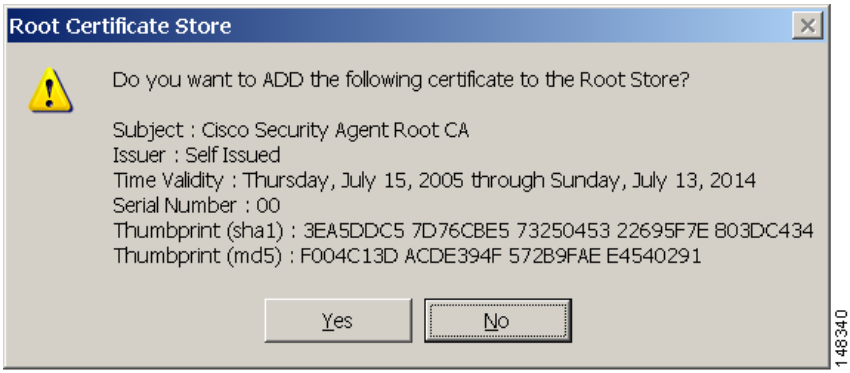
Step 6 You've now imported your certificate for the server. Click the **Finish** button (Figure 3-22) to continue.

Figure 3-22 Certificate Wizard Finish Page



Step 7 Now, you must save the certificate. Click the **Yes** button in the Root Certificate Store box (see Figure 3-23).

Figure 3-23 Root Certificate Store Box



Step 8 You are next prompted with a confirmation box informing you that your certificate was created successfully. Lastly, the View Certificate box remains on the screen (see Figure 3-20). Since your certificate has been generated, you can click the **Yes** button here.

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.

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.

To copy the CTA installer files, follow this procedure:

Step 1 Obtain the desired CTA installer files from Cisco Systems.

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%\CSAMC51\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

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 on 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.

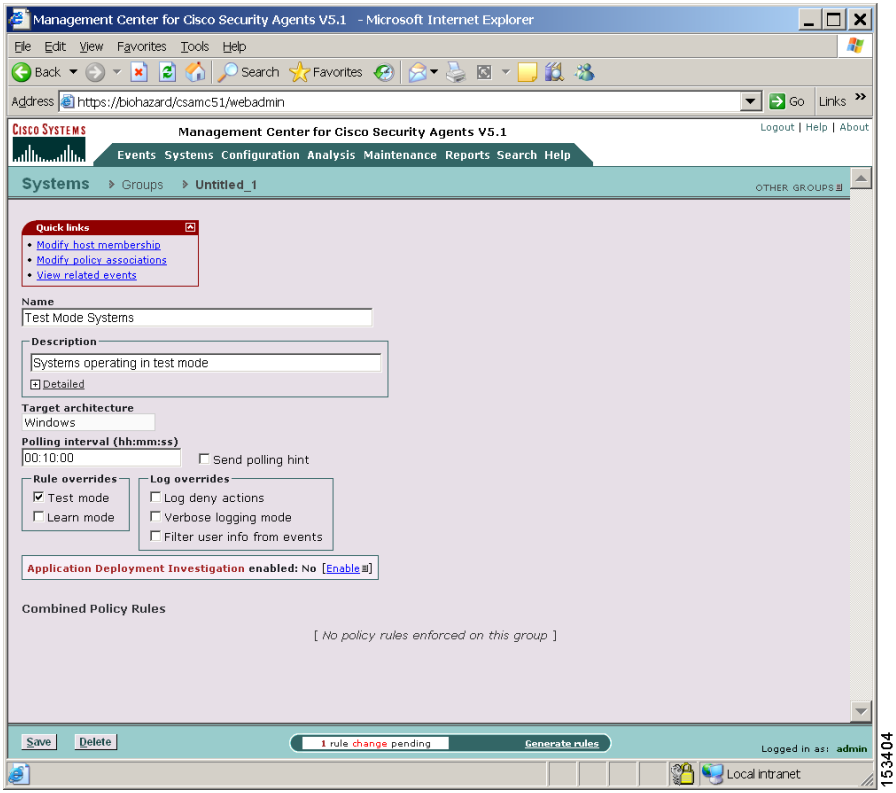
Step 1 Move the mouse over **Systems** in the menu bar of CSA MC and select **Groups** from the drop-down menu that appears. The Groups list view appears.

