CISCO SYSTEMS

Installing Management Center for Cisco Security Agents 4.5.1

Corporate 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: 408 526-4100

Customer Order Number: DOC-78-16726

Preface vii

Audience vii

Conventions viii

Obtaining Documentation ix

World Wide Web ix

Ordering Documentation ix

Documentation Feedback x

Obtaining Technical Assistance x

Cisco.com x

Technical Assistance Center xi

Obtaining Additional Publications and Information xiii

chapter 1

Preparing to Install 1-1

How the Cisco Security Agent Works 1-1

Cisco Security Agent Overview 1-2

Before Proceeding 1-2

System Requirements 1-3

DNS and WINS Environments 1-8

Browser Requirements 1-8

Time and Date Requirements 1-9

Windows Cluster Support 1-9

Internationalization Support 1-9

Internationalization Support Tables 1-11

CSA MC Local Agent and Policies 1-15

Installation Note 1-16
About CSA MC 1-17

chapter 2 **Deployment Planning** 2-1
Overview 2-1
Piloting the Product 2-2
Running a Pilot Program 2-2
Scalable Deployments 2-3
Hardware Sizing 2-3
Configuration Recommendations for Scalability 2-4
Policy Migration 2-5
Configuration Item Mapping 2-5
Policy Tuning and Troubleshooting 2-7
Overall Guidelines 2-7
Using Test Mode 2-10
Disabling Specific Rules 2-11
Caching and Resetting Query Responses 2-12
Setting Up Exception Rules 2-13

chapter 3 **Installing the Management Center for Cisco Security Agents** 3-1
Overview 3-1
Licensing Information 3-2
Upgrading from Version 4.0.x to 4.5.x 3-3
Upgrade Instructions 3-4
Solaris Agent Migration 3-7
Upgrading from CSA Version 4.5 to 4.5.1 3-7
Piloting the Upgrade of CSA from Version 4.5 to 4.5.1 3-8
Installing Management Center for Cisco Security Agents 3-9

Installing CSA MC with a Local Database 3-11
Installing CSA MC with a Remote Database 3-20
Installation Log 3-26
Accessing Management Center for Cisco Security Agents 3-27
Initiating Secure Communications 3-29
Uninstalling Management Center for Cisco Security Agents 3-36
Copying Cisco Trust Agent Installer Files 3-37

chapter 4

Quick Start Configuration 4-1

Overview 4-1
Access Management Center for Cisco Security Agents 4-2
CiscoWorks Administrator Roles in CSA MC 4-3
Cisco Security Agent Policies 4-4
Configure a Group 4-5
Creating Agent Kits 4-7
The Cisco Security Agent 4-12
View Registered Hosts 4-13
Configure a Rule Module 4-14
Configure a Policy 4-20
Attach a Rule Module to a Policy 4-21
Attach a Policy to a Group 4-21
Generate Rule Programs 4-22

Cisco Security Agent Installation and Overview A-1

Overview A-1
Downloading and Installing A-2
Network Shim Optional A-2
The Cisco Security Agent User Interface A-5
Installing the Solaris Agent A-7

Installing the Linux Agent A-9

Preface

This manual describes how to configure the Management Center for Cisco Security Agents on Microsoft Windows 2000 operating systems and the Cisco Security Agent on supported Microsoft Windows 2003, Microsoft Windows XP, Microsoft Windows 2000, Microsoft Windows NT, 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

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

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

Ordering Documentation

Cisco documentation is available in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance.

Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world. Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise

- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center. Cisco TAC inquires are categorized according to the urgency of the issue:

- Priority level 4 (P4) You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3) Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2) Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1) Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

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

- *The Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

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

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:

  http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html

- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:

  http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html

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

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

Preparing to Install

How the Cisco Security Agent Works

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

This section includes the following topics.

- Cisco Security Agent Overview, page 1-2
- Before Proceeding, page 1-2
- System Requirements, page 1-3
- DNS and WINS Environments, page 1-8
- Browser Requirements, page 1-8
- Time and Date Requirements, page 1-9
- Windows Cluster Support, page 1-9
- Internationalization Support, page 1-9
- Internationalization Support Tables, page 1-11
- CSA MC Local Agent and Policies, page 1-15
- Installation Note, page 1-16
- About CSA MC, page 1-17

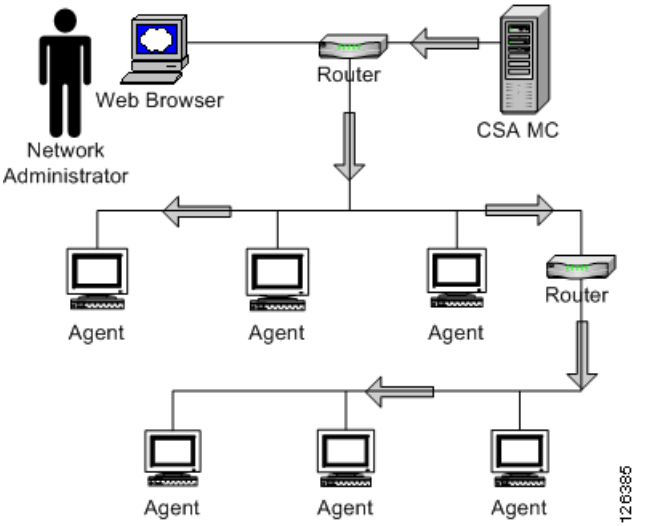
Cisco Security Agent Overview

Cisco Security Agent contains two components:

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

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

Figure 1-1 Product Deployment



Before Proceeding

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

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

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

System Requirements

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

CSA MC is a component of the CiscoWorks VPN/Security Management Solution (VMS). The CSA MC installation also checks for the required version of VMS and will abort the installation if the correct version is not present.

For information on all bundle features and their requirements, see the CiscoWorks2000 VPN/Security Management Solution Quick Start Guide.

Table 1-1 shows VMS bundle server requirements for Windows 2000 systems.

Table 1-1 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 2000 Server or Advanced Server (Service Pack 4) Note: Terminal services are not supported on Server and Advanced Server running CSA MC. Note: Running CSA MC on dual homed systems is not supported.
File System	NTFS
Memory	1 GB minimum memory

System Component	Requirement
Virtual Memory	2 GB virtual memory
Hard Drive Space	9 GB minimum available disk drive space **Note** The actual amount of hard drive space required depends upon the number of CiscoWorks Common Services client applications you are installing and the number of devices you are managing with the client applications. Additionally, a large agent deployment requires substantial space for the database to operate properly.

- 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 not previously been installed, the CSA MC setup program first installs the Microsoft SQL Server Desktop Engine (MSDE) with Service Pack 3a. 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 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.

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** Uni-processor, dual processor, and quad processor systems are supported.
Operating Systems	• Windows Server 2003 (Standard, Enterprise, Web, or Small Business Editions) • Windows XP (Professional 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 • All Windows, Internet Explorer 4.0 or higher required. **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	15 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 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

System Component	Requirement
Hard Drive Space	15 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 **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	15 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 20 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.

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 the CiscoWorks UI. In order to view CSA MC both locally on the system where you are installing CiscoWorks and for remote access. 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.

Netscape:

- Version 7.1 or later
- You must have cookies enabled. Locate this feature from the following menu, Edit>Preferences>Advanced.
- JavaScript must be enabled.

Note Java Virtual Machine is required to access the CiscoWorks UI and subsequently CSA MC. Java plug-in version 1.4.2_06 is the current supported version. If you do not have this plug-in, when you attempt to access CiscoWorks, you are prompted to download and install it.

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.

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
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
Japanese	L	L(S)	L(S)
Korean	L	L(S)	L(S)
Norwegian	S	NA	NA
Polish	S	S	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)
Japanese	L	L(S)
Korean	L	L(S)
Norwegian	S	S
Polish	S	S
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	S	S	S
Portuguese	S	S	S
Russian	S	S	S
Spanish	L	L(S)	L(S)
Swedish	S	S	S
Turkish	S	S	S

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

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

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

Step 1 Move your mouse over **Systems** in the menu bar and select **Hosts** from the drop-down menu.

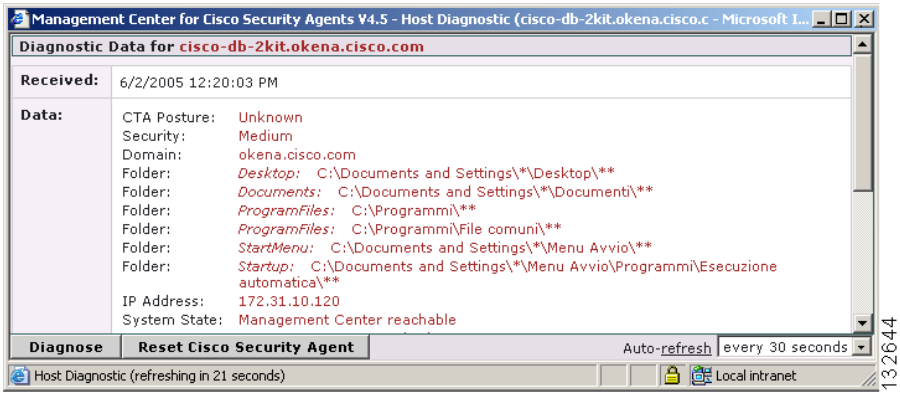
Step 2 Click the link to the host name using the language you want to verify.

Step 3 In the Host Status area, click the **Detailed Status and Diagnostics** link.

Step 4 Click the **Diagnose** button.

Step 5 Look at the folder information in the Data area of the Diagnosis Data page. (See Figure 1-2 on page 1-15.) 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



CSA MC Local Agent and Policies

The CSA recommended deployment is to have only CSA MC and Security Monitor installed as part of your VMS bundle on the CSA MC system. When you install CSA MC, an agent containing the policies necessary to protect CSA MC and other limited CiscoWorks daemons and operations is automatically installed as well. The policies that are enforced by this agent are fairly restrictive and are appropriate if you are running the recommended deployment.

If you are running other non VMS products or software on the CiscoWorks system, this restrictive policy may impede these other products. Although, it is recommended that you do not install other products on the CSA MC system (other than Security Monitor), you can do so if you remove the restrictive policy from the agent protecting the system, leaving you with a more open policy. Without the restrictive policy, the system remains protected, but the policy allows more products to run on the system and access network resources. Therefore, the system is inherently less secure. If you wish to deploy CSA MC on a system running other software, navigate to the "CiscoWorks VMS Systems" Group and remove the "CiscoWorks Restrictive VMS Module" from the group.

Note If you feel comfortable doing so, rather than removing the CiscoWorks Restrictive VMS Module, you can edit it to allow the actions your other installed products require.

Caution If you are installing or uninstalling various VMS components, and you have a Cisco Security Agent protecting the VMS bundle, you should disable the agent service before you begin the install/uninstall of any other VMS component. (You do not have to do this when installing/uninstalling CSA MC.) To disable the agent service, from a command prompt type `net stop "Cisco Security Agent"`. (You may receive a prompt asking if you want to stop the agent service. You should answer Yes.) To enable the service, type `net start "Cisco Security Agent"`.

If you do not disable the agent service and you attempt to alter a CiscoWorks system configuration, the agent may disallow the action or it may display multiple queries to which you must respond.

Installation Note

Any system to which you are installing CSA MC or the Cisco Security Agent itself must not have the Cisco IDS Host Sensor Console or the Cisco IDS Host Sensor installed. If the CSA MC or the agent installer detect the presence of any Cisco IDS Host Sensor software on the system, the installation will abort.

Because there may be incompatibilities between Cisco IDS Host Sensor software and CSA MC or agent software, you must uninstall the Cisco IDS Host Sensor and Cisco IDS Host Sensor Console software before installing CSA MC or agent software. Documentation for uninstalling Cisco IDS Host Sensor software can be found at the following location:

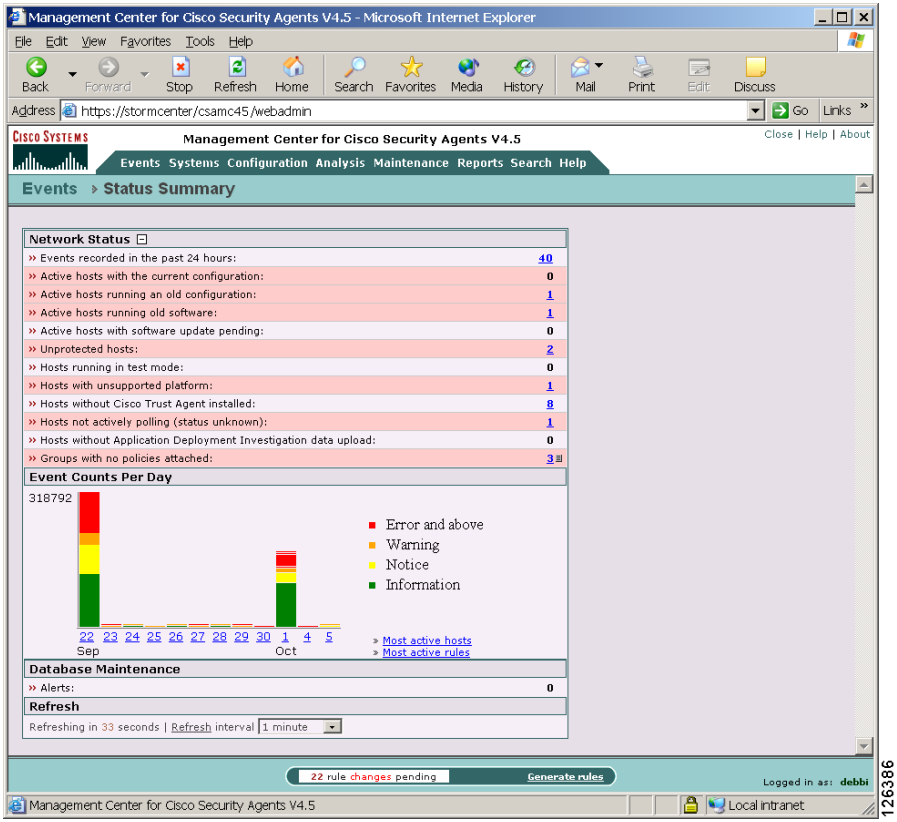
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/host/host25/install/hidsch2.htm#1024883

About CSA MC

The CSA MC user interface installs as part of the overall Cisco Security Agent solution installation and is managed from CiscoWorks 2000. 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



Deployment Planning

Overview

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

This section contains the following topics:

- Piloting the Product, page 2-2
- Running a Pilot Program, page 2-2
- Scalable Deployments, page 2-3
- Hardware Sizing, page 2-3
- Configuration Recommendations for Scalability, page 2-4
- Policy Migration, page 2-5
- Configuration Item Mapping, page 2-5
- Policy Tuning and Troubleshooting, page 2-7
- Overall Guidelines, page 2-7
- Using Test Mode, page 2-10
- Disabling Specific Rules, page 2-11
- Caching and Resetting Query Responses, page 2-12
- Setting Up Exception Rules, page 2-13

Piloting the Product

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

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

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

Running a Pilot Program

Your pilot program should proceed in the following manner:

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

  Details:

  – If your entire deployment will be very small, be sure to pilot at least 15-20 systems.

