Cisco Systems

Installing Management Center for Cisco Security Agents 4.0

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: OL-3956-01

Installing Management Center for Cisco Security Agents 4.0

CONTENTS

APPENDIX C

INDEX

Preface

Objectives

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

In addition to the information contained in this manual, consult the release notes for the latest information on the current release. Note that this manual does not provide tutorial information on the use of Windows and Solaris operating systems.

Intended Audience

This manual is intended for system managers or network administrators responsible for installing, configuring, and maintaining Management Center for Cisco Security Agents software. It is assumed that installers have a solid grounding in networking concepts and system management and have experience installing software on Windows operating systems.

Typographical Conventions

This manual uses the following conventions.

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

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

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

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

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

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

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

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

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) 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. On the Cisco Documentation home page, click **Feedback** at the top of the page.

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- 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

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, 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 website. Some services on the Cisco TAC website require 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://tools.cisco.com/RPF/register/register.do

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

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

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

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 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 quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

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

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

- Training—Cisco offers world-class networking training. Current offerings in network training are 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 intrinsic, distributed security to your enterprise by deploying agents that defend against the proliferation of attacks across networks and systems. These agents operate using a set of rules provided by the Management Center for Cisco Security Agents and selectively assigned to each client node on your network by the network administrator.

This section includes the following topics.

- Cisco Security Agent Overview, page 1-2
- Before Proceeding, page 1-3
- System Requirements, page 1-3
- CSA MC Local Agent and Policies, page 1-8
- RME Gatekeeper Remote Access Issue, page 1-9
- Installation Note, page 1-9
- About CSA MC, page 1-10

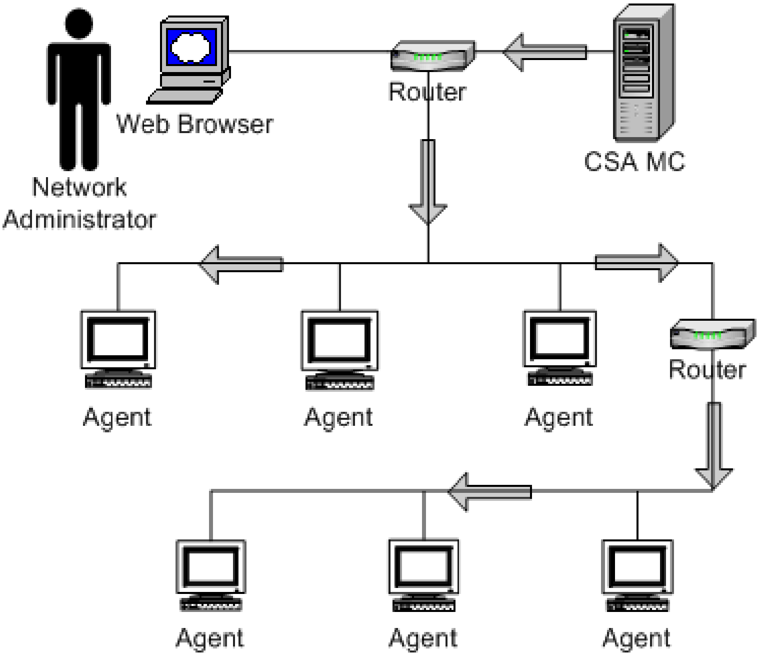
Cisco Security Agent Overview

Cisco Security Agent product 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).

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 Professional, Server, or Advanced Server (Service Pack 3) Note: Support for Advanced Server requires turning Terminal Services off.
File System	NTFS
Memory	1 GB minimum memory

Table 1-1 Server Requirements (continued)

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.

- 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 3. 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.

To run the Cisco Security Agent on your Windows XP, Windows 2000 or Windows NT 4.0 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 and dual processor systems are supported
Operating Systems	• Windows XP (Professional English128 bit) Service Pack 0 or 1 • Windows 2000 (Professional, Server or Advanced Server) with Service Pack 0, 1, 2, or 3 • Windows NT (Workstation, Server or Enterprise Server) with Service Pack 5 or higher **Note** Terminal Services are supported on Windows XP and Windows 2000 (Terminal Services are not supported on Windows NT.)
Memory	128 MB minimum—all supported Windows platforms
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.

Note The Cisco Security Agent uses approximately 20 MB of memory. This applies to agents running on all supported Microsoft platforms.

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

Table 1-3 Agent Requirements (UNIX)

System Component	Requirement
Processor	UltraSPARC 500 MHz or higher **Note** Uni-processor and dual processor systems are supported
Operating Systems	Solaris 8, 64 bit **Note** If you have the minimal Sun Solaris 8 installation (Core group) on the system to which you are installing the agent, the Solaris machine will be missing certain libraries and utilities the agent requires. Before you install the agent, you must install the "SUNWlibCx" library which can be found on the Solaris 8 Software disc (1 of 2) in the /Solaris_8/Product directory. Install using the pkgadd -d . SUNWlibCx command.
Memory	256 MB minimum
Hard Drive Space	15 MB or higher **Note** This includes program and data.
Network	Ethernet **Note** Maximum of 64 IP addresses supported on a system.

Caution On UNIX 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.

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 5.5 or higher
- 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 6.2 or higher
- You must have cookies enabled. Locate this feature from the following menu, Edit>Preferences>Advanced.
- JavaScript must be enabled.

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

CSA MC Local Agent and Policies

When you install CSA MC, an agent containing the policies necessary to protect CSA MC and other CiscoWorks daemons and operations is automatically installed as well. The policies that are enforced by this agent protect CSA MC, other VMS products, and general CiscoWorks operations.

If you are only running CSA MC and SecMon as part of your VMS bundle on the CiscoWorks system, you can lock down that system with a more restrictive policy that is also shipped with CSA MC but not attached to the CiscoWorks group by default. To do this, you should create a new group and attach the following policies to that new group: “CiscoWorks Restrictive VMS Module”, “CiscoWorks VMS Module”, and the “CiscoWorks Base Security Module.” Then make the CSA MC host a member of the new group (in addition to the default group to which it already belongs). This restrictive policy puts tighter restrictions on the system because it does not have to account for other VMS bundle products that might be running on the system.

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.

RME Gatekeeper Remote Access Issue

Remote access to the CiscoWorks RME Gatekeeper daemon is not required for correct operation of any of the components in the VMS bundle. Therefore, remote client access to this daemon is normally disabled through a deny rule in the "CiscoWorks VMS module" policy.

If other products that require the RME Gatekeeper daemon to be accessed remotely, such as Campus Manager or ACLM, are installed on the same system as the VMS bundle, the CSAMC "CiscoWorks VMS module" policy protecting the VMS system should be modified as follows:

Step 1 Login to CSAMC and navigate to the "CiscoWorks VMS module" policy. The policy is accessible from **Configuration>Policies** in the menu bar.

Step 2 Once you locate the policy, click the **<#>rules** link to access the policy rules list.

Step 3 Change the Allow rule "CiscoWorks RME Gatekeeper daemon, server for TCP and UDP services" from Disabled to Enabled. (Select the checkbox beside the rule and click the Enable button in the footer frame of CSAMC. Remember to save your changes.)

Step 4 Generate rules.

Optionally, force polling on the agent to download the rule change.

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:

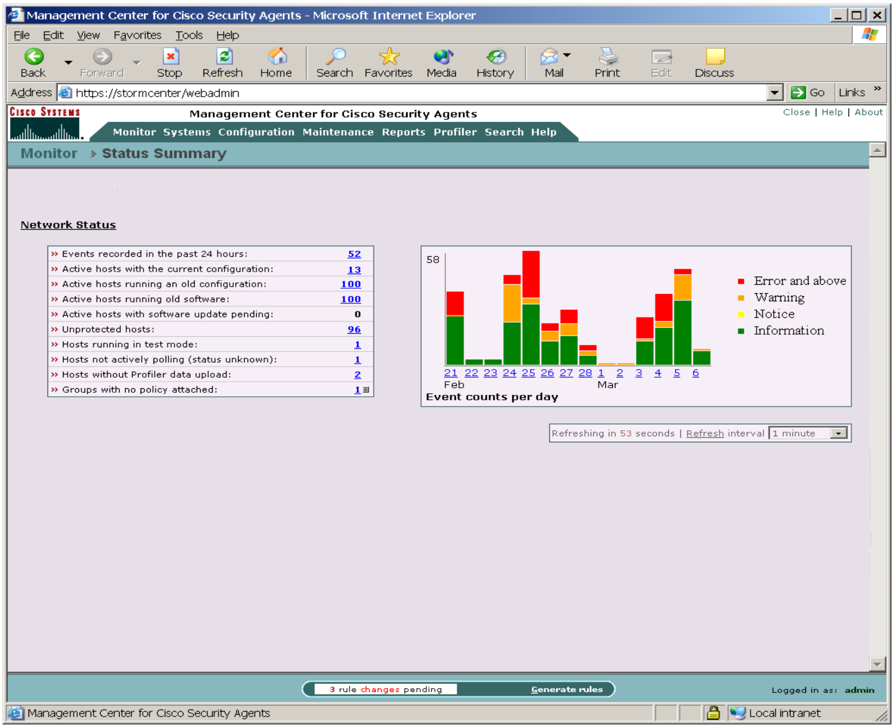
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/host/host25/install/hidsch2.htm#1024883