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).

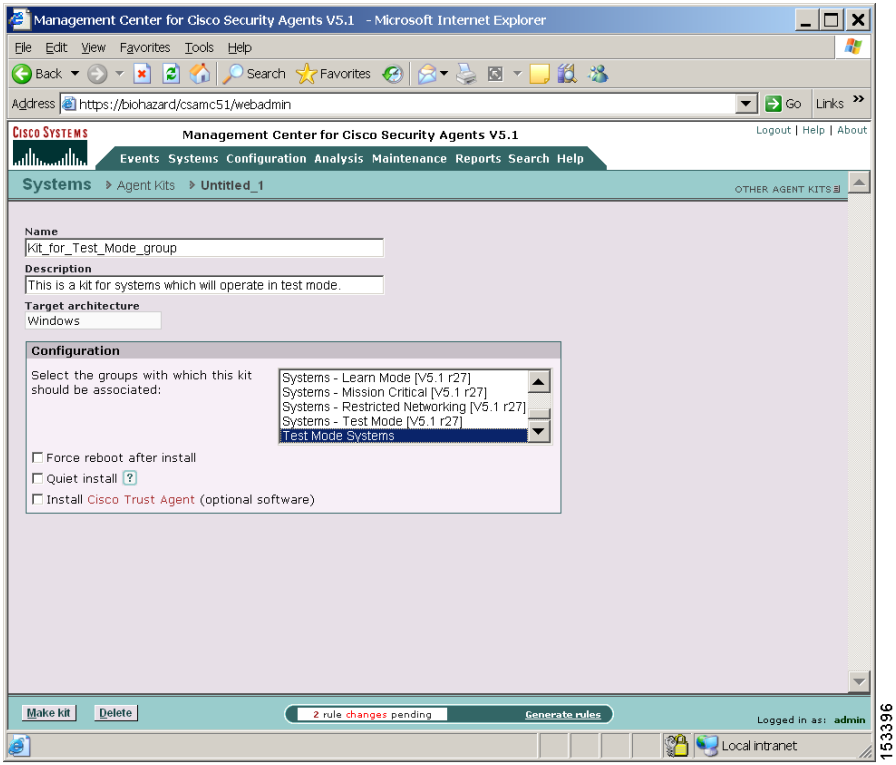
Step 4 Enter a **Description**. This is an optional line of text that is displayed in the agent kit list view.

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.