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

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

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

  Details:

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

Scalable Deployments

The Cisco Security Agent V4.5 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

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

Table 2-1 Server Configuration 1: Single Server

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

Table 2-2 Server Configuration 2: Two Servers

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

Table 2-3 Server Configuration 3: Three Servers

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

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 Migration

If you are upgrading to CSA MC V4.5 from a previous version, you may want to continue to use policies that you've created and deployed successfully with CSA MC V4.0.x. Because some configuration items, such as rule types and application classes, have changed in V4.5, you cannot do a straight import of your existing configurations into V4.5 and expect them to behave as they did previously.

The next section provides information on configuration item mapping from previous CSA MC versions to this latest release. Because feature implementation has changed in V4.5, you should plan to pilot even those imported configuration items that you've successfully run with a previous version. CSA MC V4.5 contains significant changes which will require some administrator oversight that is best performed in the process of a pilot program.

Configuration Item Mapping

You should refer to *Using Management Center for Cisco Security Agents 4.5* for details on the hierarchal changes that have been made to the CSA MC configuration process. More specifically, the following features that appeared in V4.0.x now appear in V4.5 as follows:

Note This is not a listing of new features in CSA MC V4.5. This is simply a list of items that were previously in the product and have been changed in a significant manner in this release. This change will affect any existing configurations you import from a previous version into CSA MC V4.5. Therefore, you should double-check and possibly tweak affected, imported items to correctly adapt them to V4.5.

Downloaded Content Application Class Change

The configuration application class named "Processes executing downloading content" in previous versions has been split into two non-configurable application classes in V4.5. Those new classes are "Processes executing untrusted content" and "Applications internally interpreting content." These classes are now built through pre-configured policies.

If you were using the "Processes executing downloading content" application class in a previous version, and you have imported those policies into V4.5, you may need to manually add "Processes executing untrusted content" and "Applications internally interpreting content" to those imported rules in V4.5.

Mandatory Group Enrollment

This functionality takes the place of mandatory settings on the individual policy level. CSA MC now provides three auto-enrollment architectural groups (Windows, Solaris, Linux) that are mandatory for all hosts of a given OS architecture. By providing group auto-enrollment for hosts, any policies you attach to these groups also become mandatory by association.

Monitoring Rule Action Functionality

The File monitor rule has been removed in this release in favor of adding Monitor as a new action type available for most rules. This way, in addition to file monitoring, you can configure network, registry, etc., monitoring rules.

Network Shield Rule Change

The Network shield rule page now contains a network address field. This allows you to optionally apply network shield settings to specified system addresses. This page now has an action pulldown field so that it can be written as an Allow or Deny, etc.

Network Worm Detection Rule Change

The Network worm detection heuristic is no longer configured using a checkbox on/off switch. This functionality still exists and has been enhanced. It is now provided as a self-contained policy that can be edited by the administrator.

Query Settings Variable Addition

You must now configure the query text in combination with the query buttons that appear in the query pop-up box the end user will see when query rules are triggered. Query responses are now also persistent across reboots.

System API Control Rule Change

What was called the Trojan detection rule in previous releases is now called the System API control rule. The look and feel of this page has been changed and new functionality has been added. This page now has an action pulldown field so that it can be written as an Allow or Deny, etc.

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.

Note If you are trying to reduce the number of events reported to the MC you can evaluate the most active hosts or most active rules reporting events. The Status Summary page provides information on which rules are being triggered most often and which hosts are most active.

Once the MC is installed, go to Events > Status Summary page. Click either the "Most active hosts" link or the "Most active rules" link.

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. 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.

Installing the Management Center for Cisco Security Agents

Overview

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

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

This section contains the following topics.

- Licensing Information, page 3-2
- Upgrading from Version 4.0.x to 4.5.x, page 3-3
- Upgrade Instructions, page 3-4
- Solaris Agent Migration, page 3-7
- Upgrading from CSA Version 4.5 to 4.5.1, page 3-7
- Piloting the Upgrade of CSA from Version 4.5 to 4.5.1, page 3-8
- Installing Management Center for Cisco Security Agents, page 3-9
- Installing CSA MC with a Local Database, page 3-11
- Microsoft SQL Server 2000 Local Installation Notes, page 3-19

- Installing CSA MC with a Remote Database, page 3-20
- Installation Log, page 3-26
- Accessing Management Center for Cisco Security Agents, page 3-27
- Initiating Secure Communications, page 3-29
- Uninstalling Management Center for Cisco Security Agents, page 3-36
- Copying Cisco Trust Agent Installer Files, page 3-37

Licensing Information

CSA MC and agents require a license obtained from Cisco in order to operate with full functionality. You can install and run both the MC and the agent without a license. If you do not have a valid license, CSA MC and all associated agents will not operate until you obtain a valid license.

The information contained in your 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 one of the following manners:

During installation

During the installation, you are prompted to copy the license into the CSA MC directory. If you choose Yes, you can browse to the license file on the system (or in an accessible file share), save it, and continue the installation. Or you can choose No when prompted and copy the license when the installation has completed and the system is rebooted.

Note If you copy a valid license key to CSA MC during the installation, after the system reboots, all downloaded and installed agent kits immediately operate with full functionality. You do not have to login and generate rules to have this occur.

After installation

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.

Upgrading from Version 4.0.x to 4.5.x

Upgrading from versions of the product earlier than version 4.0.x to version 4.5.x is not supported. (If you are trying to upgrade from version 4.5 to version 4.5.1 see Upgrading from CSA Version 4.5 to 4.5.1, page 3-7.)

You have two options when upgrading from CSA MC 4.0.x to CSA MC 4.5.x.

- Install V4.5.x on the same machine as V4.0.x.

Caution Both CSA MC 4.0.x and CSA MC 4.5.x will co-exist on the same system after upgrading. Therefore you should note that if you select this first option, you cannot apply any upgrades that may be released to the V4.0.x CSA MC once V4.5.x is installed. Additionally, after upgrading to the same machine, Profiler will no longer work with the V4.0.x CSA MC and agents.

Also note the following about this first upgrade option: You CANNOT select the Remote Database option if you upgrade on the same machine. (If you are planning to increase your number of deployed agents, it is highly recommended that you install CSA MC V4.5.x to a fresh machine and use a remote database.)

- Install V4.5.x on a different machine with the knowledge that V4.0.x agents will eventually be migrated to the new V4.5.x machine.

The CSA MC V4.5.x installation does not automatically upgrade or overwrite the V4.0.x installation. Ultimately, the upgrade process described here will allow you to import your V4.0.x configuration items into the newly installed V4.5.x system. It will also allow you to migrate V4.0.x hosts to V4.5.x. After installing V4.5.x, it is expected that you will spend some time examining how policies and other functionality has changed between versions and you will gradually apply the V4.5.x policies to the migrated hosts.

Caution You should not uninstall V4.0.x until you have migrated all agents to V4.5.x.

When you install CSA MC V4.5.x, a new *Security Agents V4.5* menu item appears in your CiscoWorks UI. If you install CSA MC V4.5.x on the same machine as V4.0.x, your original *Security Agents* menu item remains in place and you continue to manage your existing V4.0.x configurations from there. The CSA MC V4.5.x installation also creates a new directory structure. (If you install CSA MC V4.5.x on the same machine as V4.0.x, your original CSAMC directory structure remains in place, co-existing with the new V4.5 structure.) Note that subsequent releases of CSA MC will continue to include the new version number in the directory structure. Refer to the following chart.

Table 3-1 Menu Item and Directory Path

	Menu Item	Directory Path
CSA MC V4.5.1	Security Agents V4.5	CSCOpx\CSAMC45
CSA MC V4.5	Security Agents V4.5	CSCOpx\CSAMC45
CSA MC V4.0	Security Agents	CSCOpx\CSAMC

Upgrade Instructions

The following upgrade process contains instructions for installing CSA MC V4.5.x on the same system as CSA MC V4.0.x and for installing CSA MC V4.5.x to a separate machine. Both scenarios are covered here.

Caution If you intend to upgrade 4.0.x Solaris agents, please read Solaris Agent Migration, page 3-7 before starting your upgrade.

To upgrade to V4.5.x, do the following:

Step 1 Install the Management Center for Cisco Security Agents V4.5.x. See page 3-9 for instructions.

- If you're installing CSA MC V4.5.x on the same machine running CSA MC V4.0.x, an xml file containing V4.0.x configuration items and host information is automatically generated by the installation and ready for importing once the install is complete.
- If you're installing CSA MC V4.5.x on a different machine from the system running V4.0.x, after installing V4.5.x, you must copy and manually run an executable file on the V4.0.x machine to create the xml file needed for importing V4.0.x configuration and host information to V4.5.x.

Step 2 If you have installed V4.5.x on the same machine as V4.0.x, you can skip to the end of Step 6. Otherwise, once you've installed CSA MC V4.5.x and rebooted the system, navigate to the CSCOpx\CSAMC45\migration directory. Copy the file named `prepare_migration.exe` to your V4.0.x system. (You can copy it to any place on the system.)

Step 3 On your CSA MC V4.0.x, disable agent security and run the `prepare_migration.exe` file that you copied from the V4.5.x system. (You must disable security in order to run the executable file and create the import xml data.) This launches a command prompt which displays the progress of the migration.

Step 4 When the `prepare_migration.exe` file is finished, on the V4.0.x system, navigate to the CSCOpx\CSAMC\bin directory and locate a newly created file named `migration_data_export.xml`.

Step 5 Then from the V4.5 system, import the `migration_data_export.xml` file to the CSA MC V4.5 machine. If V4.5.x and V4.0.x are on different machines, do this by either copying the xml file to the V4.5.x system first and then importing it or by browsing to it from the V4.5.x system if you have network shares set up.

Step 6 You must generate rules once the import is complete. If you do not generate rules at this point, you cannot upgrade and migrate agent hosts as described in the next section.

Note CSA MC V4.5.x ships with policies that contain new V4.5.x functionality. This new functionality does not match all V4.0.x configurations. Beginning with V4.5, CSA MC configuration item names are labeled with the release version number to distinguish them from older (or newer) configuration items or items created by administrators. When you import your V4.0.x configuration, new V4.5.x items are not overwritten. You will likely have items from both versions in your CSA

MC V4.5.x. If the import process finds that two items have the exact same contents and the only difference is the V4.5.x appended name field, the old V4.0.x item is not imported and the newer V4.5.x item is used in its place.

Step 7 To upgrade and migrate V4.0.x agents to V4.5.x, schedule V4.5.x software updates for V4.0.x agents. You schedule this upgrade from CSA MC V4.0.x system. (Performing the V4.5.x installation placed a V4.5.x software update on the V4.0.x machine.)

Once V4.0.x agents receive the scheduled software update, they will point to and register with the new CSA MC V4.5.x. The update contains the appropriate new certificates to allow this to occur.

Caution When upgrading 4.0.x agents to software version 4.5.x, the upgrade program disables the system network interfaces to ensure a secure upgrade process. The agent service is also stopped to allow the update to occur. Once the update is complete, the agent service is restarted and the network interfaces are enabled. Note that this information only applies to 4.0.x to 4.5.x software upgrades. (Also note, that secure upgrades are not supported for Windows NT systems.)

Note that when you import your V4.0.x configurations to the V4.5.x system, old V4.0.x agent kits are also imported. When V4.0.x hosts perform software updates and register with the V4.5.x system, they are placed in groups according to the group information that was part of their original installation kit. If you want a host to be placed in a different group when it registers with V4.5.x, you have the ability to click on the original agent kit now listed along with the new V4.5.x agent kits and change the group association. You must generate rules after you change a group kit association.

Note Note that when hosts register with CSA MC V4.5.x, they appear in their assigned group(s) and they also appear in the mandatory V4.5.x groups that match their OS type.

Also note, the once you have migrated all V4.0.x agents to V4.5.x, you can uninstall CSA MC V4.0.x.

Solaris Agent Migration

You should note that Solaris host migration is a bit different than Windows migration.

Caution Only Solaris agent versions 4.0.3.735 or higher can be upgraded to version 4.5.x Earlier Solaris agents cannot be upgraded.

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

Upgrading from CSA Version 4.5 to 4.5.1

Upgrading Cisco Security Agent from 4.5 to 4.5.1 is supported. (If you are trying to upgrade from CSA version 4.0.x to 4.5.1 see, Upgrading from Version 4.0.x to 4.5.x, page 3-3). The new software and policy changes are included in one self-extracting executable file and they can be installed alongside version 4.5. You do not need to uninstall CSA version 4.5 to proceed.)