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 1-2 CSA MC, Top Level View


Management Center for Cisco Security Agents - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Mail Print Edit Discuss
Address https://stormcenter/webadmin
Go Links
Cisco Systems
Management Center for Cisco Security Agents
Close | Help | About
Monitor Systems Configuration Maintenance Reports Profiler Search Help
Monitor › Status Summary

Network Status

» Events recorded in the past 24 hours:	52
» Active hosts with the current configuration:	13
» Active hosts running an old configuration:	100
» Active hosts running old software:	100
» Active hosts with software update pending:	0
» Unprotected hosts:	96
» Hosts running in test mode:	1
» Hosts not actively polling (status unknown):	1
» Hosts without Profiler data upload:	2
» Groups with no policy attached:	1

Refreshing in 53 seconds | Refresh interval 1 minute

3 rule changes pending

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 2-2
- Upgrading from Version 3.x, page 2-3
- Installing Management Center for Cisco Security Agents, page 2-11
- Accessing Management Center for Cisco Security Agents, page 2-18
- Initiating Secure Communications, page 2-20
- Uninstalling Management Center for Cisco Security Agents, page 2-29

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 products 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 and whether you are licensed to use the Cisco Security Agent Profiler feature. Profiler is licensed separately (see the User Guide for Profiler feature details).

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 3.x

Upgrading from versions of the product earlier than version 3.1 to version 4.0 is not supported.

Caution The specifications (memory, disk space) for the system to which you are installing Management Center for Cisco Security Agents are different from the system specifications StormWatch V3.x required. Therefore, make sure the StormWatch system you are planning to upgrade meets the new V4.0 specifications. If it does not, you must either install Management Center for Cisco Security Agents to a new machine that meets system requirements and not perform the upgrade or move your StormWatch V3.x configuration to the new machine that meets system requirements and then perform the upgrade. If you want to do the latter, refer to the instructions Moving StormWatch V3.x and Then Upgrading, page 2-6

Caution The Management Center for Cisco Security Agents V4.0 (CSA MC) requires either MSDE with at least Service Pack 3 or SQL Server 2000 with at least Service Pack 3.

If you were using StormWatch V3.x and you did not upgrade your version of MSDE to at least Service Pack 3, the CSA MC V4.0 installation will detect this and abort. At this point, you can uninstall MSDE and begin the CSA MC installation again. CSA MC installs MSDE with SP3 and it will use the V3.x configuration files that remain on the system to populate the database. You do not lose your existing policies or other configuration items.

If you were using StormWatch V3.x with SQL Server 2000 and you did not upgrade to SQL Server 2000 Service Pack 3, the CSA MC V4.0 installation aborts. You must upgrade to at least SQL Server 2000 SP3 and then you can begin the CSA MC V4.0 installation again. See Microsoft SQL Server 2000 Installation Notes, page 2-17 for information.

To upgrade from StormWatch V3.x to Management Center for Cisco Security Agents 4.0, you must do the following on the StormWatch system:

Step 1 Uninstall StormFront, if present.

Step 2 Uninstall the StormWatch agent, if present on the StormWatch server system.

Step 3 Uninstall the StormWatch Management Console. Your database (including policies) is preserved when you perform this uninstall.

Step 4 Install CiscoWorks Common Services.

Note After upgrading from V3.x to V4.0, all pre-existing administrator usernames and passwords will NO LONGER BE VALID. CiscoWorks has it's own login schema and you will have to create usernames and passwords for CiscoWorks. During the installation of CiscoWorks Common Services you are prompted to create a username and password. You can then log into CiscoWorks and create additional usernames and passwords.

Step 5 Install the Management Center for Cisco Security Agents. See page 2-11 for instructions.

Note Create new agent kits as appropriate. Existing V3.x Windows agents will need to perform software updates to 4.0. Note that existing V3.x agents (Windows and UNIX) will continue to function with the new CSA MC but their policies should not be changed until software updates or new agent installations are performed.

Caution StormWatch V3.x UNIX agents are NOT upgradable. You must uninstall V3.x UNIX agents and reinstall new Cisco Security Agents V4.0 for UNIX per the procedure Upgrading UNIX Agents, page 2-5.

Upgrading Windows Agents

After upgrading to CSA MC V4.0, you should perform the following tasks to update your existing Windows agents with the appropriate 4.0 functionality.

Step 1 Associate hosts with the appropriate new 4.0 groups (if necessary).

An upgrade does not replace your existing database configuration with a new configuration. Rather it renames existing items and populates the database with new 4.0 items. (See Duplicate Configuration Naming Convention, page 2-10). Any changes made to shipped policies, via the wizard or manually, are not automatically copied to new versions of policies added by the upgrade. For example, existing agents in the Default Desktops group may now be associated with the Default Desktops_V3.2 group. This is the same group, but it was renamed during the upgrade.

To deploy upgraded policies, associate hosts with the appropriate groups for the current version. To apply new 4.0 Desktop policy functionality to these agents, you must reassociate them with the Default Desktops group (no version number). This is the appropriate 4.0 group.

Step 2 Schedule software updates for existing V3.x agents.

Step 3 Generate rules.

Upgrading UNIX Agents

StormWatch V3.x UNIX agents are NOT upgradable. You must uninstall V3.x UNIX agents and reinstall new Cisco Security Agents V4.0 for UNIX. After upgrading to CSA MC V4.0, you should perform the following tasks to update your existing UNIX agents with the appropriate 4.0 functionality as follows.

Step 1 Download a V4.0 UNIX agent from CSA MC as if it were a new installation.

Step 2 Stop the V3.x UNIX StormWatch agent service with a `/etc/init.d/stormwatch stop` command.

Step 3 Uninstall the V3.x UNIX StormWatch agent with a `pkgrm OKENAswa` command.

Step 4 When the uninstall completes, reboot the system.

Step 5 Extract the V4.0 UNIX agent from the tar file.

```
# tar xf CSA-Server_4.0.0.15-setup.tar
```

Step 6 Perform a pkgadd on the V4.0 agent as if it were a new installation.

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

Step 7 Copy the following V3.x StormWatch agent configuration files to their new locations. (This example uses paths for StormWatch V3.2.)

Copy /opt/OKENAswa/3.2/cfg/agent.state to /opt/CSCOcsa/cfg/agent.state

Copy /opt/OKENAswa/3.2/cfg/syslog.state to /opt/CSCOcsa/cfg/syslog.state

Step 8 Reboot the machine to provide full security coverage.

Moving StormWatch V3.x and Then Upgrading

If you do not have sufficient hardware or other required V4.0 specifications, use the following procedure to move the StormWatch Management Console V3.x to a new system that meets specifications and to then upgrade it to Management Center for Cisco Security Agents V4.0. If you already have sufficient hardware with enough memory (minimum of 1 GIG) for your V4.0 installation and will not be moving StormWatch V3.x to another machine, go to Upgrading from Version 3.x, page 2-3.

Note After upgrading from V3.x to V4.0, all pre-existing administrator usernames and passwords will NO LONGER BE VALID. CiscoWorks has it's own login schema and you will have to create usernames and passwords for CiscoWorks. During the installation of CiscoWorks Common Services you are prompted to create a username and password. You can then log into CiscoWorks and create additional usernames and passwords.

Caution You MUST remember the passphrase you created during the initial installation of the StormWatch Management Console V3.x if you are going to move the StormWatch Management Console from one machine to another.

Prerequisite

You must have a viable configuration backup either on tape backup or other media of at least your Okena directory. Read the appropriate sections of this procedure in its entirety before you proceed with the upgrade.

Key

- Machine A is the original StormWatch Management Console V3.2. (This procedure uses StormWatch V3.2 for the examples given.)
- Machine B is the new machine that you are upgrading to Management Center for Cisco Security Agents V4.0.

Upgrade Procedure

Step 1 Log into Machine A's StormWatch Management Console and initiate the Backup Configuration feature (Maintenance >Backup Configuration).

Note You must choose a local drive for the backup files and you must be at the Management Console machine itself. In addition, the folder you specify must already exist, it will not be automatically created.

The following files are saved to your destination folder when you click the Backup Now button:

- full_backup_stormwatch.bak
- kledia
- *.lic
- sslca.crt
- sslca.csr
- sslca.key
- sslca.sn
- sslhost.crt
- sslhost.csr
- sslhost.key

Step 2 Copy the files listed above to a shared drive so you can copy them locally to Machine B (or burn them to CDs or DVD).

Step 3 Disconnect Machine A from the network.

Step 4 Go to Machine B and name it exactly the same as Machine A.

Step 5 Give Machine B the exact same IP address as Machine A.