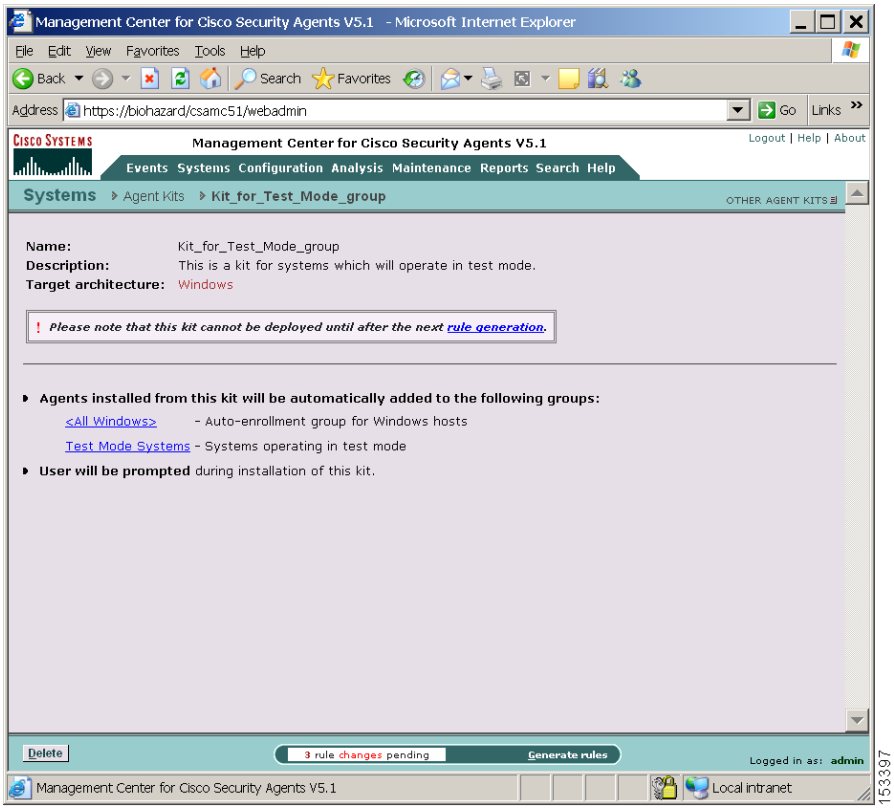
But you may also point users to a URL for the CSA MC system. This URL will allow them to see all kits that are available. That URL is:

```
https://<system name>/csamc51/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>/csamc51/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 this kits URL.

Figure 4-3 Download Agent Kits



The Cisco Security Agent

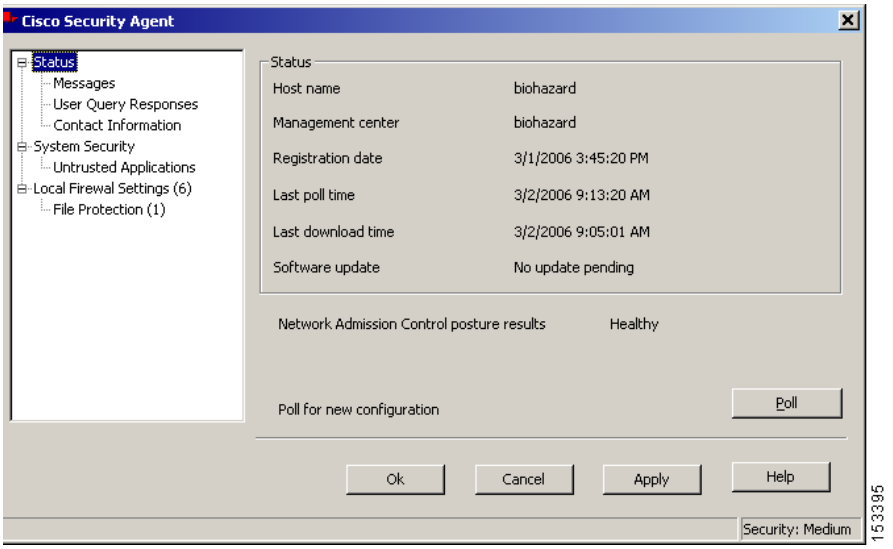