If the installation process finds that two security components are identical, and the only difference is the version number appended name field, the newer item fromV4.5.1 overwrites the older version.

To upgrade CSA 4.5 to CSA 4.5.1, follow this procedure:

Step 1 From the system running CSA MC V4.5, download the new kit from Cisco's web site (http://www.cisco.com/cgi-bin/tablebuild.pl/csa).

Step 2 Choose to **Save** the download locally rather than to open it.

Step 3 Open the folder where you saved the self-extracting ZIP file.

Step 4 Double-click the self-extracting ZIP file to open it.

Step 5 Double-click **setup.exe** to begin the installation.

Step 6 Click **OK**.

Step 7 At the Welcome screen (Figure 3-1), click **Next.**

Step 8 CSA prompts you with message that an attempt is being made to disable security for the Cisco security Agent. Select **Yes** and click **Apply** to allow the activity.

Step 9 Your response is then challenged. Type the letters you see in the Cisco Security Agent Challenge window in the text field and click **OK**.

Step 10 New files are copied to your system. (See Figure 3-7.)

Step 11 Once all the files are copied, the installation performs some preliminary system setup tasks. (See Figure 3-8.)

Note The agent protecting the system on which CSA MC runs is upgraded at the same time as CSAMC.

Step 12 You receive a message that installation is complete. Save and close any open files and click **OK** for the system to be restarted.

Step 13 In order for all the agents to receive the software upgrade, you must schedule a software upgrade for all the groups running version 4.5 software. See *Using Management Center for Cisco Security Agents* for information about scheduling a software upgrade.

Note The software upgrade deployed to agents does not contain policy changes, it only upgrades the agent application.

Piloting the Upgrade of CSA from Version 4.5 to 4.5.1

Once you have upgraded CSA MC with the version of 4.5.1 software and have distributed the software upgrade to all the agents running version 4.5, you should review the policy changes that came with version 4.5.1 and determine which of these changes you should deploy.

Step 1 Move the mouse over **Systems** and click **Groups** from the drop-down menu.

Step 2 From the Groups List page you can see which groups have both an old version and a new version and how many hosts would be affected by receiving policy changes.

Step 3 See the Release Notes for CSA version 4.5.1 for a list of policies that have changed to provide greater security, be less restrictive, or to be more efficient. Evaluate the policies that have changed in a particular group.

- If a policy changed because its rules were made more efficient or less restrictive, do not move existing hosts into the CSA version 4.5.1 groups associated with CSA version 4.5.1 policies. Your system is up and running and these sorts of changes were probably accounted for when CSA was originally piloted.
- If the policies have changed in order to enforce security more strictly, begin a pilot program by associating a small number of systems with the new CSA version 4.5.1 groups and see how the policy changes affect day to day work on those systems.

Step 4 After the pilot program has ended, and you are satisfied with the security provided by the new policies, associate the remaining hosts with the CSA version 4.5 groups with the CSA version 4.5.1 groups. See *Using Management Center for Cisco Security Agents* for information about bulk transferring hosts from one group to another.

Note CSA version 4.5 policies will contine to function with the version 4.5.1 agent.

Installing Management Center for Cisco Security Agents

Caution CSA MC is a component of the CiscoWorks VPN/Security Management Solution (VMS). You must have CiscoWorks Common Services installed on the system to which you are installing CSA MC. See the CiscoWorks2000 VPN/Security Management Solution Quick Start Guide for details.

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

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 limit. In this case, you can have CSA MC and Microsoft SQL Server 2000 on the same system if you are planning to deploy no more than 5,000 agents. 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 3-21.)

  Use this configuration option if you are planning to deploy 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 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 3-21.)

  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. This way, if your network is under attack and a flurry of events is causing one MC's CPU to spike, for example, your configuration MC remains unaffected and you can still push configuration changes to your hosts.

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.

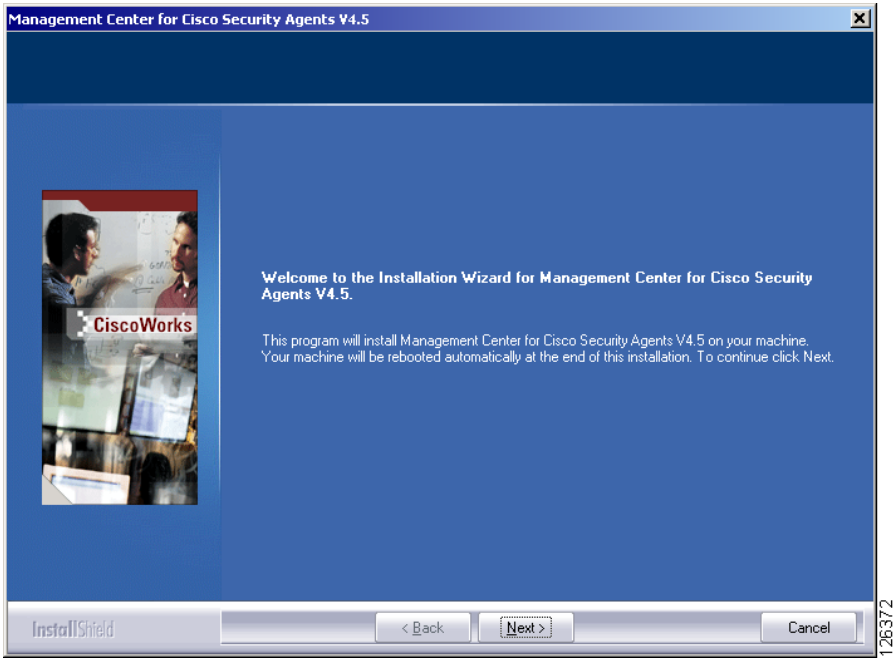
Before beginning, exit any other programs you have running on the system where you are installing CSA MC.

To install the CSA MC, do the following:

Step 1 Log on as a local Administrator on your Microsoft Windows 2000 server system with Service Pack 4 installed.

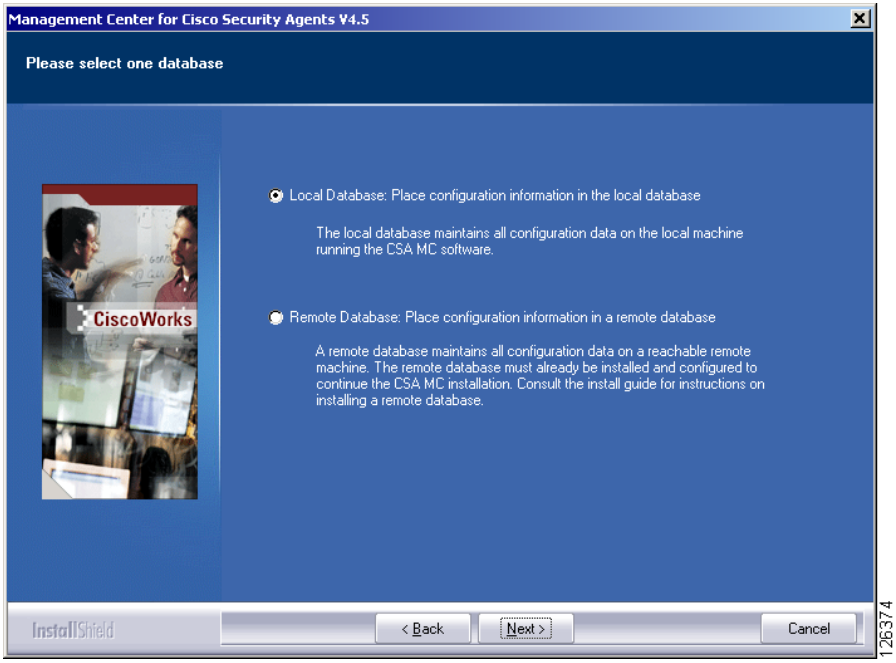
Step 2 Insert the VPN/Security Management Solution CD into the CDROM drive. When the installation screen listing all available VMS products appears, select the checkbox beside **Managing Cisco Security Agents—Servers and Desktops** and click Next to start the installation. The welcome screen appears. See Figure 3-1.

Figure 3-1 CSA MC Installation Welcome Screen



Step 3 After you click **Next** in the welcome screen, the install begins by prompting you to choose a database setup type. See Figure 3-2. In this case, you will keep the default selection of **Local Database** and click the **Next** button.

Figure 3-2 Database Setup Type

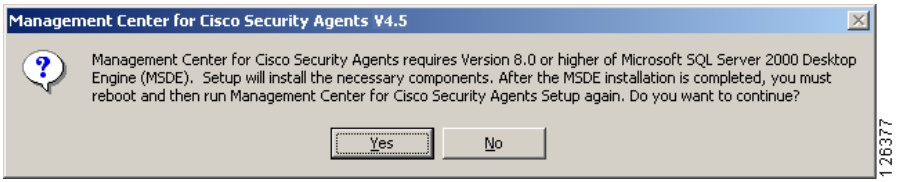


Step 4 If installing locally, the installation next checks to see if you have Microsoft SQL Server Desktop Engine (MSDE) installed. CSA MC uses MSDE for its local configuration database. If this software is not detected, you are prompted to install it. See Figure 3-3.

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 3-10 for more information. If you are using Microsoft SQL Server 2000, refer to Microsoft SQL Server 2000 Local Installation Notes, page 3-19 for details.

Caution On a system where CSA MC has not previously been installed, the setup program first installs 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 3a, the installation will abort. This database configuration is not qualified.

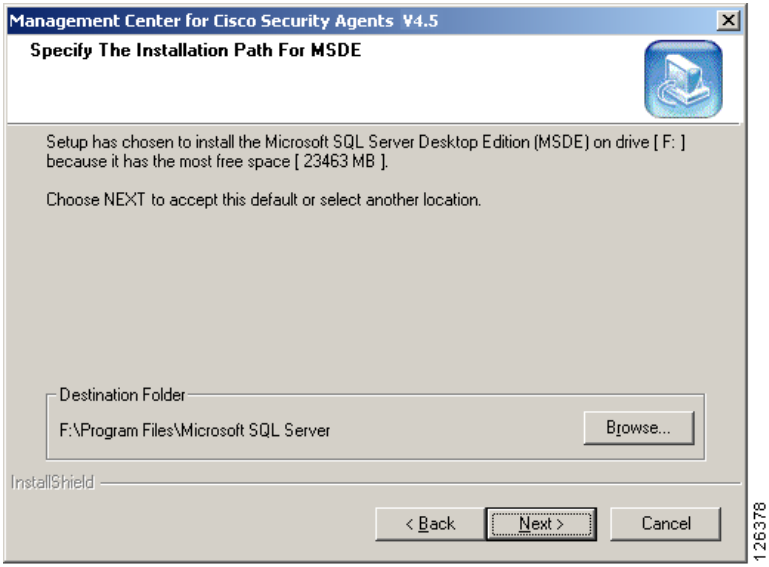
Figure 3-3 Install Microsoft SQL Server Desktop Engine



Once you click Yes, you proceed through the Microsoft SQL Server installation. It only takes a few minutes.

The first installation screen prompts you to accept the default SQL Server install directory path. The default is selected by searching the system disk for a location that provides the most space for the database. You can select a different path if you choose.

Figure 3-4 Microsoft SQL Server Directory Prompt



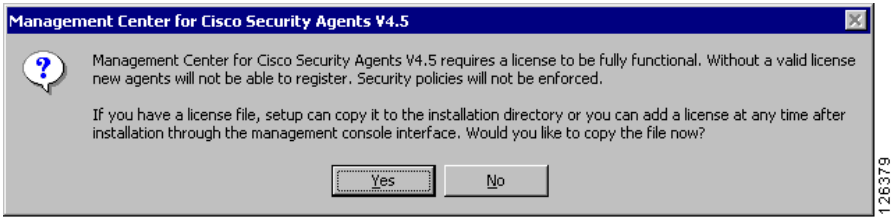
Note When the Microsoft SQL Server installation finishes, you must begin the CSA MC installation again. You may have to restart your system before beginning the CSA MC installation.

Step 5 Begin the CSA MC installation again. This time the installation detects the Microsoft SQL Server software and proceeds.

Step 6 You are reminded that you must obtain a license key (see page 3-2 for information). If you already have a license key file on the system to which you are installing CSA MC, you can copy it to the installation directory at this time by clicking the Yes button (see Figure 3-5) and browsing to it on the system. You can also click No and copy it any time after the installation.

Note If you copy a valid license key to CSA MC during the installation, after the system reboots, all downloaded and installed agent kits immediately operate with full functionality. You do not have to login and generate rules to have this occur.

Figure 3-5 License Key Popup



Once you copy a valid license key to the system, you are prompted to begin the installation (see Figure 3-6). The install then proceeds copying the necessary files to your system (see Figure 3-7).