Step 6 Optionally, install the full version of Microsoft SQL Server 2000 and Service Pack 3 for Microsoft SQL Server 2000 onto Machine B if you choose to use the full version. Reboot.

Caution If you are not using the full version of Microsoft SQL Server 2000 with Service Pack 3, StormWatch Management Console V3.x installs Microsoft SQL Server 2000 Desktop Engine (MSDE). You must install at least Service Pack 3 for MSDE.

Step 7 Install the StormWatch Management Console V3.2 on Machine B and reboot. Do not install the StormWatch Agent when prompted. Do not install StormFront.

Step 8 Log into the StormWatch Management Console on Machine B to make sure it is working.

Step 9 Copy the files listed in step 1 to a local folder on Machine B.

Step 10 Open a command prompt window and enter `net stop stormwatchserver` on Machine B.

Step 11 On Machine B, locate the `program files\okena\stormwatchserver\3.2\bin` directory and double-click the **Restore Configuration** file located there.

Step 12 In the Restore Configuration window that appears, browse to the folder where you saved the step 1 files on Machine B.

Step 13 Click the **Restore Configuration** Button.

Step 14 Click **OK** when the configuration is restored successfully.

Step 15 Manually copy the following files (which were automatically copied by the backup configuration function) into Machine B's `program files\okena\stormwatchserver\3.2\cfg` directory. You will be prompted that you are about to overwrite files. Go ahead and overwrite the said files.

- kledia
- sslca.crt
- sslca.csr
- sslca.key
- sslca.sn
- sslhost.crt
- sslhost.csr
- sslhost.key

Step 16 Open a command prompt window and run keymgr to recover the keys. Enter the following: `keymgr server recoverkeys -p "passphrase"`
The passphrase is the passphrase you created when you first installed StormWatch Management Console V3.2.

Step 17 Open a command prompt window and enter `net start stormwatchserver` on Machine B.

Step 18 Log into the StormWatch Management Console on Machine B to ensure it is functioning properly.

Step 19 Make sure existing deployed agents can communicate with Machine B by performing a fastpoll or updating host contact information.

Step 20 Proceed to the upgrade instructions detailed in Upgrading from Version 3.x, page 2-3.

Duplicate Configuration Naming Convention

When you upgrade Management Center for Cisco Security Agents, existing configuration items are preserved. This occurs when the upgrade process checks the existing database. If it is found that there is already an existing exact match for an item, the new configuration data is not copied over. Rather the existing one is left as is.

But if the upgrade process finds that there is an existing item with the same name as a new one, but with different configuration components (variables, etc.), the existing item is renamed by appending the version number (V3.2, for example) to the name. The new version is then copied into the database with no version number so that both items can co-exist in the database. Therefore, for any partial configuration item duplications that may exist after an upgrade, the item with no version number appended to its name is always the most recent version.

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. 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 3 installed.

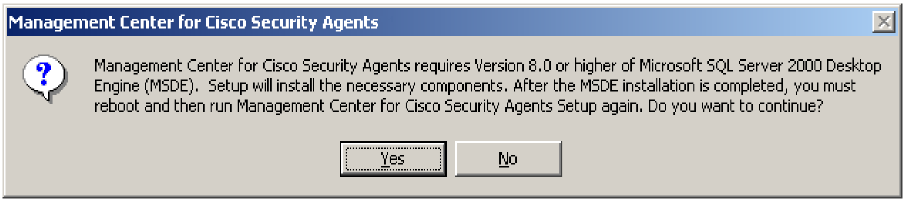
Step 2 Insert the VPN/Security Management Solution CD into the CDROM drive. When the installation screen listing all available VMS products appears, select the checkbox beside **Managing Cisco Security Agents—Servers and Desktops** and click Next to start the installation.

Step 3 The installation first checks to see if you have Microsoft SQL Server Desktop Engine (MSDE) installed. CSA MC uses MSDE for its configuration database. If this software is not detected, you are prompted to install it (see Figure 2-1).

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. Microsoft SQL Server Desktop Engine has a 2 GB limit. Note that SQL Server 2000 must be licensed separately and it must be installed on the system before you begin the CSA MC installation. See Microsoft SQL Server 2000 Installation Notes, page 2-17 for information.

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

Figure 2-1 Install Microsoft SQL Server Desktop Engine

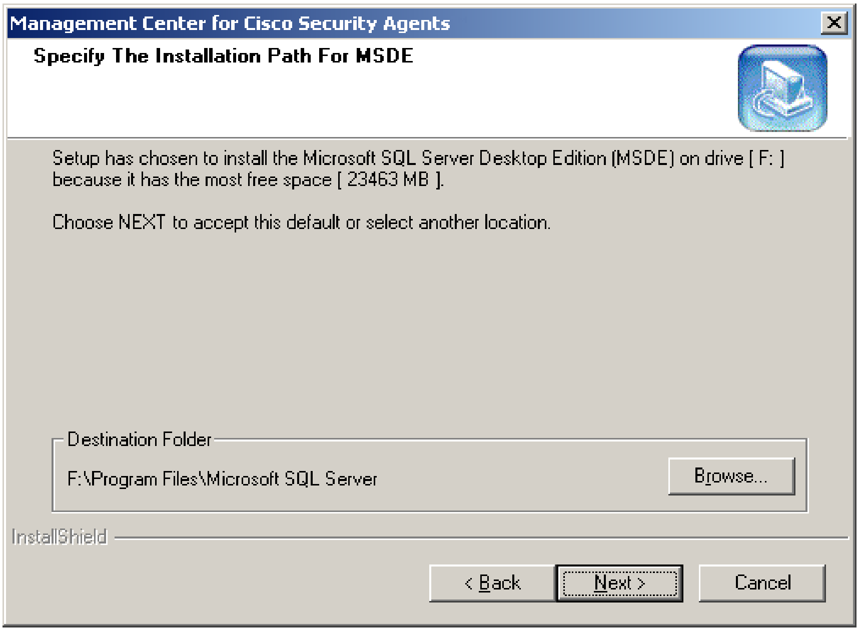

Management Center for Cisco Security Agents

Management Center for Cisco Security Agents requires Version 8.0 or higher of Microsoft SQL Server 2000 Desktop Engine (MSDE). Setup will install the necessary components. After the MSDE installation is completed, you must reboot and then run Management Center for Cisco Security Agents Setup again. Do you want to continue?

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 2-2 Microsoft SQL Server Directory Prompt



Management Center for Cisco Security Agents

Specify The Installation Path For MSDE

Setup has chosen to install the Microsoft SQL Server Desktop Edition (MSDE) on drive [F:] because it has the most free space [23463 MB].

Choose NEXT to accept this default or select another location.

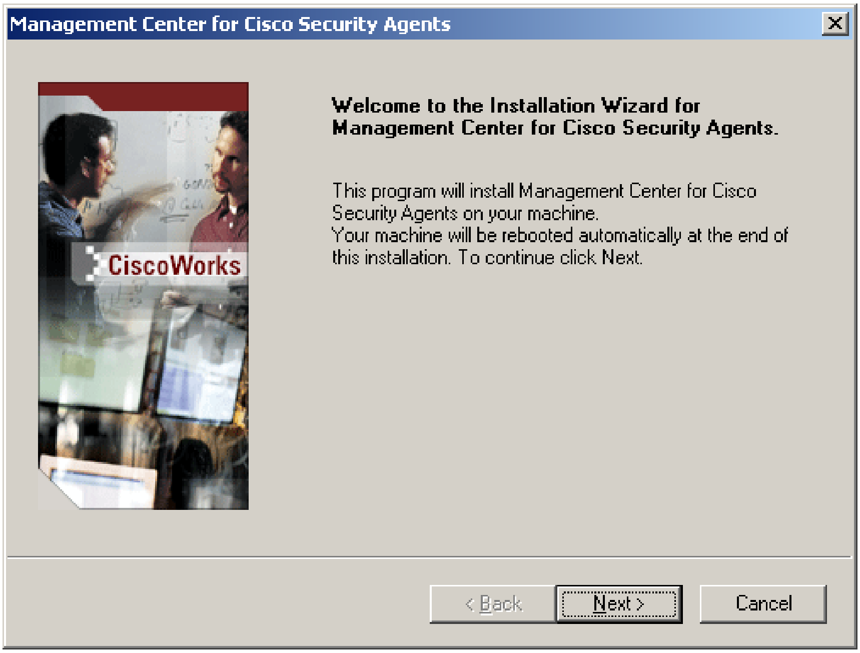
Destination Folder

F:\Program Files\Microsoft SQL Server

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 4 Begin the CSA MC installation again. This time the installation detects the Microsoft SQL Server software and proceeds by displaying the introduction screen. Click **Next** to continue.