- Users must have administrator privileges on their systems to install the Cisco Security Agent software.
- The Cisco Security Agent installs on supported Windows, Linux, and Solaris platforms. (Note that on Solaris systems there is no agent user interface. See Appendix A in the User Guide for information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

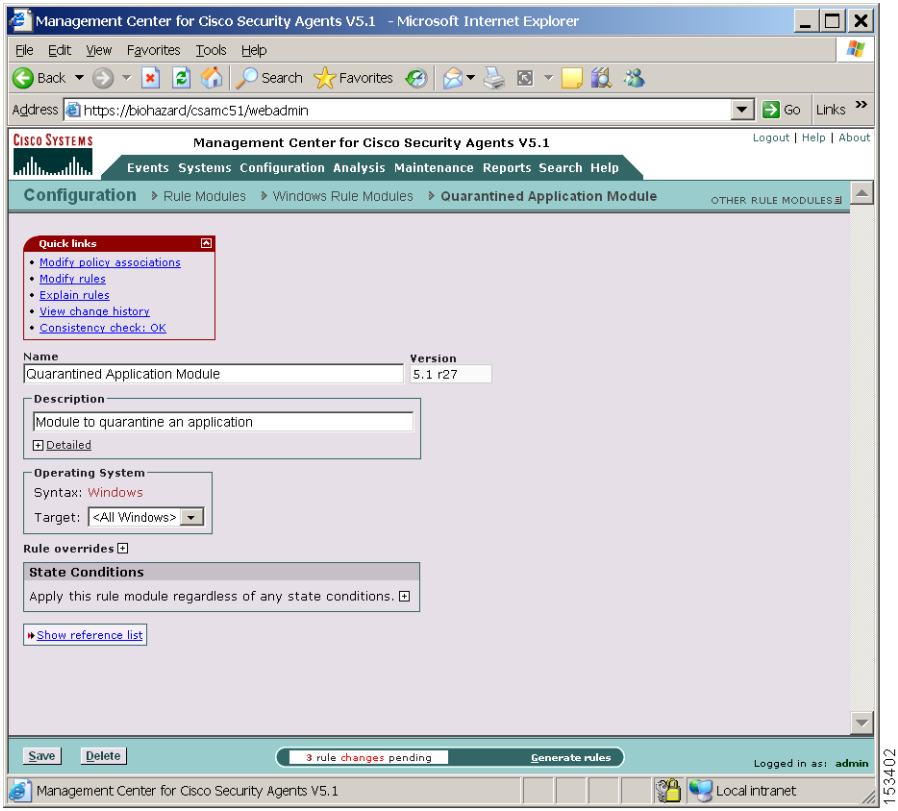
Step 3 In the configuration view, enter the **Name** *Quarantined Application Module*. Note that names are