Figure 3-6 Installation Prompt

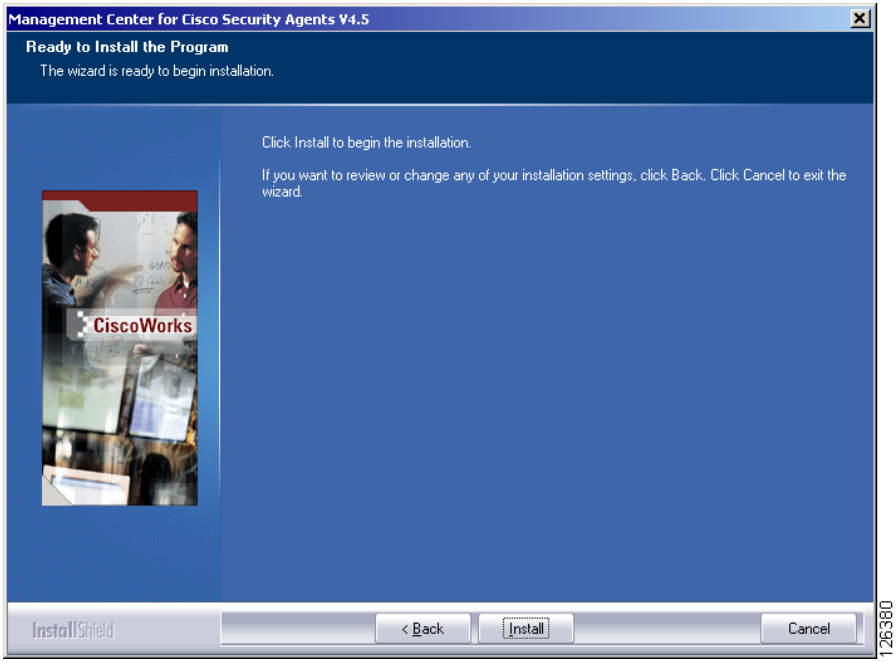
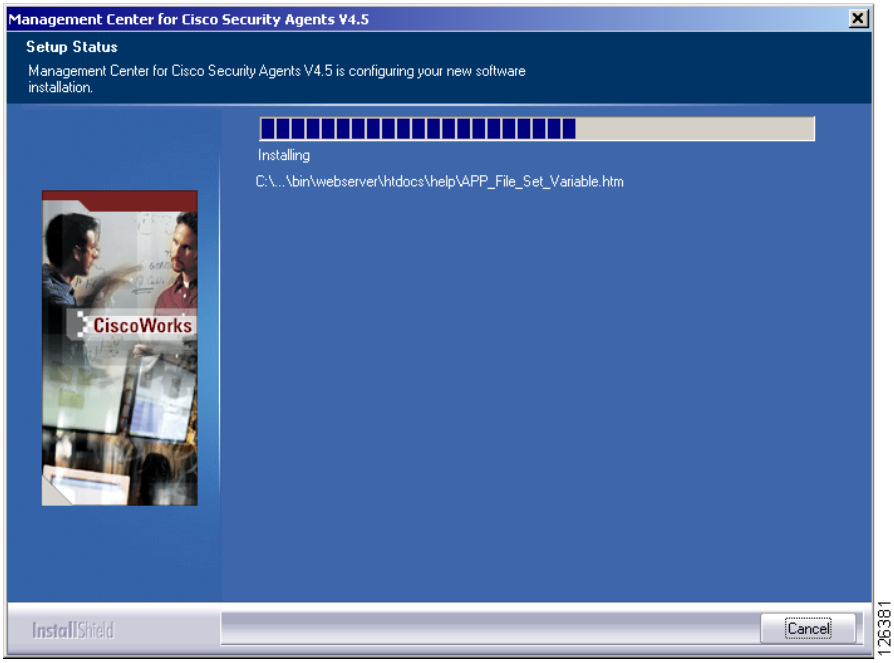
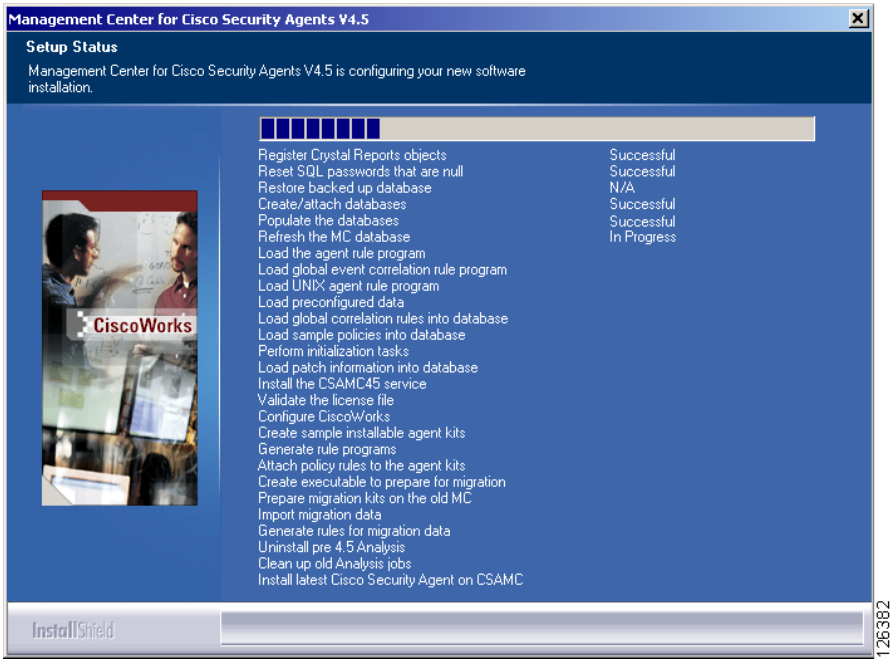


Figure 3-7 Copy Files



Once all the files are copied, the installation performs some preliminary system setup tasks (see Figure 3-8).

Figure 3-8 System Setup



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, you are prompted to reboot the system. It will automatically reboot within 5 minutes.

Note When you install CSA MC, the installation enables SSL in CiscoWorks. When you access the CSA MC UI from CiscoWorks, you must have SSL enabled in CiscoWorks for CSA MC to allow the connection.

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 3-20.

For local database installations exceeding 5,000 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 3a. 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 SP3a (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 In a distributed (multiple MC) environment, when installing, upgrading, or uninstalling any MC in the distributed configuration, the service must be stopped on the other MCs. For example, in a configuration with 2 MCs, you *must* first *stop* the CiscoWorks Daemon Manager (`net stop crmdmgtd`) on one MC before you install the software update on the other MC.

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.

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.)

- 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 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.

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 Windows 2000 server system with Service Pack 4 installed.

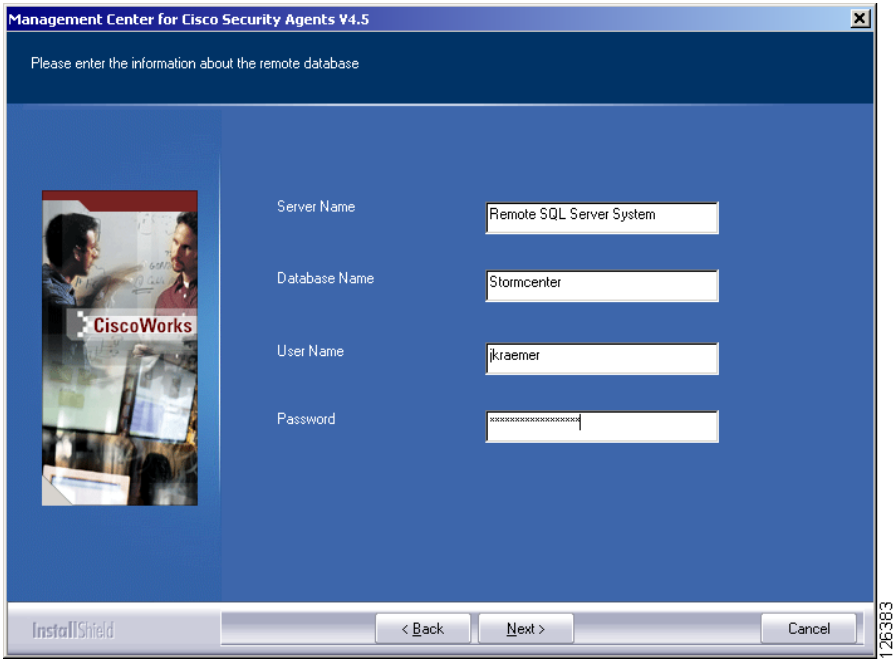
Step 2 Insert the VPN/Security Management Solution CD into the CDROM drive. When the installation screen listing all available VMS products appears, select the checkbox beside **Managing Cisco Security Agents—Servers and Desktops** and click Next to start the installation.

Step 3 The install begins by prompting you to choose a database setup type. See Figure 3-2. 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 3-9):

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

Figure 3-9 Remote Database Information

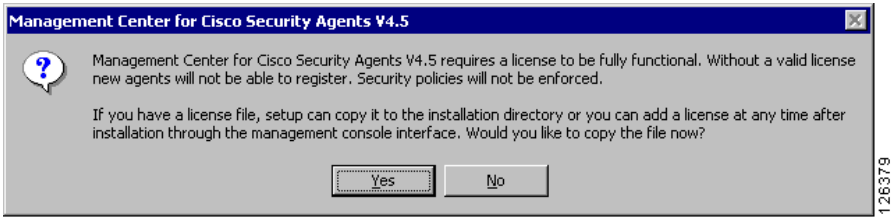


Step 4 Once you enter the database information and click **Next**, the installation attempts to locate the database and verify that it is configured appropriately. If the database is not setup correctly, you are prompted with this information and the installation will not continue. Otherwise, the installation proceeds.

Step 5 You are next reminded that you must obtain a license key (see page 3-2 for information). If you already have a license key file on the system to which you are installing CSA MC, you can copy it to the installation directory at this time by clicking the Yes button (see Figure 3-10) and browsing to it on the system. You can also click No and copy it any time after the installation.

Note If you copy a valid license key to CSA MC during the installation, after the system reboots, all downloaded and installed agent kits immediately operate with full functionality. You do not have to login and generate rules to have this occur.

Figure 3-10 License Key Popup



Step 6 Once you copy a valid license key to the system, you are prompted to begin the installation (see Figure 3-11). The install then proceeds copying the necessary files to your system (see Figure 3-12).

Figure 3-11 Installation Prompt

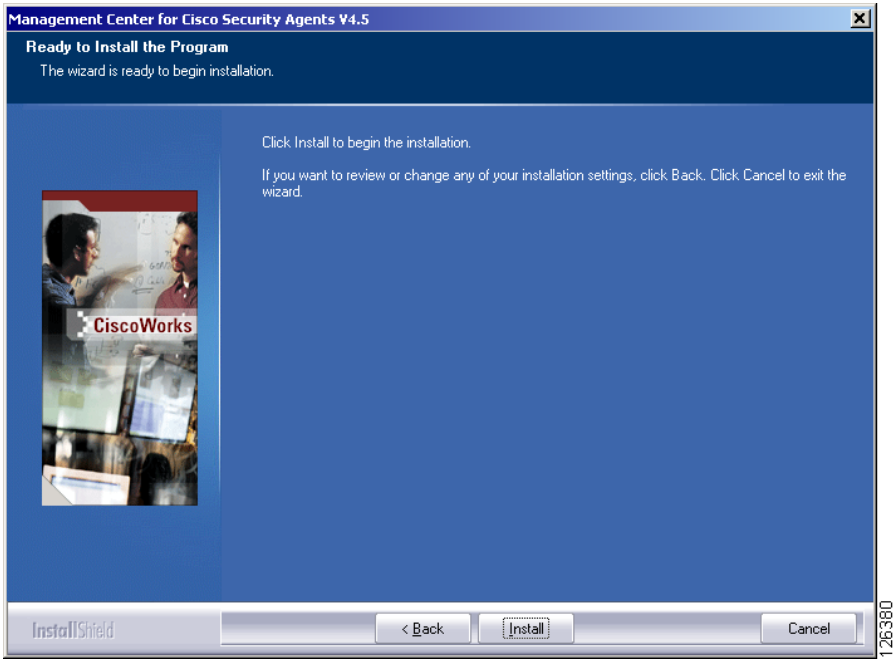
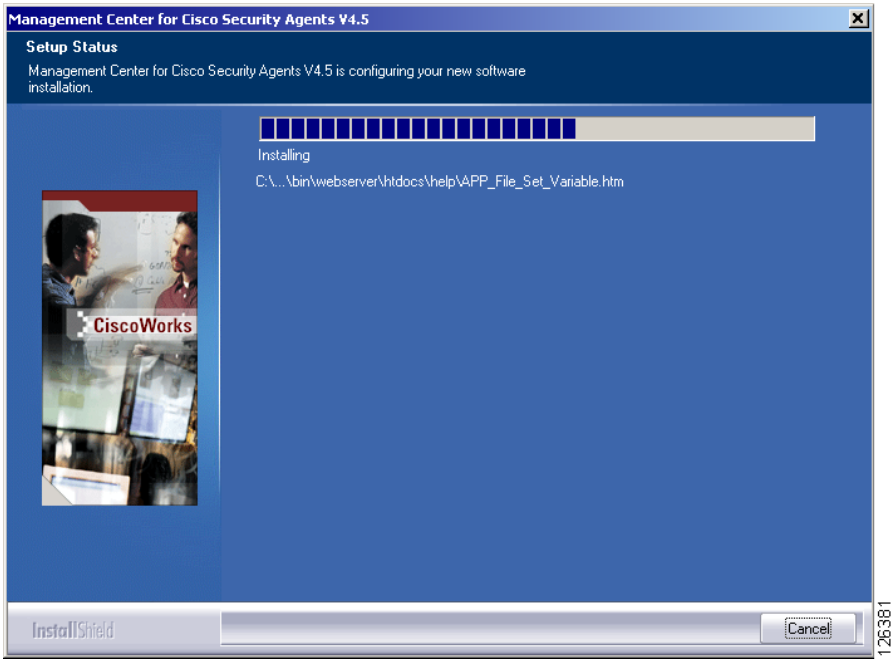


Figure 3-12 Copy Files



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.)

You are prompted to reboot the system after the CSA MC protecting agent installation is complete. The reboot occurs automatically after 5 minutes.

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. For example, in a configuration with 2 MCs, you *must* first *stop* the CiscoWorks Daemon Manager (`net stop crmdmgtd`) on one MC before you install the other MC.

Installation Log

The installation of CSA MC produces a log file. This log file, called "CSAMC-Install.log" and located in the CSCOpx\CSAMC45\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 Security Agent category becomes available in the left pane of the CiscoWorks UI. Cisco Security Agent management screens are accessible from the CiscoWorks VPN/Security Management Solution "drawer". Security Agents (the category by which you access the CSA MC UI) are located in the Management Center and Administration>Management Center folders.