Figure 2-3 Installation Introduction Screen

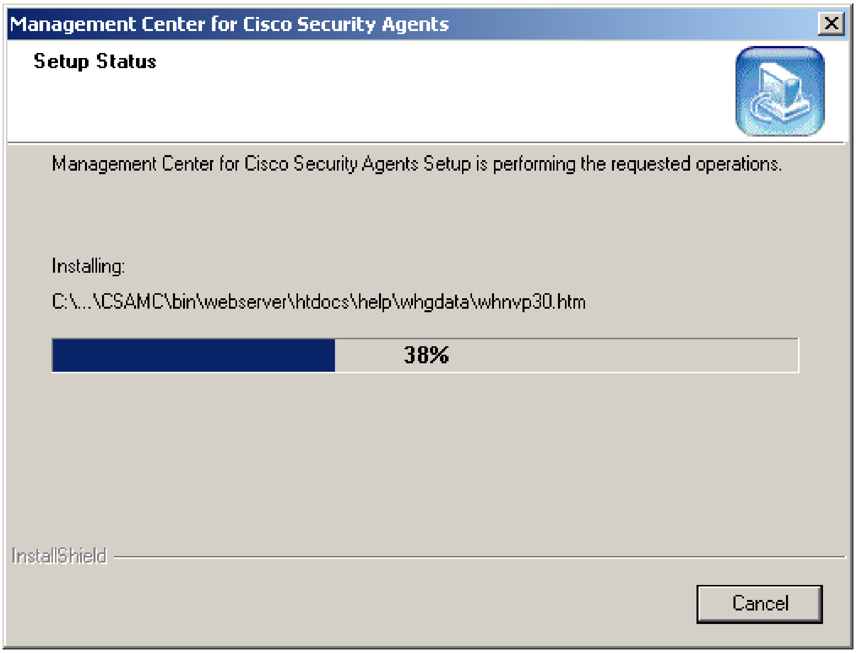


Welcome to the Installation Wizard for Management Center for Cisco Security Agents.

This program will install Management Center for Cisco Security Agents on your machine.
Your machine will be rebooted automatically at the end of this installation. To continue click Next.

The installation copies the necessary files to your system (see Figure 2-4).

Figure 2-4 Copy Files


Management Center for Cisco Security Agents

Setup Status

Management Center for Cisco Security Agents Setup is performing the requested operations.

Installing:

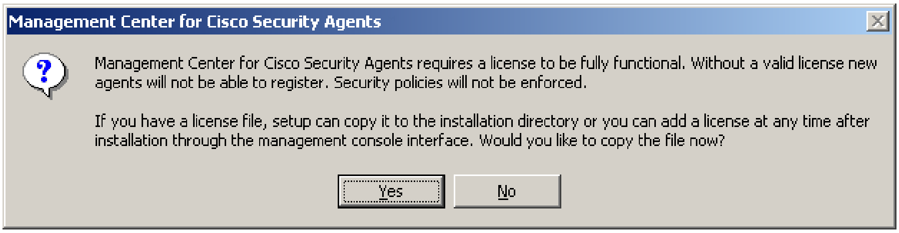
C:\...\CSAMC\bin\webserver\htdocs\help\whgdata\whnvp30.htm

38%

You are reminded that you must obtain a license key (see page 2-2 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 2-5) 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 2-5 License Key Popup

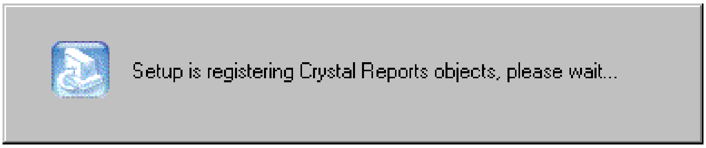

Management Center for Cisco Security Agents

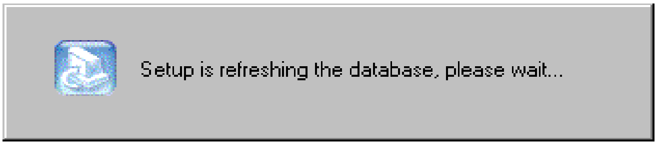
Management Center for Cisco Security Agents requires a license to be fully functional. Without a valid license new agents will not be able to register. Security policies will not be enforced.

If you have a license file, setup can copy it to the installation directory or you can add a license at any time after installation through the management console interface. Would you like to copy the file now?

Once all the files are copied, the installation performs some preliminary system setup tasks (see Figure 2-6).

Figure 2-6 System Setup


Setup is registering Crystal Reports objects, please wait...


Setup is refreshing the database, please wait...

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 within 2 minutes after the CSA MC protecting agent installation is complete. You must reboot your system before you can begin using CSA MC.

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 Installation Notes

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. Microsoft SQL Server Desktop Engine has a 2 GB limit. SQL Server 2000 must be licensed separately and it must be installed on the 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.) 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 to the largest partition on the system. This will ensure enough space for current data and expected data growth.
- 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 3. 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 SP3 (required)** checkbox.

Installation Log

The installation of CSA MC produces a log file. This log file, called "Management Center for Cisco Security AgentsInstallInfo.txt" and located in the CSCOpx\CSAMC\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 "Cisco Security AgentInstallInfo.txt" and is located in the Cisco\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** item is located in the **Management Center** and **Administration>Management Center** folders. See Figure 2-7.

Note See Initiating Secure Communications, page 2-20 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:

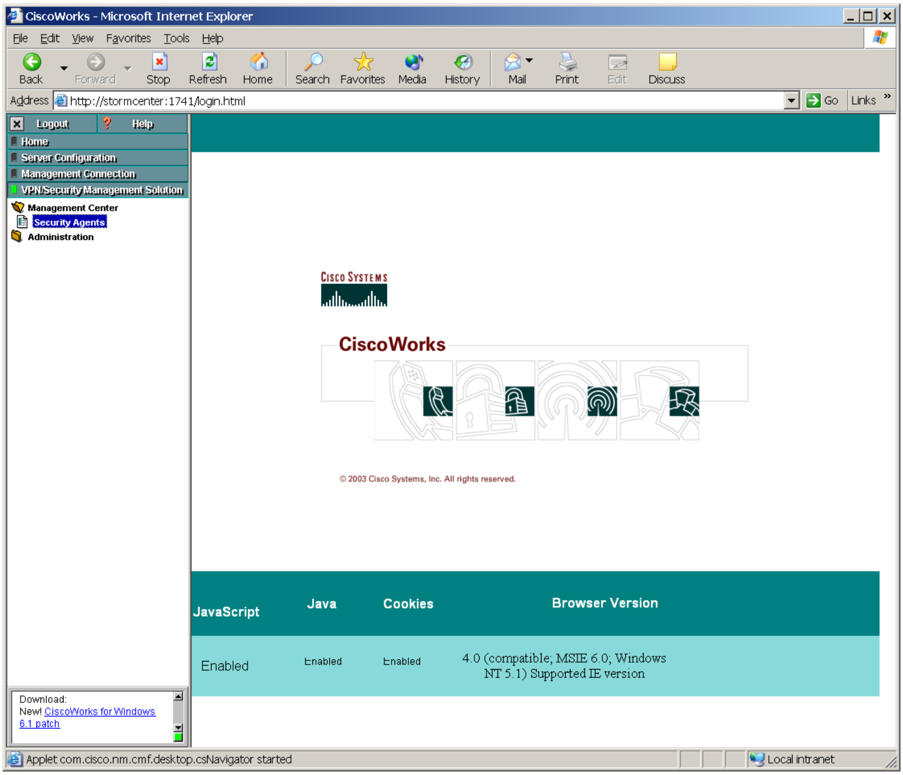
  ```
  http://<ciscoworks system hostname>:1741
  ```

  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 2-7 CiscoWorks Main Page


CiscoWorks - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Mail Print Edit Discuss
Address http://stormcenter:1741/login.html
Go Links
Logout Help
Home
Server Configuration
Management Connection
VPN/Security Management Solution
Management Center
Security Agents
Administration
Cisco Systems
CiscoWorks
© 2003 Cisco Systems, Inc. All rights reserved.
Download:
New! CiscoWorks for Windows 6.1 patch
Applet com.cisco.nm.cmf.desktop.csNavigator started
Local intranet

JavaScript	Java	Cookies	Browser Version
Enabled	Enabled	Enabled	4.0 (compatible; MSIE 6.0; Windows NT 5.1) Supported IE version

Initiating Secure Communications

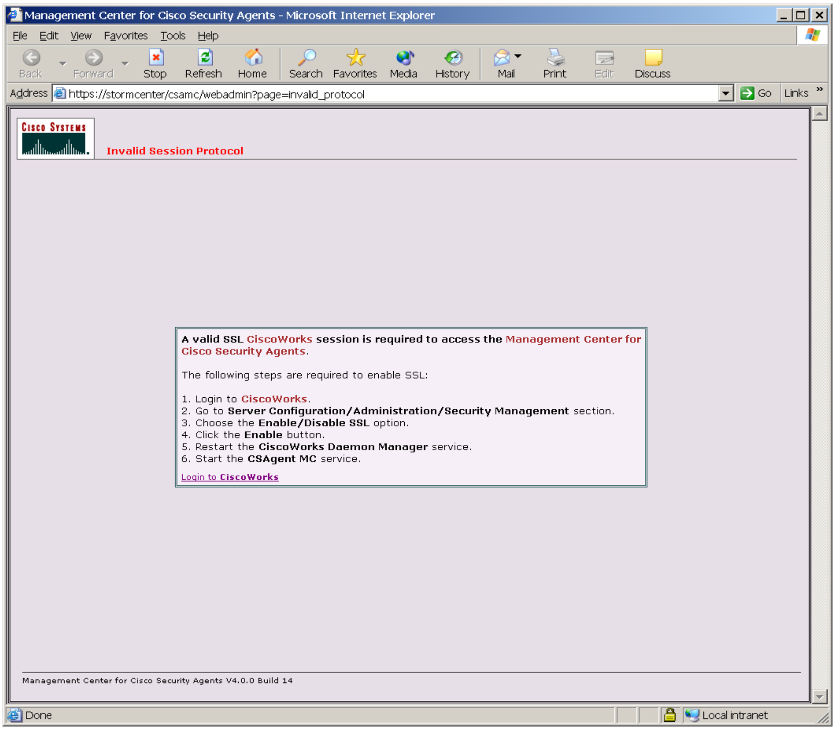
CSA MC uses SSL to secure all communications between the CSA MC user interface (locally and remotely) and the Management Center for Cisco Security Agents system itself. This way, all configuration data travels over secure channels irrespective of the location of the CSA MC host system.