case insensitive, must start with an alphabetic character, can be up to 64 characters long. Spaces are also allowed in names.

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



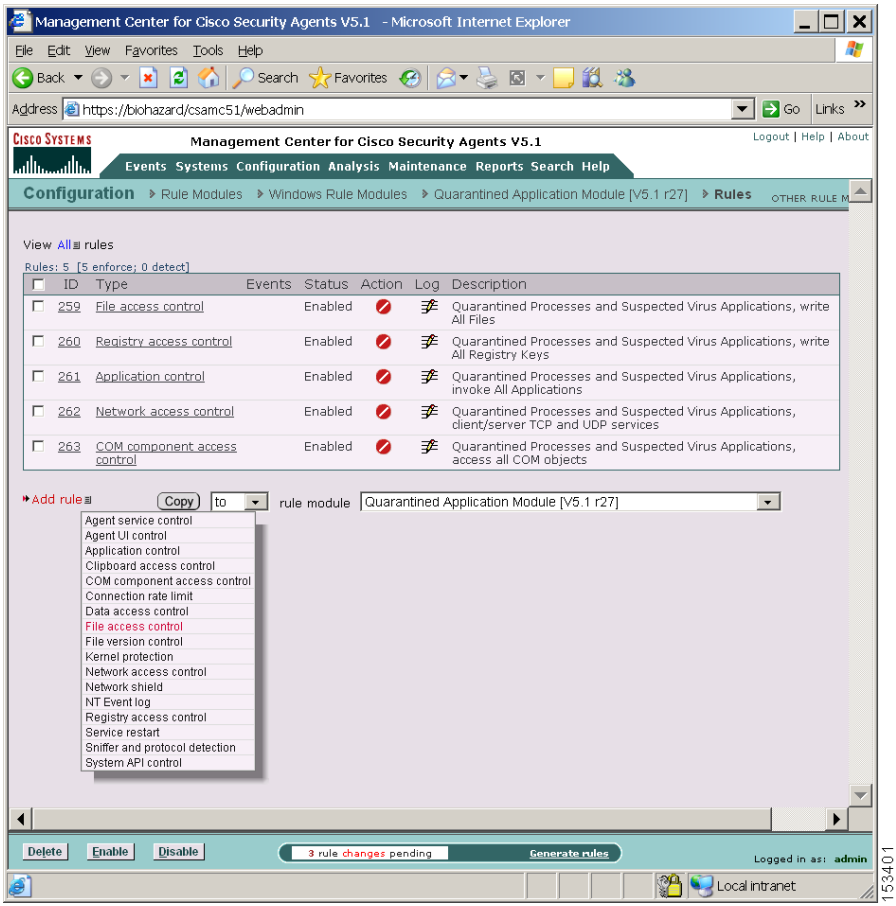
Create a File Access Control Rule

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.

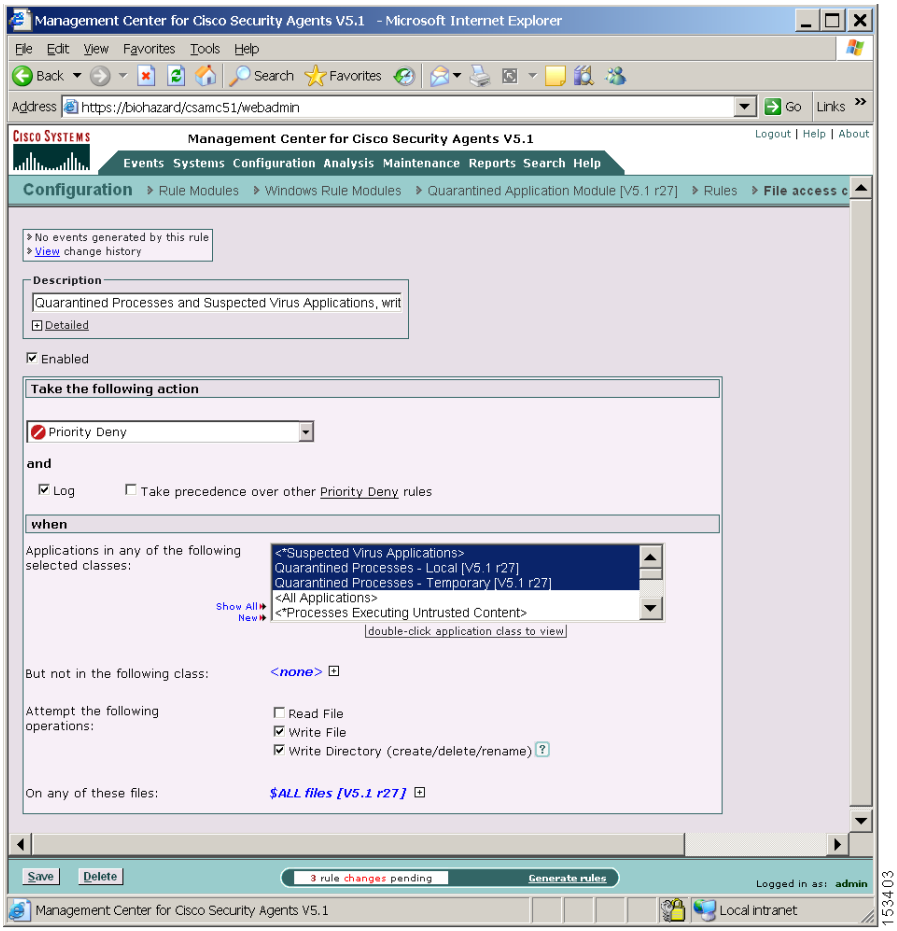
Step 8 Select the and **Write File** and **Write Directory** checkboxes to indicate the actions we are denying.