Note Refer to the Using CiscoWorks Common Services manual for CiscoWorks installation instructions and login information.

Local Access

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

- From the **Start** menu, go to **Programs>CiscoWorks>CiscoWorks** to open the CiscoWorks 2000 management UI.
- Login to CiscoWorks. To access CSA MC, open the **VPN/Security Management Solution** "drawer". The **Security Agents 4.5** item is located in the **Management Center and Administration>Management Center** folders. See Figure 3-13.

Note See Initiating Secure Communications, page 3-29 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:

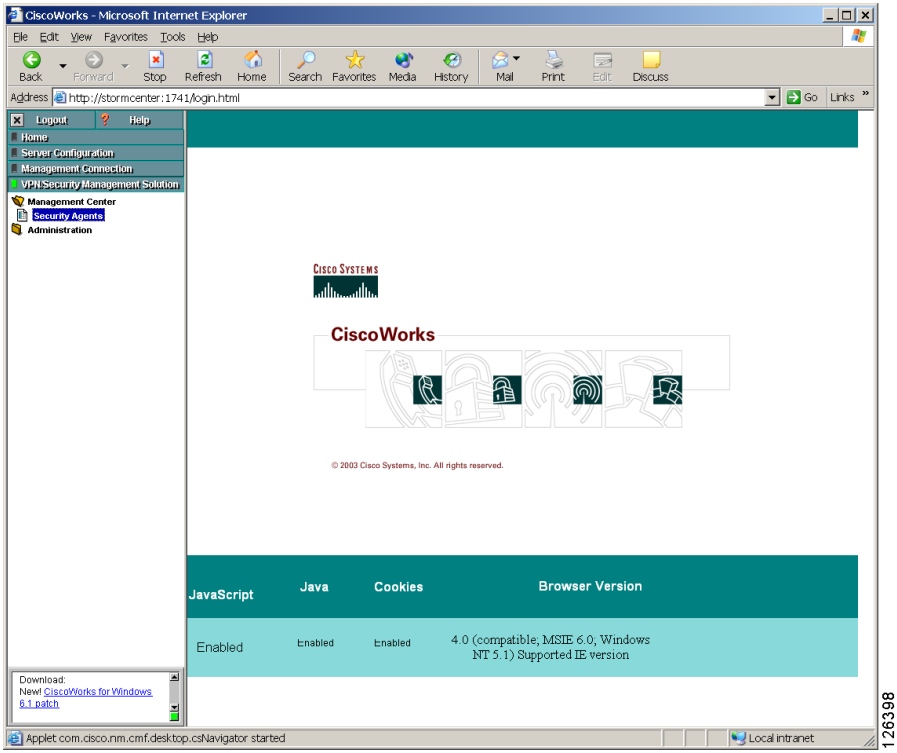
  `http://<ciscoworks system hostname>:1741`

  in the Address or Location field (depending on the browser you're using) to access the Login view.

For example, enter `http://stormcenter:1741`

Note In this example, the CiscoWorks and CSA MC are installed on a host system with the name stormcenter.

Figure 3-13 CiscoWorks Main Page



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 CiscoWorks UI. From the **VPN/Security Management Solution** drawer, expand the **Administration** folder and click the **Import Root Certificate** item. See Figure 3-14.

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

Step 3 The certificate information box appears (see Figure 3-15). 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 3-14 Import Root Certificate

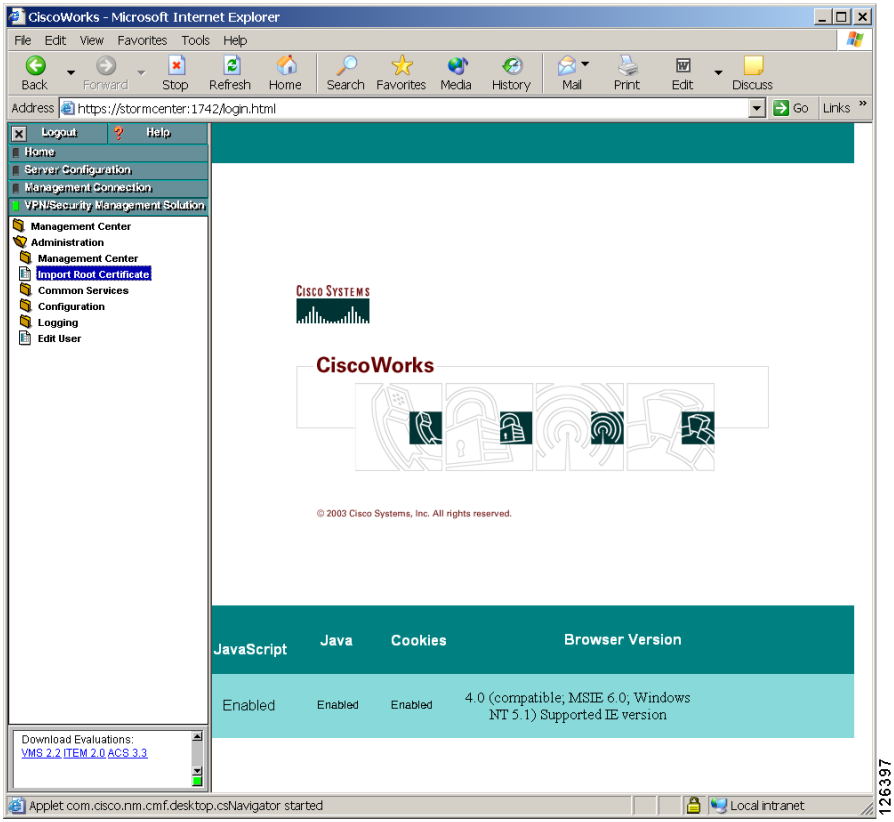
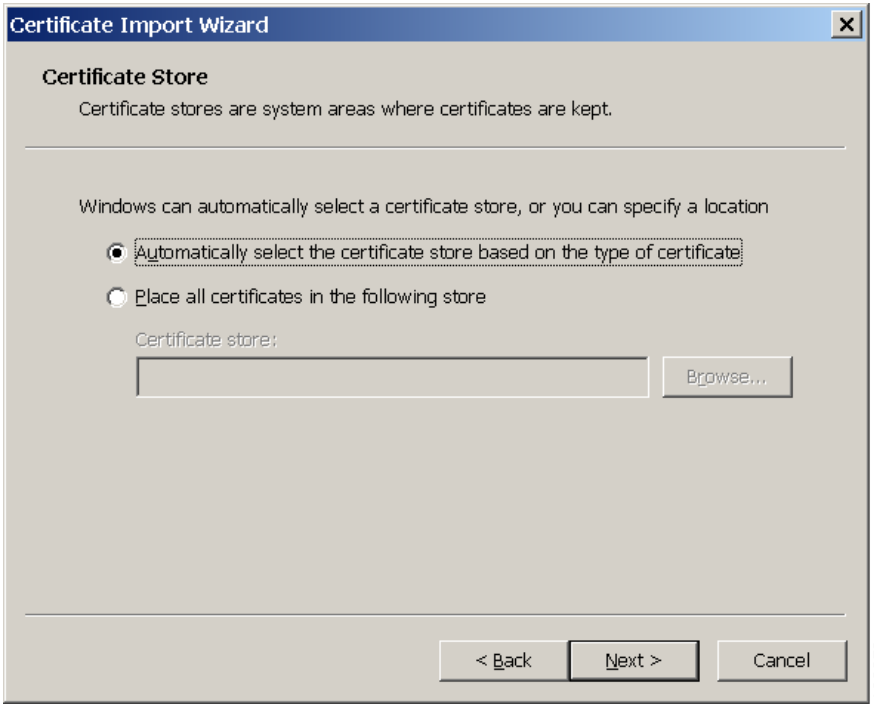


Figure 3-15 Certificate Information

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

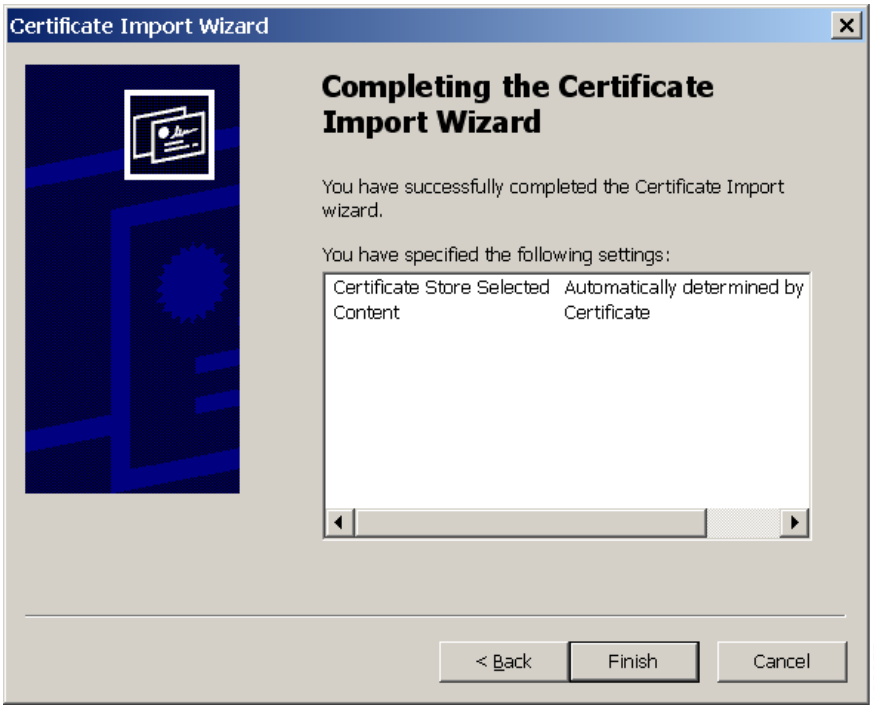
Step 5 From the Select a Certificate Store page, make sure the **Automatically select the certificate store based on the type of certificate** radio button is selected. Click **Next**.

Figure 3-16 Certificate Wizard



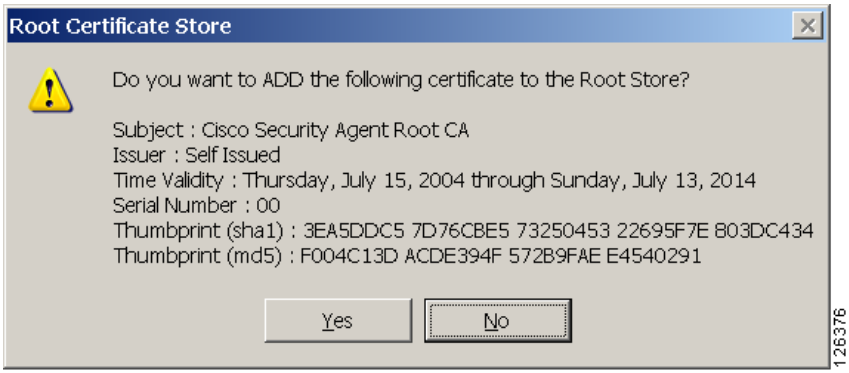
Step 6 You've now imported your certificate for the server. Click the **Finish** button (Figure 3-17) to continue.

Figure 3-17 Certificate Wizard Finish Page



Step 7 Now, you must save the certificate. Click the **Yes** button in the Root Certificate Store box (see Figure 3-18).