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 you access the CSA MC UI from CiscoWorks, you must have SSL enabled in CiscoWorks for CSA MC to allow the connection. When you install CSA MC, the installation enables SSL. But if this enable procedure does not succeed and SSL is not enabled when you attempt to access CSMAC, a web page appears (see Figure 2-8) informing you that you must switch to SSL mode and restart the services on the CiscoWorks server.

Enable SSL in CiscoWorks from the **Server Configuration** drawer. Go to **Administration>Security Management>Enable/Disable SSL**. Click the **Enable** button in the right pane. You may have to restart both the CiscoWorks and CSA MC services for this change to take effect.

Figure 2-8 Invalid Protocol Page


Management Center for Cisco Security Agents - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Mail Print Edit Discuss
Address https://stormcenter/csamc/webadmin?page=invalid_protocol
Go Links
Cisco Systems
Done
Local intranet

Invalid Session Protocol

A valid SSL CiscoWorks session is required to access the Management Center for Cisco Security Agents.

The following steps are required to enable SSL:

1. Login to CiscoWorks.
2. Go to **Server Configuration/Administration/Security Management** section.
3. Choose the **Enable/Disable SSL** option.
4. Click the **Enable** button.
5. Restart the **CiscoWorks Daemon Manager** service.
6. Start the **CSAgent MC** service.

Login to **CiscoWorks**

Management Center for Cisco Security Agents V4.0.0 Build 14

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.

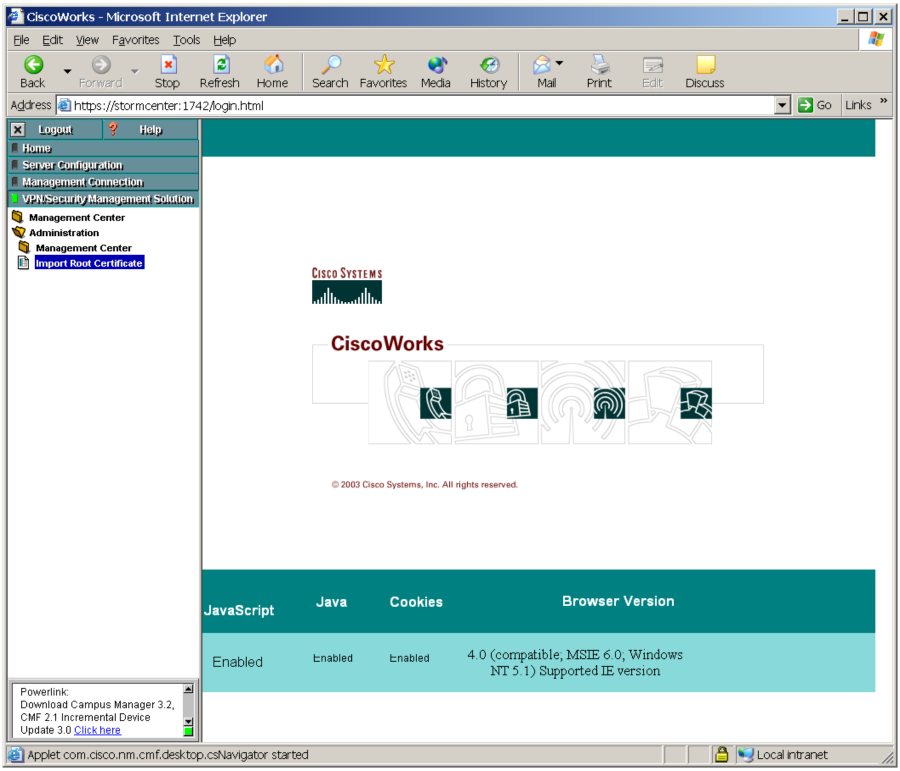
Internet Explorer: Importing the Certificate

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 2-9.

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

Step 3 The certificate information box appears (see Figure 2-10). 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 2-9 Import Root Certificate



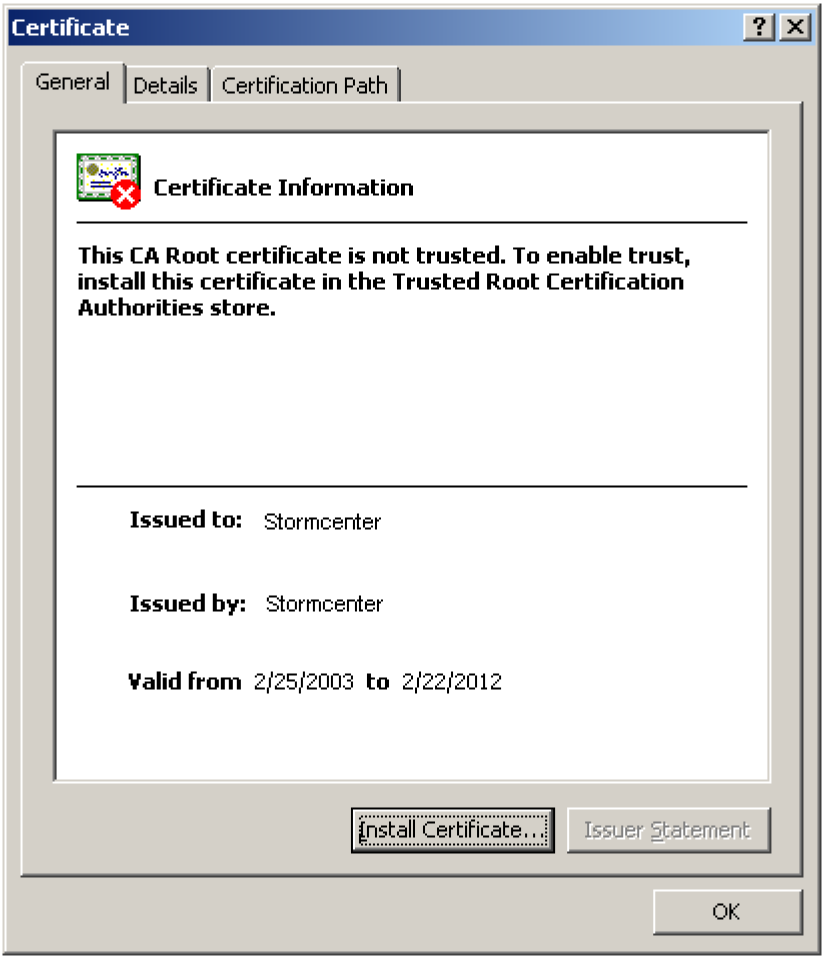
© 2003 Cisco Systems, Inc. All rights reserved.