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.

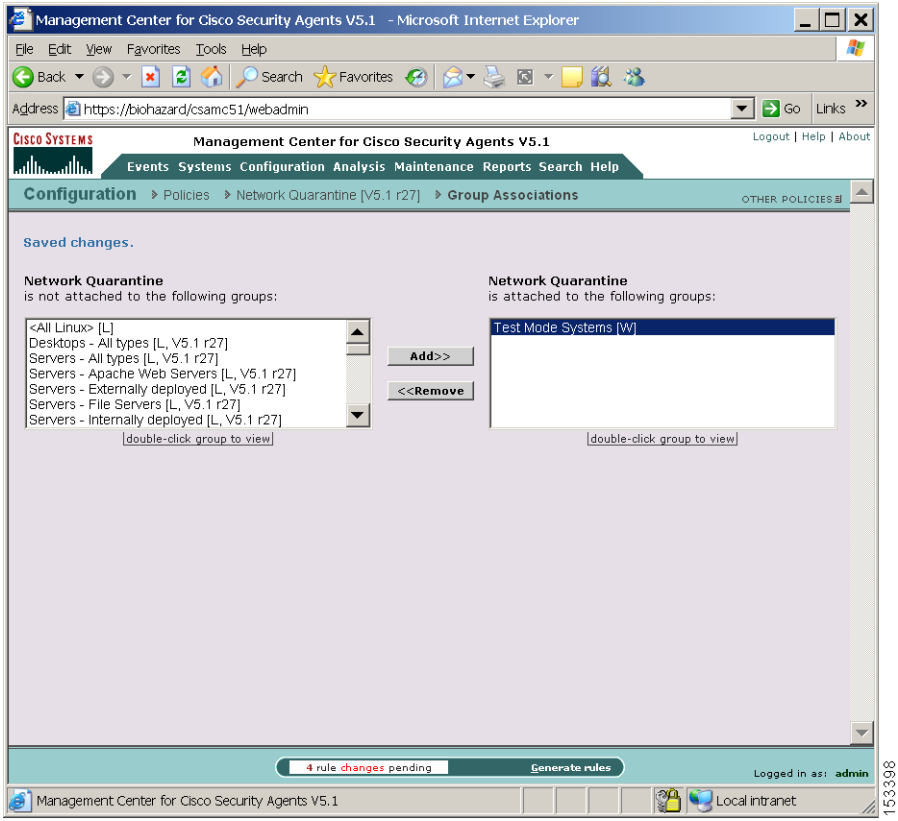
Step 2 From the group list view, click the link for the group you want to attach the policy to. This brings you to that group's edit view.

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



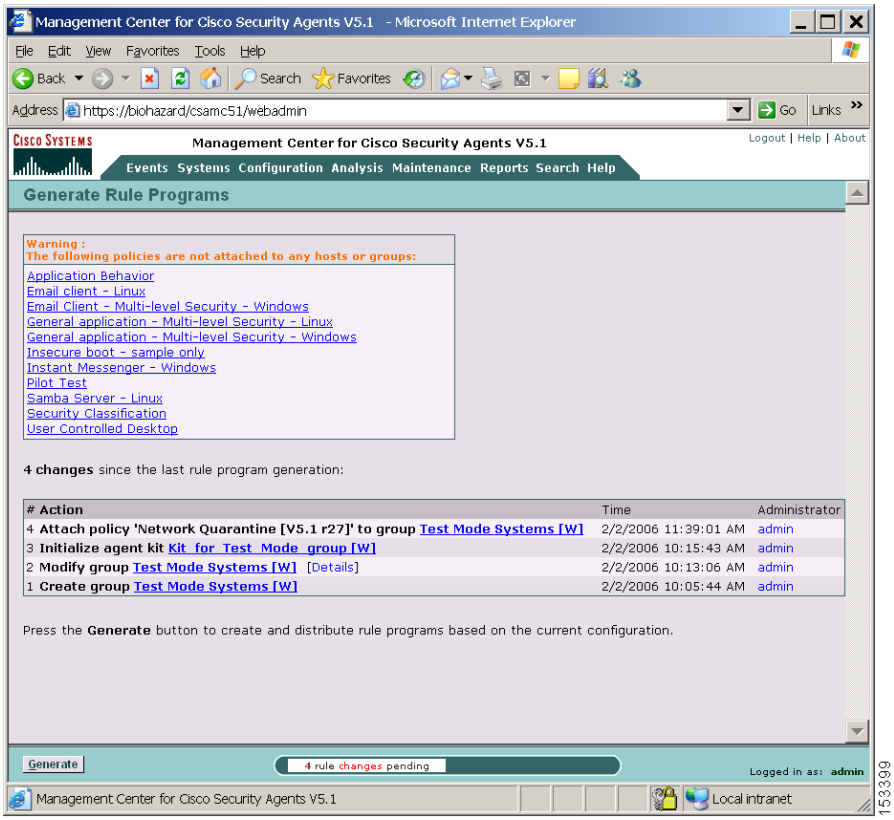
Generate Rule Programs

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

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>/csamc51/kits
```