Figure 3-18 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 3-15). 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://<ciscoworks system hostname>:1741
```

For example, enter `http://stormcenter:1741`

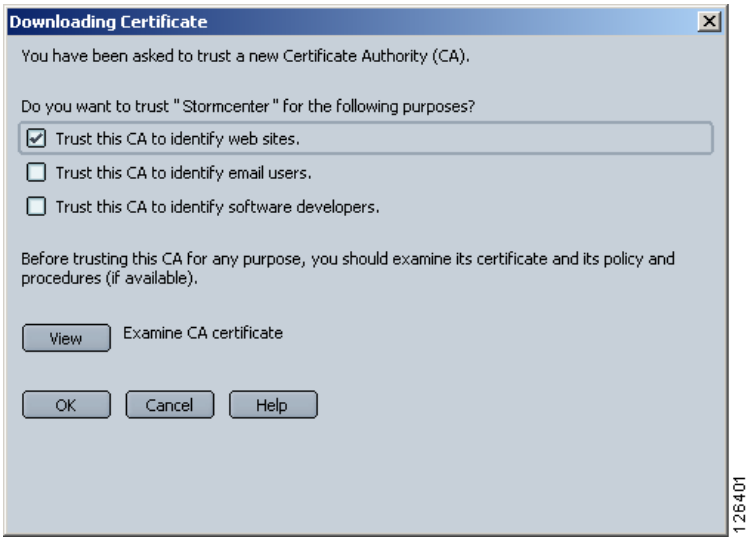
Caution If you have not obtained a valid license from Cisco, when you login to CSA MC, you'll receive a warning informing you that your license is not valid. Refer back to page 3-2 for further licensing information.

Netscape: Importing the Root Certificate

Step 1 You import the certificate from the CiscoWorks UI. From the **VPN/Security Management Solution** drawer, expand the **Administration** folder and click the **Import Root Certificate** item. See Figure 3-14.

Step 2 In the Downloading Certificate window, select the **Trust this CA to identify web sites** checkbox.

Figure 3-19 Downloading Certificate Window



Step 3 Click **OK** to import the certificate.

Note You should 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 without further certificate prompts.

Uninstalling Management Center for Cisco Security Agents

Uninstall the CSA MC software as follows:

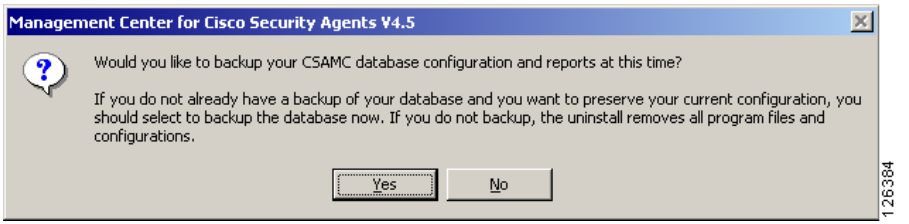
Step 1 From **Start>Settings>Control Panel**, access the **Add/Remove Programs** window. Locate the **CiscoWorks** item and click **Change/Remove**.

Step 2 From the window that appears, select the appropriate checkbox to remove the **Management Center for Cisco Security Agents** program item and click **Uninstall**. This also removes the Cisco Security Agent and Cisco Security Agent Profiler programs on the CSA 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.)

Figure 3-20 Backup Database Prompt



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, install your desired CTA installer files on the system running CSA MC.

To install 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%\CSCOpx\CSAMC45\cfg\cta** directory.

Step 3 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.

Quick Start Configuration

Overview

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

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

This section contains the following topics.

- Access Management Center for Cisco Security Agents, page 4-2
- CiscoWorks Administrator Roles in CSA MC, page 4-3
- Cisco Security Agent Policies, page 4-4
- Configure a Group, page 4-5
- Creating Agent Kits, page 4-7
- The Cisco Security Agent, page 4-12
- View Registered Hosts, page 4-13
- Configure a Rule Module, page 4-14
- Configure a Policy, page 4-20
- Attach a Rule Module to a Policy, page 4-21

- Attach a Policy to a Group, page 4-21
- Generate Rule Programs, page 4-22

Access Management Center for Cisco Security Agents

You access CSA MC from the CiscoWorks UI. An initial administrator account was created as part of the CiscoWorks installation process. Once that administrator account is entered to login into CiscoWorks, it is not necessary to login again to CSA MC.

- To access CSA MC locally on the system hosting CSA MC software, launch the CiscoWorks UI from **Start> Programs>CiscoWorks>CiscoWorks**. Login into CiscoWorks.
- To access CSA MC from a remote location, launch a browser application and enter

  `http://<ciscoworks system hostname>:1741`

  For example, enter `http://stormcenter:1741`

- From the CiscoWorks UI, the Security Agents item is located in the VPN/Security Management Solution “drawer.” Expand the **Management Center** or the **Administration>Management Center** folders.

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.

CiscoWorks Administrator Roles in CSA MC

Administrators can have different levels of CSA MC database access privileges. The initial administrator created by the CiscoWorks installation automatically has configuration privileges.

CiscoWorks/CSA MC Administrator Roles:

- Configure—If the CiscoWorks administrator has the Network Administrator or System Administrator option enabled, this provides full read and write access to the CSA MC database.
- Deploy—If the CiscoWorks administrator has only the Network Operations option enabled, 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—If the CiscoWorks administrator has none of the roles listed in the first two bullets enabled, this provides administrators with read access to the entire CSA MC database. Administrators can also create reports, alerts, and event sets.

Note To view or edit your CiscoWorks administrator profile, in the CiscoWorks UI go to **Server Configuration>Setup>Security>Modify My Profile**.

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 8 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.

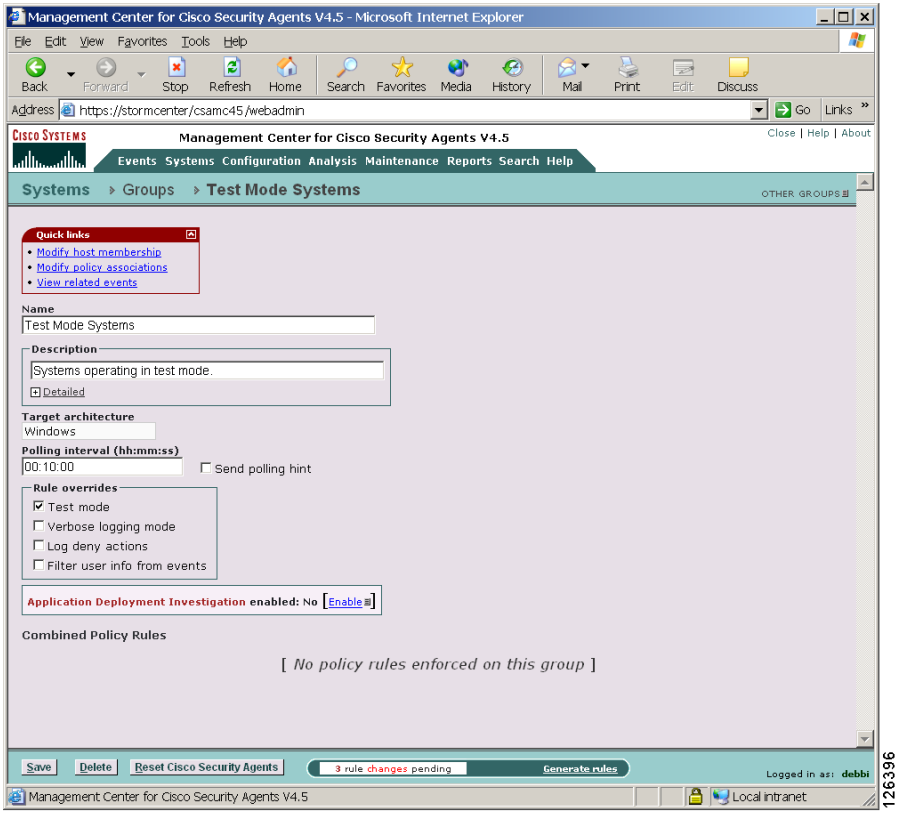
Step 1 Move the mouse over **Systems** in the menu bar of CSA MC and select **Groups** from the drop-down menu that appears. The Groups list view appears.

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.

Creating Agent Kits

The Management Center for Cisco Security Agent allows for the creation of custom agent installation kits that greatly reduce the administrative burden of deploying the agent on new systems. CSA MC also ships with preconfigured agent kits you can use if they meet your initial needs. There are kits for generic desktops, generic servers, and CSA MCs (CiscoWorks VMS). These kits place hosts in the corresponding groups and enforce the associated policies of each group.

At the time of creation of the agent kit, it must be associated with one or more groups. The particular agent kit a host installs determines with what groups(s) the host is associated. You can create as many kits as necessary to distribute your policies to targeted hosts.

After a kit is installed on a host, the agent running on that host registers itself with CSA MC. CSA MC then automatically places the host in the groups that were associated with the installed kit.

Note CSA MC ships with preconfigured agent kits that you can use if they meet your needs. The desktop and server kits are distributed in test mode so they will not interfere with you work before you have had a chance to study their behavior. (If you use a preconfigured agent kit, you do not have to build your own kit as detailed in the following pages.)

To create agent kits, 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. Existing agent kits are displayed.

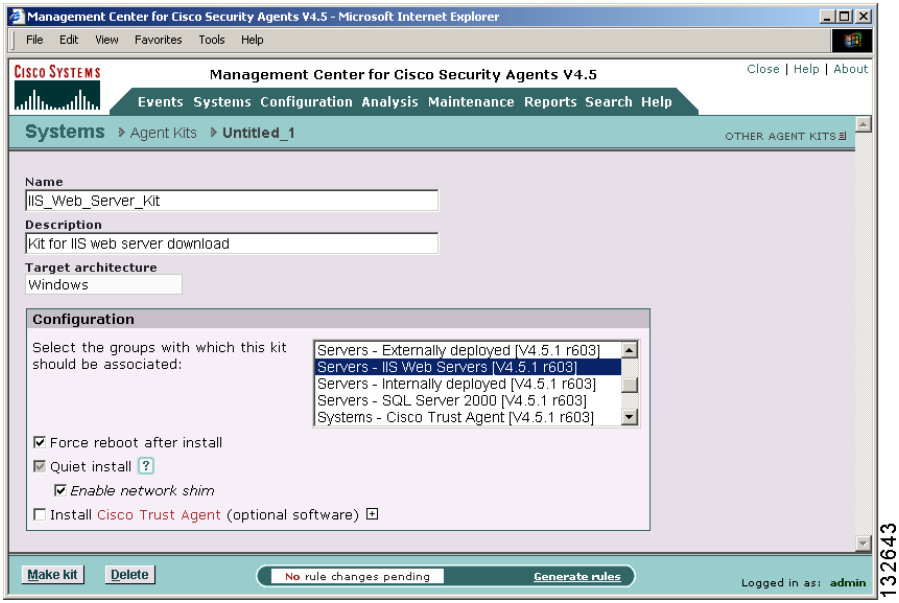
Step 2 Click the **New** button to create a new agent kit.

Note If you have "All" designated as the operating system type for your administrator session, you are prompted to select whether this is a Windows, Linux, or Solaris kit. (You cannot select a Solaris group for an agent kit that you have configured for Windows systems.)

Step 3 In the agent kit configuration view (see Figure 4-2), enter a **Name** for this kit. This must be a unique name. Agent kit names cannot have spaces. Generally, it's a good idea to adopt a naming convention that lets you and the systems that will be downloading the kit, recognize it easily.

Step 4 (Optional) Enter a description in the **Description** field. The description appears in the agent kit list view to help you identify this particular kit.

Figure 4-2 Create Agent Kit



Step 5 From the available list box, select the group or groups of host systems that will download and install this kit. To select multiple items in a list box, hold down the **Ctrl** key as you select each item. To unselect a single item, hold down the **Ctrl** key when you click on the item in question. Press and hold the **Shift** key when you click on an item to select multiple successive items.

Step 6 You have the option of forcing systems to reboot after the agent installation completes (Windows and Linux only). 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 For Windows kits, if you select Quiet install, you can also select whether the **Network shim** is enabled or not during the installation. (See the User Guide for more informatioin on enabling the Network Shim.)

Step 8 Click the **Make Kit** button. A new page opens with the message, "The kit was successfully created."

Step 9 Click the **rule generation** link to advance to the Generate Rule Program page. The rules that require generation are listed at the bottom of the page.

Step 10 Click **Generate** to generate these rules and make your kit available for deployment. Once the generation rules operation completes, you receive the message, "Rule program generation successful."

Step 11 Move the mouse over **Systems** in the menu bar and select **Agent Kits** from the drop-down menu that appears. The agent kit you just created has been added to the list of available kits.

Step 12 Click the name of your new kit to see its agent kit page. The page displays a URL for this particular kit (see Figure 4-3). You may distribute this 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 CiscoWorks system. This URL will allow them to see all kits that are available. That URL is:

```
https://<ciscoworks system name>/csamc45/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. See Figure 4-4.

Note Note that the Registration Control feature also applies to the <ciscoworks system name>/csamc45/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 Agent Kit Download URL

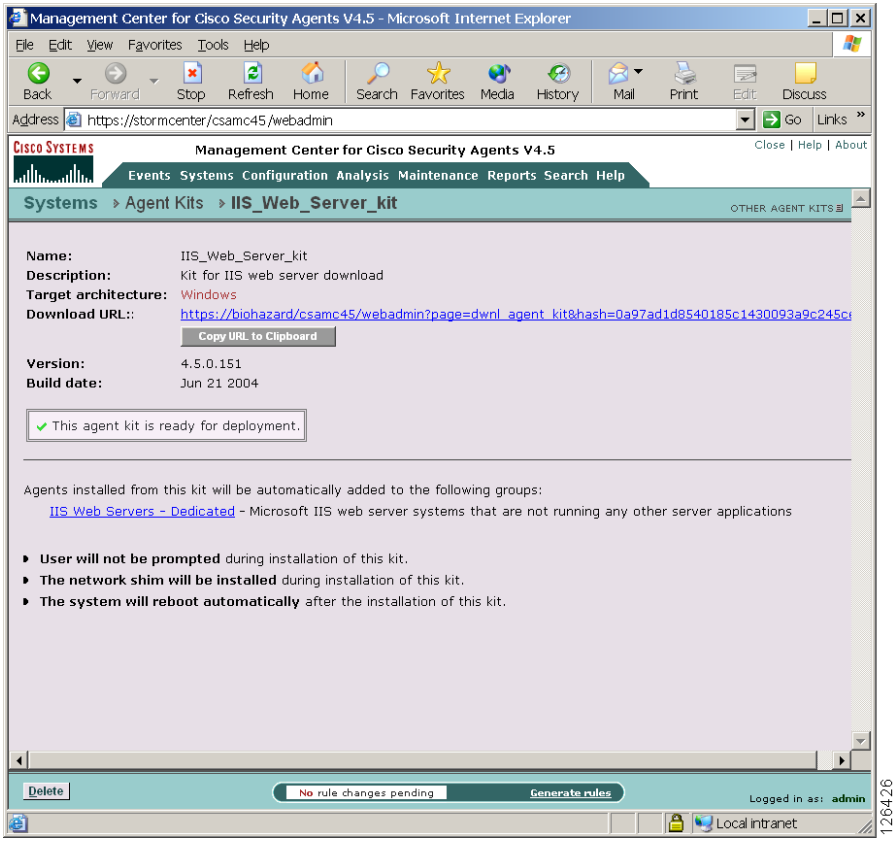
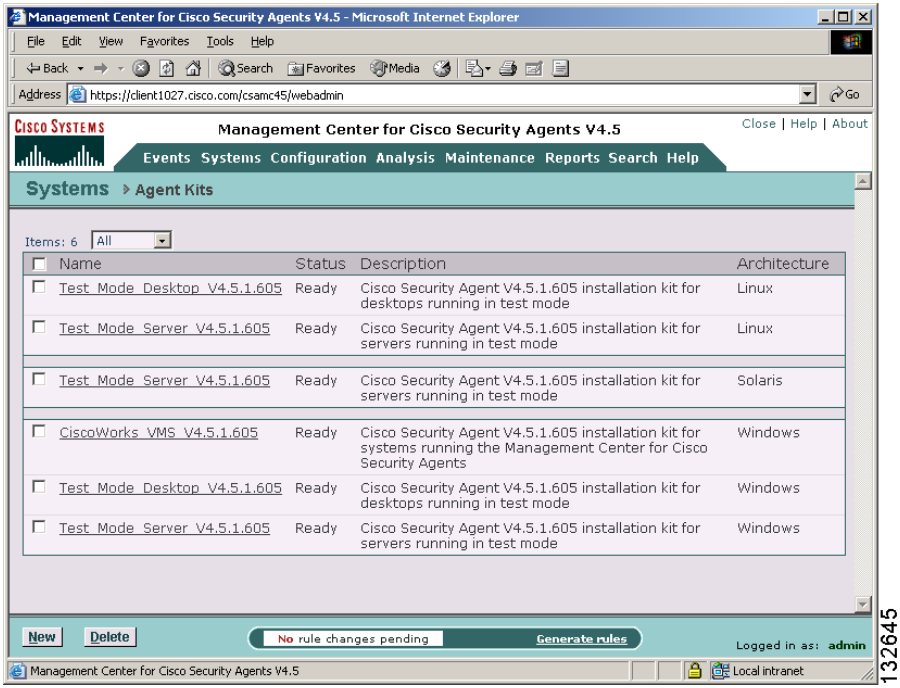