JavaScript	Java	Cookies	Browser Version
Enabled	Enabled	Enabled	4.0 (compatible; MSIE 6.0; Windows NT 5.1) Supported IE version

Powerlink:
Download Campus Manager 3.2, CMF 2.1 Incremental Device Update 3.0 Click here

Applet com.cisco.nm.cmf.desktop.csNavigator started

Figure 2-10 Certificate Information



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: Stormcenter

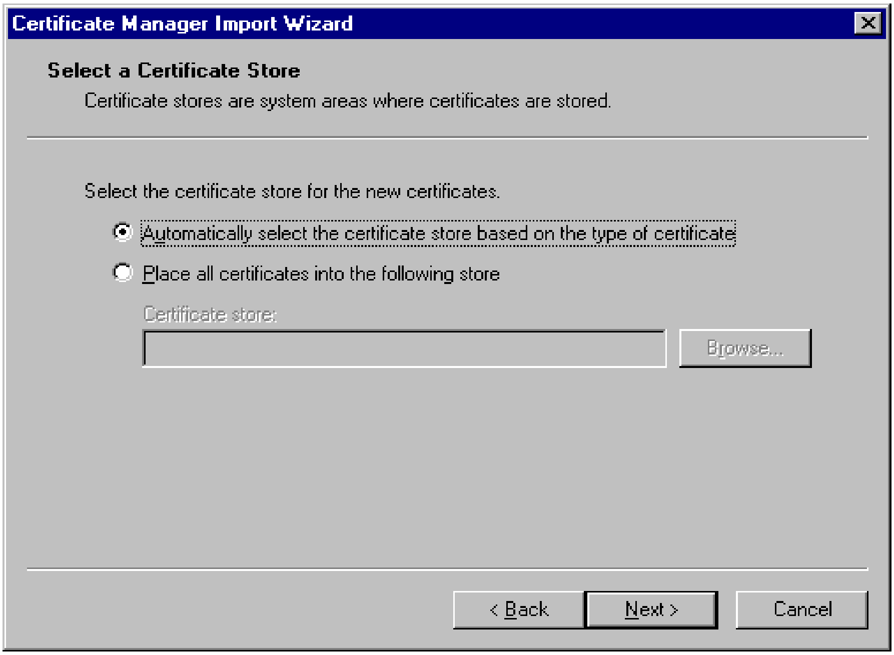
Issued by: Stormcenter

Valid from 2/25/2003 to 2/22/2012

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 2-11 Certificate Wizard



Certificate Manager Import Wizard

Select a Certificate Store

Certificate stores are system areas where certificates are stored.

Select the certificate store for the new certificates.

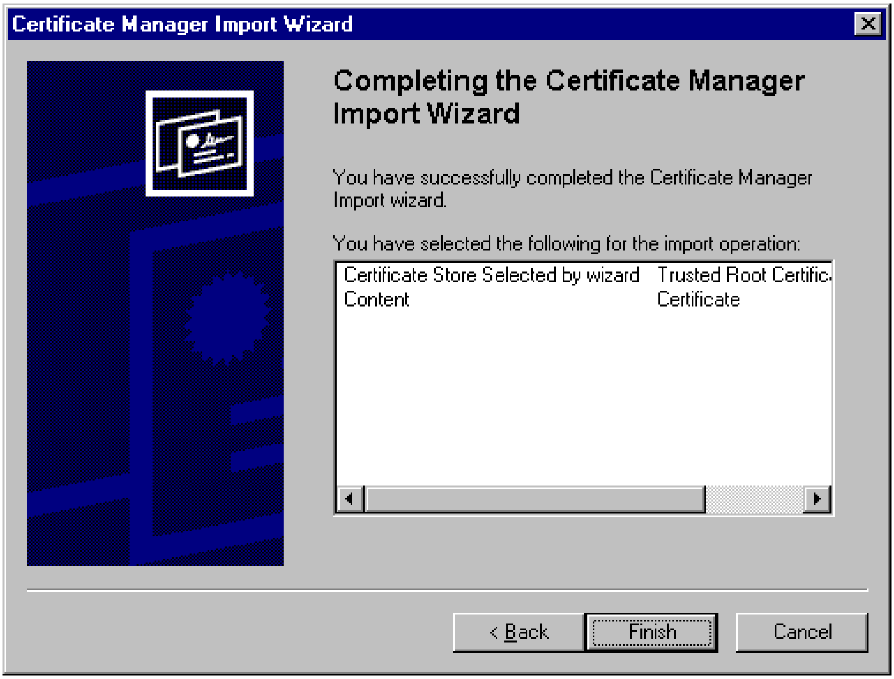
● Automatically select the certificate store based on the type of certificate

○ Place all certificates into the following store

Certificate store:

Step 6 You’ve now imported your certificate for the server. Click the **Finish** button (Figure 2-12) to continue.

Figure 2-12 Certificate Wizard Finish Page



Completing the Certificate Manager Import Wizard

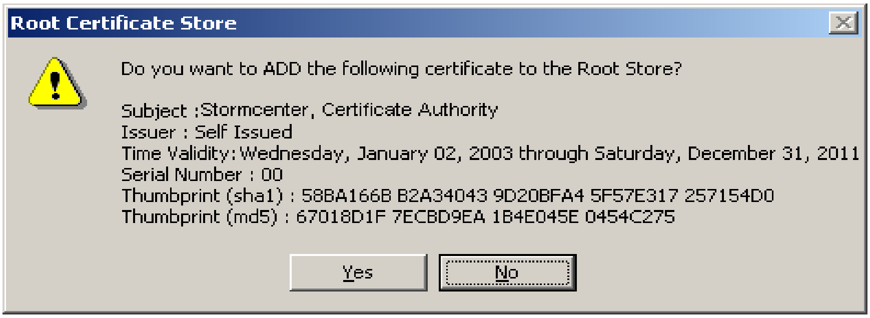
You have successfully completed the Certificate Manager Import wizard.

You have selected the following for the import operation:

Certificate Store Selected by wizard	Trusted Root Certific.
Content	Certificate

Step 7 Now, you must save the certificate. Click the **Yes** button in the Root Certificate Store box (see Figure 2-13).

Figure 2-13 Root Certificate Store Box



Do you want to ADD the following certificate to the Root Store?

Subject :Stormcenter, Certificate Authority
Issuer : Self Issued
Time Validity: Wednesday, January 02, 2003 through Saturday, December 31, 2011
Serial Number : 00
Thumbprint (sha1) : 58BA166B B2A34043 9D20BFA4 5F57E317 257154D0
Thumbprint (md5) : 67018D1F 7ECBD9EA 1B4E045E 0454C275

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 2-10). 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`

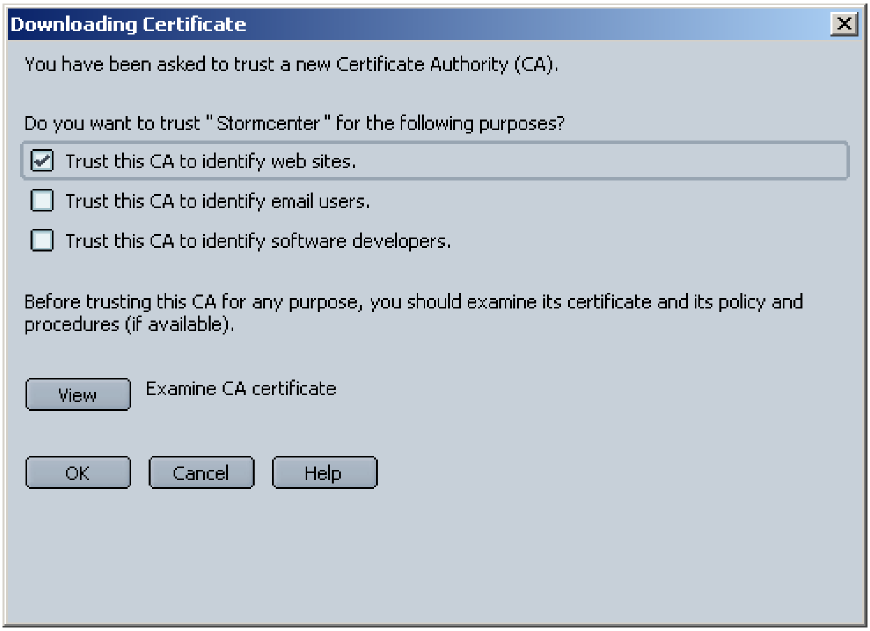
Caution If you have not obtained a valid license from Cisco, when you login to CSA MC, you'll receive a warning informing you that your license is not valid. Refer back to page 2-2 for further licensing information.

Netscape: Importing the 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 2-9.

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

Figure 2-14 Downloading Certificate Window



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "Stormcenter" for the following purposes?

☑ Trust this CA to identify web sites.

□ Trust this CA to identify email users.

□ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Examine CA certificate

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:

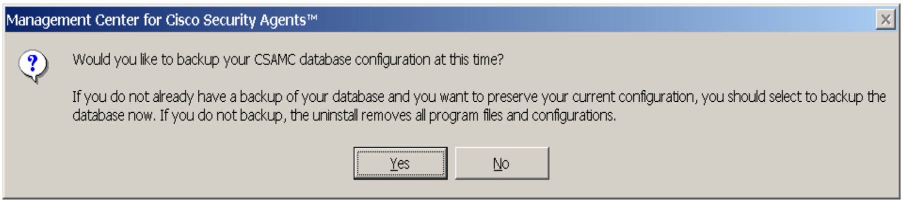
Step 1 From **Start>Settings>Control Panel**, access the **Add/Remove Programs** window. Locate the **CiscoWorks** item. Select the program you want to uninstall. In this case, it's the **Management Center for Cisco Security Agents** program item.

Step 2 Select the appropriate chekbox to remove the CSA MC installation 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.

Figure 2-15 Backup Database Prompt



Management Center for Cisco Security Agents™

Would you like to backup your CSAMC database configuration at this time?

If you do not already have a backup of your database and you want to preserve your current configuration, you should select to backup the database now. If you do not backup, the uninstall removes all program files and configurations.