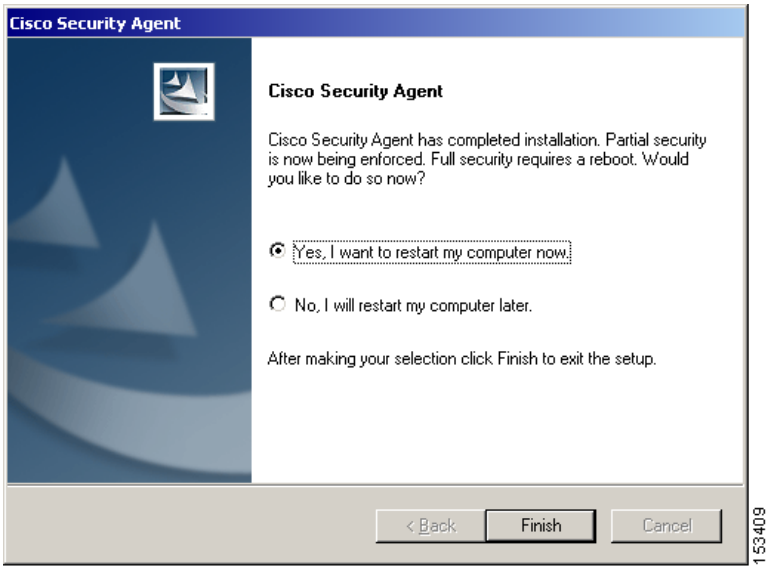
If you are pointing users to the "kits" URL and you have multiple agent kits listed here, be sure to tell users which kits to download.

Note Note that the Registration Control feature also applies to the <system name>/csamc51/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_V5.1.0.265-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) 5.1.0.15
```

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) 5.1.0.15
```

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_V5.1.0.218-lin-setup-1a969c667ddb0a2d2a8da3e7959
a30b2.tar /tmp
```

Step 2 Untar the file.

```
$ cd /tmp
$ tar xvf
CSA-Server_V5.1.0.218-lin-setup-1a969c667ddb0a2d2a8da3e7959
a30b2.tar
```

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

```
$ cd /tmp/CSCOcsa
```

Step 4 Run script install_rpm.sh as root.

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

The package will be installed to `/opt/CSCOcsa`, with some files being put into directories such as `/lib/modules/CSCOcsa`, `/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/CSCOcsa/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
CSAagent-5.1-218
```

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

```
# rpm -ev CSAagent-5.1-218
```

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

Open Source License Acknowledgements and 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/Open SSL Project

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

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

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

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

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

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

OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

Original SSLeay License:

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

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

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

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

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

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

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

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

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Apache [version 1.3.34]

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 1987-2003, 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.com/, the Perl Home Page.

libpcap

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 - 2005, 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.

INDEX

A

B

C

D

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W