Figure 4-4 Download Agent Kits



The Cisco Security Agent

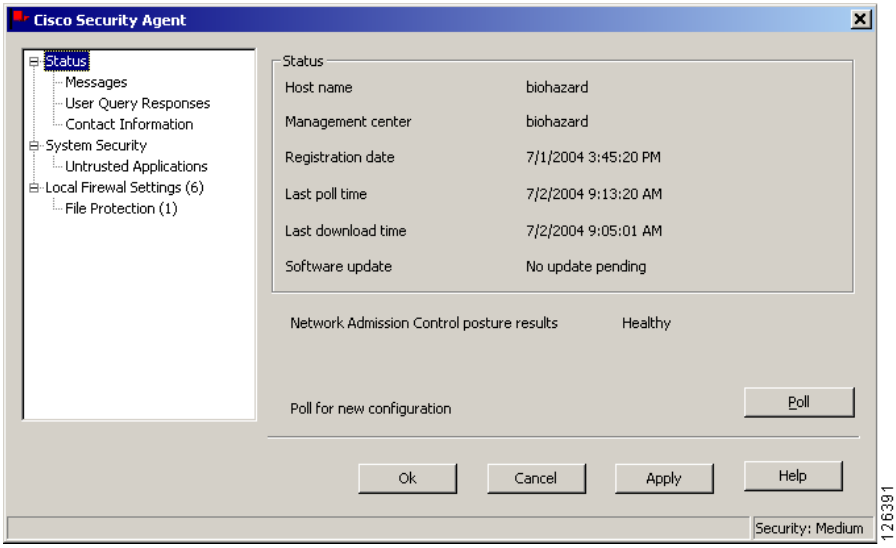
- Users must have administrator privileges on their systems to install the Cisco Security Agent software.
- The Cisco Security Agent installs on supported Windows, Linux, and Solaris platforms. (Note that on Solaris systems there is no agent user interface. See Appendix A in the User Guide for information 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 4-5 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 three 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 4-6.

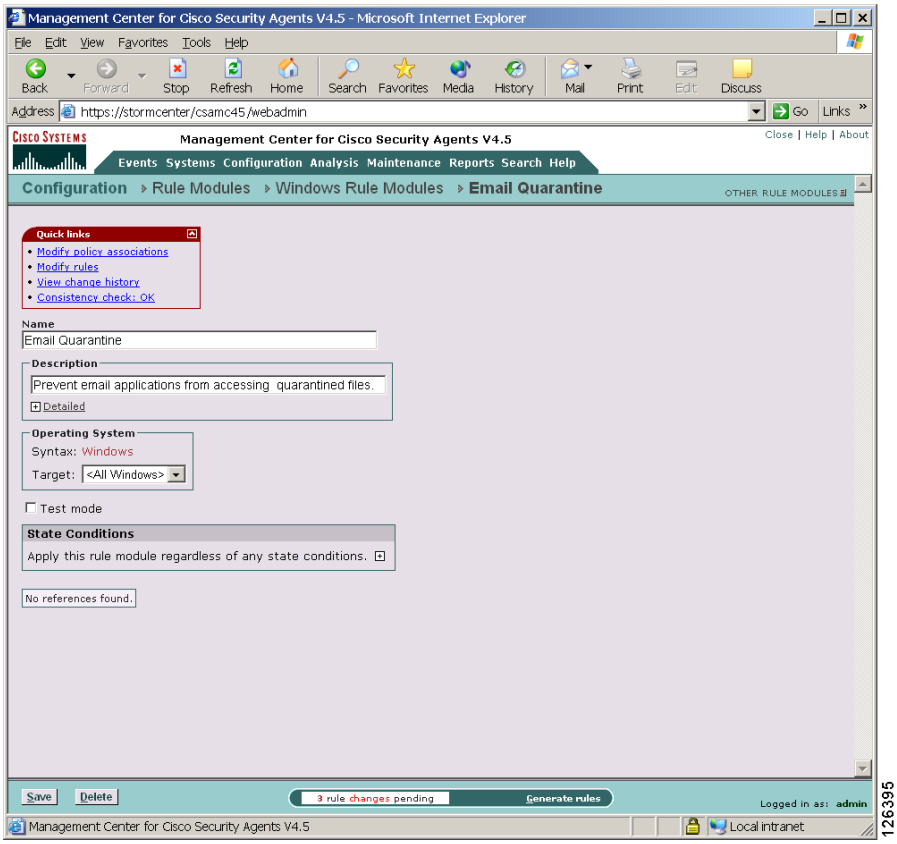
Step 3 In the configuration view, enter the **Name** *Email Quarantine*. Note that names are case insensitive, must start with an alphabetic character, can be up to 64 characters long. Spaces are also allowed in names.

Step 4 Enter a **Description** of your module. We'll enter *Prevent email applications from accessing quarantined files*.

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 4-6 Rule Module Creation View



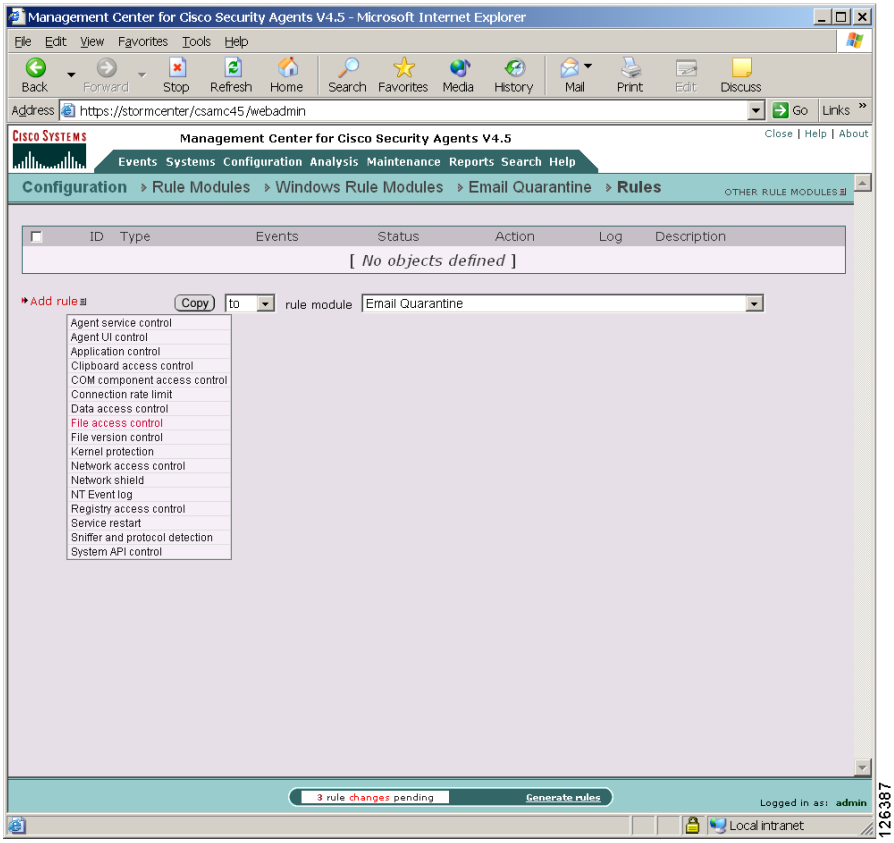
Create a File Access Control Rule

Step 1 From the Rule Module configuration page (Figure 4-6), 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 4-7). This takes you to the configuration page for this rule.

Figure 4-7 Add Rules to Module



Step 4 In the File access control rule configuration view (see Figure 4-8), enter the following information:

- **Description**—Email applications, read/write access for known virus files
- **Enabled**—(This is selected by default. Don't change this setting for this example.)

Step 5 Select **High Priority Deny** from the action pulldown list.
By selecting High Priority Deny here, we are stopping the application 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 **Email applications**. Note that when you click Save, selected application classes move to the top of the list.

Step 8 Select the **Read** and **Write Files** 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 the following:

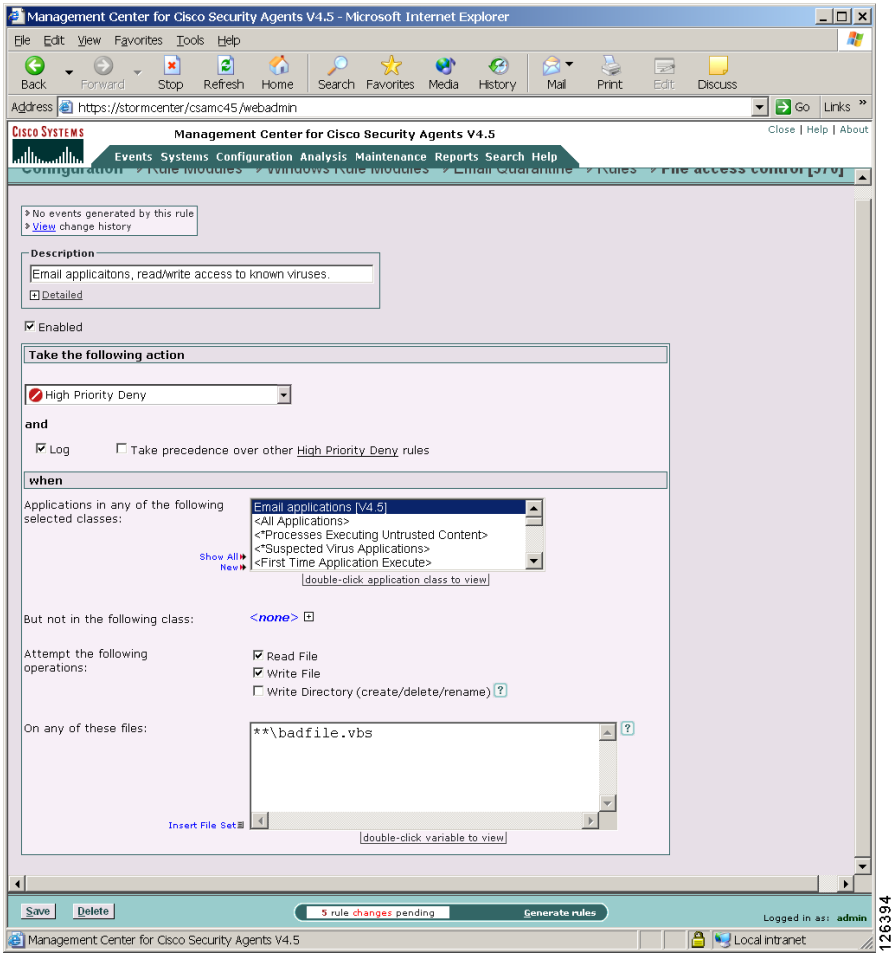
```
**\badfile.vbs
```

It is important to use the correct syntax when specifying files and file pathnames. The User Guide includes a discussion on this subject. In the meantime, in the files field, with this syntax we have indicated all executables in system directories and their subfolders found on any system drive.

Step 10 Click the **Save** button.

Next, we will create a policy to attach our rule module to.

Figure 4-8 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 *Email quarantine*.
- **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 **Email Quarantine** 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.

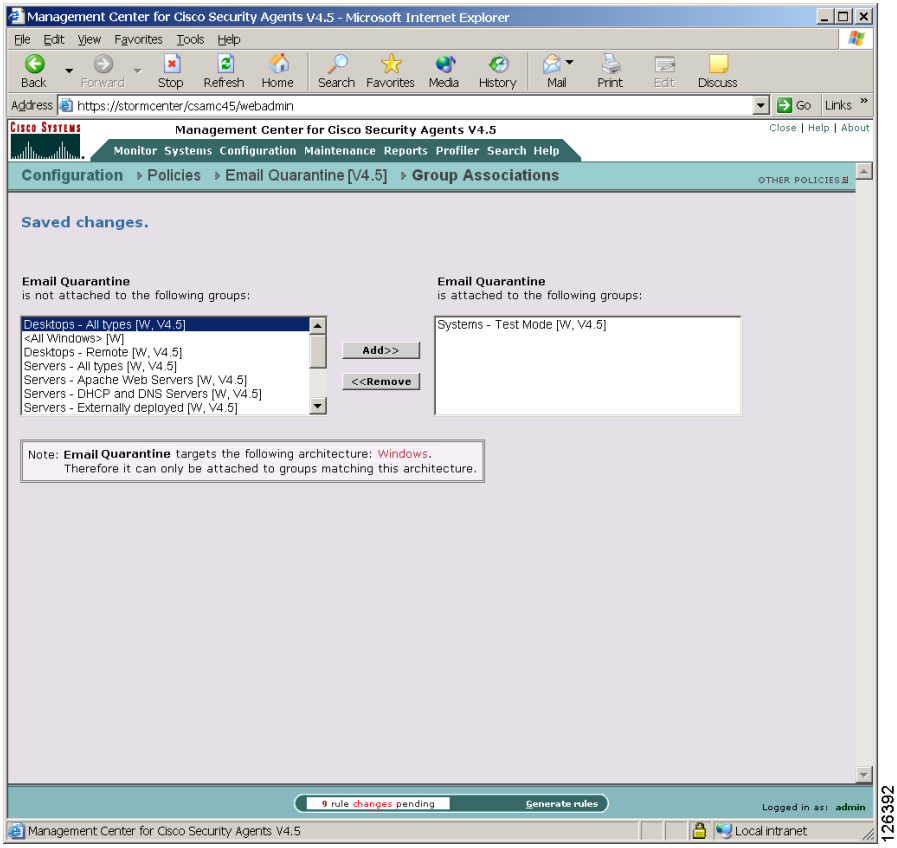
Step 2 From the group list view, click the link for the group you want to attach the policy to. This brings you to that group's edit view.