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 3-2
- Cisco Security Agent Policies, page 3-3
- Configure a Group, page 3-4
- Build an Agent Kit, page 3-6
- View Registered Hosts, page 3-12
- Configure a Policy, page 3-12

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.

To launch CSA MC from CiscoWorks, the CiscoWorks UI must have SSL enabled. See Initiating Secure Communications, page 2-20.

⚠ **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 2, “Installing 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>Administration>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, 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, 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.

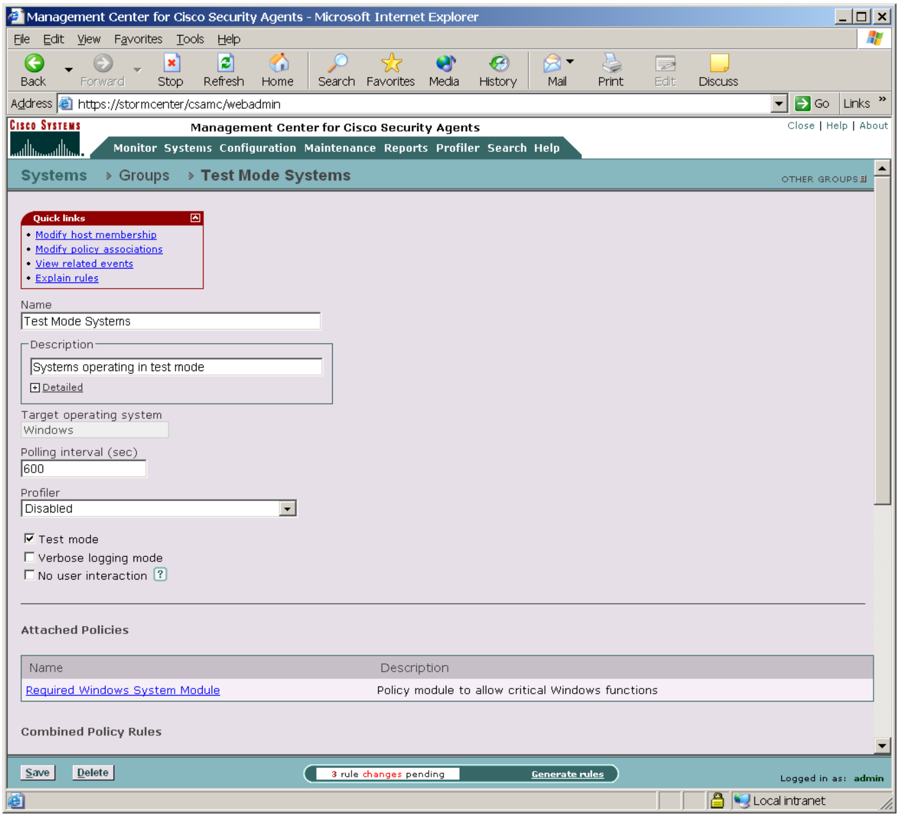
Step 2 Click the **New** button to create a new group entry. You are prompted to select whether this is a Windows or a UNIX group. For this example, click the Windows button. This takes you to the Group configuration page.

Note Any mandatory policies are automatically assigned to the new group.

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 3-1 Group Configuration View



Management Center for Cisco Security Agents - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Mail Print Edit Discuss
Address https://stormcenter/csamc/webadmin
Go Links
Cisco Systems
Management Center for Cisco Security Agents
Close | Help | About
Monitor Systems Configuration Maintenance Reports Profiler Search Help
Systems > Groups > Test Mode Systems
OTHER GROUPS
Quick links
Modify host membership
Modify policy associations
View related events
Explain rules
Detailed
Save
Delete
3 rule changes pending
Generate rules
Logged in as: admin
Local intranet

Name
Test Mode Systems

Description
Systems operating in test mode

Target operating system
Windows

Polling interval (sec)
600

Profiler
Disabled

☑ Test mode
☐ Verbose logging mode
☐ No user interaction

Attached Policies

Name	Description
Required Windows System Module	Policy module to allow critical Windows functions

Combined Policy Rules

Step 4 Cisco suggests that you select the **Test Mode** checkbox 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 **Test Mode**, **Verbose Logging Mode**, **Polling intervals,** and **No user interaction** refer to the User Guide.

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

Build an Agent Kit

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

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

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

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

Step 1 Move the mouse over **Maintenance** in the menu bar and select **Agent Kits** from the drop-down menu that appears. The agent kit list view displays the preconfigured agent kits.

Step 2 Click the **New** button to create a new agent kit. You are prompted to select whether this is a Windows or a UNIX agent kit. For this example, click the Windows button. This takes you to the Agent kit configuration page

Step 3 In the configuration view (see Figure 3-2), enter a **Name** for the kit. This is a unique name (Agent kit names are an exception. Spaces are not valid name characters for agents kits as they are for other name fields).

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

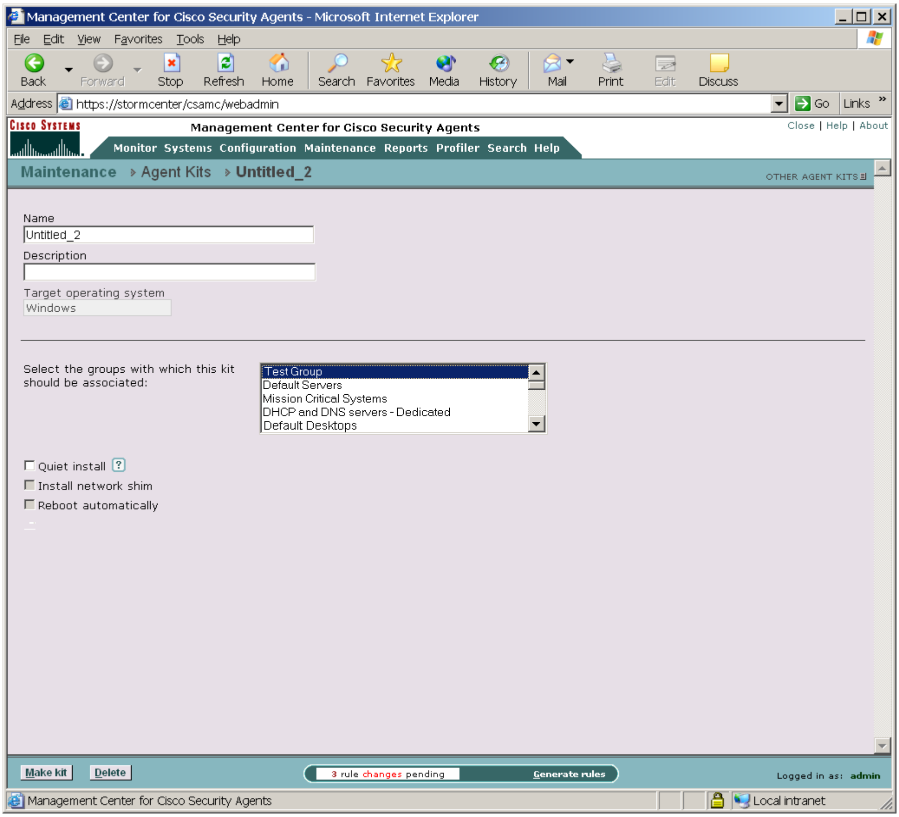
Step 5 From the available list box, select the groups you are associating with this kit. (The names of the groups you configured in the previous section should appear here.)

Step 6 Select whether or not to have agents install "quietly" on end-user systems. A **Quiet install** requires users to download the agent kit and run it as does the non-quiet install. The difference is, other than a prompt for rebooting the system once the installation has completed, no other prompts appear and the user is not required to enter any information. A non-quiet install prompts the user to select options, such as enabling the network shim, in addition to the reboot prompt. (See the User Guide for details.)

Step 7 For agent kits, if you select Quiet install, you can also select whether the **network shim** is installed or not and whether the system will **reboot automatically**. (See the User Guide for more information.)

Step 8 Click the **Make Kit** button in the bottom frame. See Figure 3-2.

Figure 3-2 Create Agent Kit


Management Center for Cisco Security Agents - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Mail Print Edit Discuss
Address https://stormcenter/csamc/webadmin
Go Links
Cisco Systems
Management Center for Cisco Security Agents
Close | Help | About
Monitor Systems Configuration Maintenance Reports Profiler Search Help
Maintenance › Agent Kits › Untitled_2
OTHER AGENT KITS
Make kit
Delete
3 rule changes pending
Generate rules
Logged in as: admin
Management Center for Cisco Security Agents
Local intranet

Name
Untitled_2

Description

Target operating system
Windows

Select the groups with which this kit should be associated:

- Test Group
- Default Servers
- Mission Critical Systems
- DHCP and DNS servers - Dedicated
- Default Desktops

☐ Quiet install ?
☐ Install network shim
☐ Reboot automatically

Once you click the Make Kit button and generate rules, CSA MC produces a kit for distribution. It displays a URL for this particular kit (see Figure 3-3). 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.