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 4-9).

Step 4 Select the **Email Quarantine** 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 4-9 Attach Policy to Group



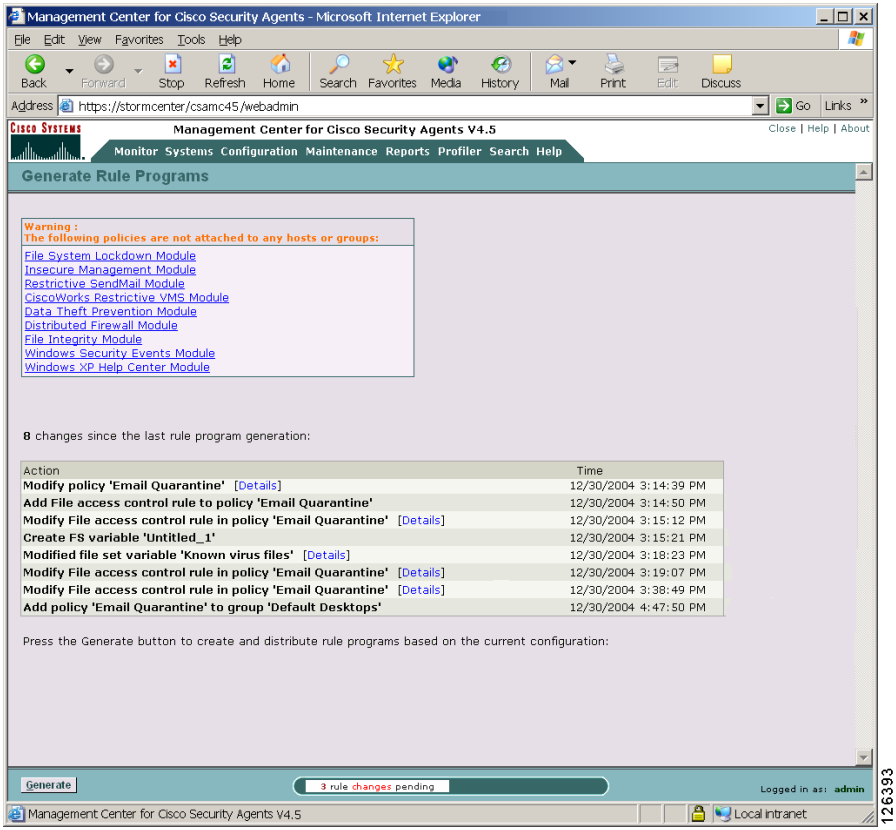
Generate Rule Programs

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 4-10).

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 4-10 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.

Cisco Security Agent Installation and Overview

Overview

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

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

This section contains the following topics.

- Downloading and Installing, page A-2
- Network Shim Optional, page A-2
- The Cisco Security Agent User Interface, page A-5
- Installing the Solaris Agent, page A-7
- Installing the Linux Agent, page A-9

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 CiscoWorks system. This URL will allow them to see all kits that are available. That URL is:

```
https://<ciscoworks system name>/csamc45/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 <ciscoworks system name>/csamc45/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.

Network Shim Optional

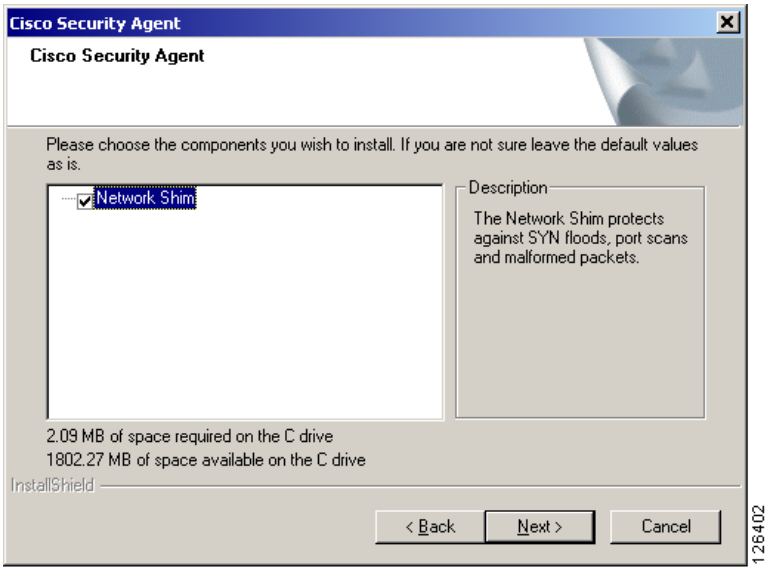
In some circumstances, you may not want users to enable the network shim on their systems as part of the agent installation. (Note that the network shim is not optional on UNIX systems.) For example, if users have VPN software or a personal firewall installed on their systems, the network shim's Portscan detection, SYN flood protection, and malformed packet detection capabilities may be in conflict with VPNs and personal firewalls. (There are no conflicts with the Cisco VPN client.)

If you check the Quiet install checkbox when you make kits, you can also select whether the network shim is installed as part of the Quiet install process.

To allow users to select whether or not to install the network shim themselves, you would create kits as non-quiet installations. (Do not select the Quiet install checkbox.) This way, users are prompted to enable the network shim during the agent installation. See Figure A-1.

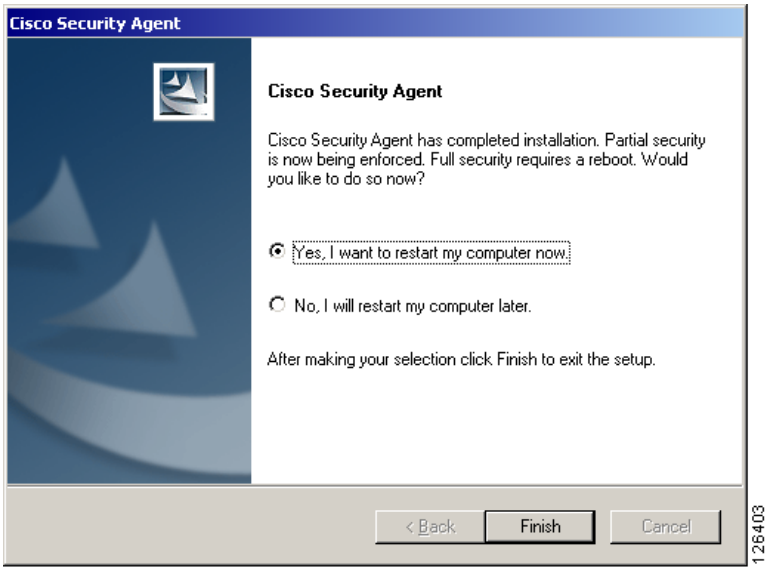
Note Not enabling the network shim does not mean that Network Access Control rules won't work. It only means that the system hardening features are not enabled.

Figure A-1 Optional Network Shim (Windows)



Once users install agents on their systems, they can optionally perform a reboot (if Force reboot is not selected). See Figure A-2. 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-2 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 **agent user interaction** is not enabled (available on Windows and Linux groups 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.

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_V4.5.0.265-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) 4.5.0.15
```

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) 4.5.0.15
```

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_V4.5.0.218-lin-setup-1a969c667ddb0a2d2a8da3e7959
a30b2.tar /tmp
```

Step 2 Untar the file.

```
$ cd /tmp
$ tar xvf
CSA-Server_V4.5.0.218-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-4.5-218
```

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

```
# rpm -ev CSAagent-4.5-218
```

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/VMS 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.

A

Active hosts 4-13
Add rule 4-16
Agent
  kits 4-7
  optional reboot after install A-4
  user interface A-5
Agent (Linux)
  installing A-9
Agent (Solaris)
  installing A-7
  migrating from V4.0.x 3-7
Agent installation automatic 3-25
Agent kit
  preconfigured sample 4-5, 4-20
Agent kits
  creating 4-7
  download URL 4-9
  network shim enable 4-9
  preconfigured sample 4-7
Agent migration 3-6
Agent-server size ratio 2-4
Application class 4-18
Attach policy to group 4-21
Attach rule module to policy 4-21
Auto-enrollment 2-6

B

Browser requirements 1-8
  Java Virtual Machine 1-9

C

Certificate import 3-29
Changes from 4.0.x 2-6, 2-7
  downloaded content 2-6
  mandatory groups 2-6
  monitoring rules 2-6
  network shield 2-6
  network worm detection 2-6
  system API, Trojan rule 2-7
Cisco Security Agent on remote database 3-21
Cisco Trust Agent (CTA) 3-37
  installation files 3-37
Cisco Works 4-9
Cluster support 1-9
Configuration item mapping 2-5
Content engine 2-5

CSA MC 1-3
about 1-2
browser requirements 1-8
login locally 3-27
login remotely 3-27
Policies 4-4
system requirements 1-3

D

Deployment overview 1-2
Detailed description 4-4
Distributed configuration 3-20, 3-26
DNS environments 1-8

F

File access control rule 4-16

G

Generate rules 4-22
Generating configurations 4-22
Group
configure 4-5, 4-20
Polling intervals 4-6
preconfigured sample 4-5, 4-20
Test Mode 4-6
Verbose logging mode 4-6
Groups
No user interaction A-5

H

Hosts
about 4-5
active 4-13
not active 4-13
search 4-13
view 4-13
HTTPS 1-7, A-2

I

IDS Host Sensor 1-16
Import Root Certificate 3-29, 3-35
Inactive hosts 4-13
Install
agent A-2
certificate (IE) 3-29
certificate (Netscape) 3-35
Microsoft SQL Server 3-13
Installation Log 3-26
Installation options 3-10
Install CSA MC 3-9, 3-27
installation options 3-10
license information 3-2
local database 3-11

remote database 3-20
upgrading 3-3, 3-7
Internationalization support 1-9
directory tokens 1-15
verifying directory tokens 1-14
Windows 2000 1-12
Windows 2003 1-14
Windows XP 1-13
Internet Explorer
version support 1-8

J

Java Virtual Machine requirement 1-9

L

Language support 1-9
directory tokens 1-15
verifying directory tokens 1-14
Windows 2000 1-12
Windows 2003 1-14
Windows XP 1-13
Licensing information 3-2
Local database install 3-10
Log
installation 3-26
Login
locally 3-27
remotely 3-27

M

Make kit button 4-9
Microsoft SQL Server 3-14
migration_data_export.xml 3-5

N

Netscape
version support 1-8
Network shim 4-9
optional A-2
Not active hosts 4-13
No user interaction A-5

O

Operating system changes, agent 1-8
Operating systems sample 2-2
Overview of product 1-1

P

Pilot
migrating policies 2-5
recommendations 2-2
Pilot Program

size of pilot 2-2
time frame of pilot 2-3
Policies
pre-configured modules 4-4
Policy
add rule 4-16
attach to group 4-21
configure 4-14
distribute to agents 4-22
exception rules 2-13
file access control 4-16
modify policy associations 4-21
modify rules 4-16
query responses 2-12
rule modules 4-14
Test Mode as a tool 2-10
tuning and troubleshooting 2-7
Policy migration 2-5
Polling interval recommendation 2-5
Polling intervals 4-6
prepare_migration.exe 3-5
Product overview 1-1

Q

query settings 2-7
Quick start setup 4-1

R

Reboot optional
agent A-3, A-4
Registered hosts
view 4-13
Remote access 3-27, 4-2
Remote database install 3-10
Requirements
agent 1-5
cluster support 1-9
DNS and WINS 1-8
server 1-3
time and date settings 1-9
web browsers 1-8
Resolution
screen requirements 1-4
Root certificate import 3-29
Rule configuration version 4-23

S

Scalability
hardware sizing 2-3
server configurations 2-3
Scalable deployment 2-3
content engines 2-5
hardware sizing 2-3
polling interval 2-5

three servers 2-3
Secure communications 3-29
Single server 2-3
Solaris agent install directory A-8
Solaris host migration 3-7
Solaris requirements
agent 1-6
SQL Server 3-14
SQL Server 2000 install 3-19, 3-21
SQL server installation 3-15
SSL 3-18, 3-29
Syntax 4-18
System requirements 1-3

T

Terminal services 1-5
Test Mode 4-6
Three servers, multi-tiered 2-3
Two servers 2-3

U

Uninstall CSA MC 3-36
UNIX agent install directory A-8
Upgrade naming conventions 3-5
Upgrading
configuration item mapping 2-5
from Version4.0.x 3-3, 3-7

V

Verbose logging mode 4-6
Version labels 3-5

W

Web-based user interface 1-2, 1-17
Web browser
requirements 1-8
Windows Cluster support 1-9
Windows requirements
agent 1-5
WINS environments 1-8