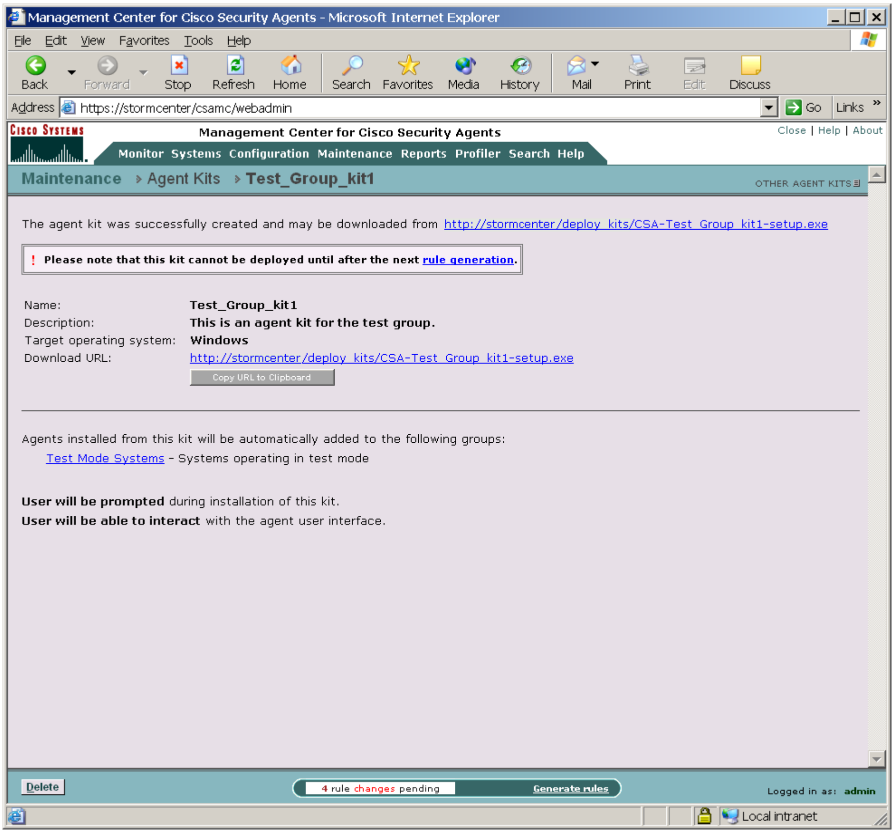
But you may also point users to a URL for the CiscoWorks system. This URL will allow them to see all kits that are available. That URL is:

```
https://<ciscoworks system name>/csamc/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 3-4.

Note Note that the Registration Control feature also applies to the <ciscoworks system name>/csamc/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 3-3 Agent Kit Download URL


Management Center for Cisco Security Agents - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Mail Print Edit Discuss
Address https://stormcenter/csamc/webadmin
Go Links
Cisco Systems
Management Center for Cisco Security Agents
Close | Help | About
Monitor Systems Configuration Maintenance Reports Profiler Search Help
Maintenance › Agent Kits › Test_Group_kit1
OTHER AGENT KITS
Copy URL to Clipboard
Delete
Generate rules
Local intranet

The agent kit was successfully created and may be downloaded from http://stormcenter/deploy_kits/CSA-Test_Group_kit1-setup.exe

! **Please note that this kit cannot be deployed until after the next rule generation.**

Name:	**Test_Group_kit1**
Description:	**This is an agent kit for the test group.**
Target operating system:	**Windows**
Download URL:	http://stormcenter/deploy_kits/CSA-Test_Group_kit1-setup.exe

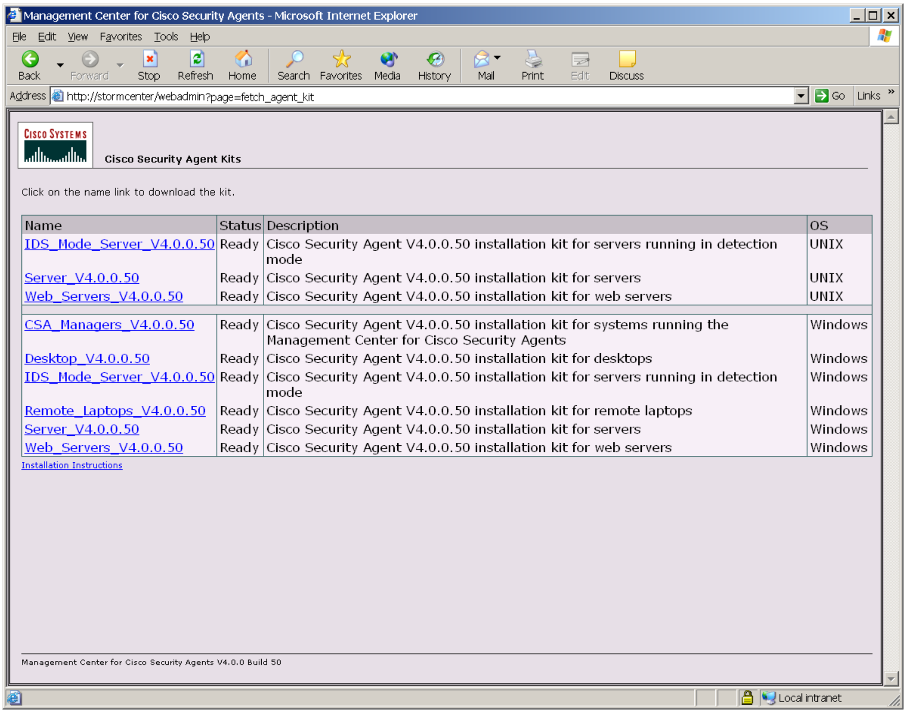
Agents installed from this kit will be automatically added to the following groups:
Test Mode Systems - Systems operating in test mode

User will be prompted during installation of this kit.
User will be able to interact with the agent user interface.

4 rule changes pending

Logged in as: **admin**

Figure 3-4 Download Agent Kits


Management Center for Cisco Security Agents - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
Media
History
Mail
Print
Edit
Discuss
Address http://stormcenter/webadmin?page=fetch_agent_kit
Go
Links
Local intranet

Cisco Security Agent Kits

Click on the name link to download the kit.

Name	Status	Description	OS
IDS_Mode_Server_V4.0.0.50	Ready	Cisco Security Agent V4.0.0.50 installation kit for servers running in detection mode	UNIX
Server_V4.0.0.50	Ready	Cisco Security Agent V4.0.0.50 installation kit for servers	UNIX
Web_Servers_V4.0.0.50	Ready	Cisco Security Agent V4.0.0.50 installation kit for web servers	UNIX
CSA_Managers_V4.0.0.50	Ready	Cisco Security Agent V4.0.0.50 installation kit for systems running the Management Center for Cisco Security Agents	Windows
Desktop_V4.0.0.50	Ready	Cisco Security Agent V4.0.0.50 installation kit for desktops	Windows
IDS_Mode_Server_V4.0.0.50	Ready	Cisco Security Agent V4.0.0.50 installation kit for servers running in detection mode	Windows
Remote_Laptops_V4.0.0.50	Ready	Cisco Security Agent V4.0.0.50 installation kit for remote laptops	Windows
Server_V4.0.0.50	Ready	Cisco Security Agent V4.0.0.50 installation kit for servers	Windows
Web_Servers_V4.0.0.50	Ready	Cisco Security Agent V4.0.0.50 installation kit for web servers	Windows

Installation Instructions

Management Center for Cisco Security Agents V4.0.0 Build 50

The Cisco Security Agent

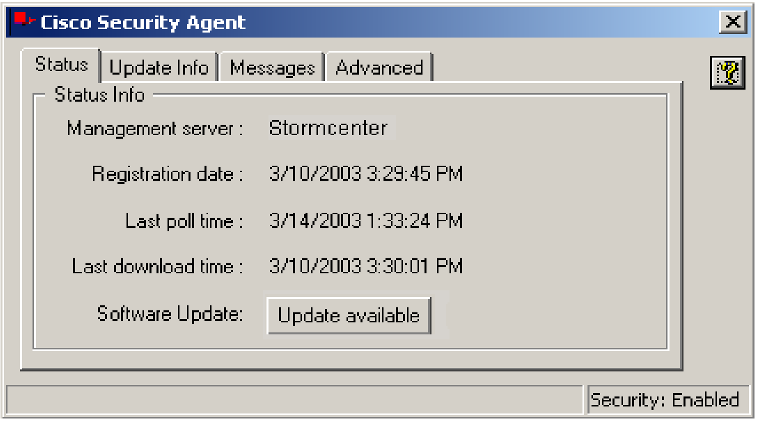
- Users must have administrator privileges on their systems to install the Cisco Security Agent software.
- The Cisco Security Agent installs on Windows XP systems, Windows 2000 systems and Windows NT systems. Agents also install on Solaris 8 systems. (On Solaris systems there is no agent user interface. See Appendix A in the User Guide for information on a UNIX 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. Most fields are read-only status displays.

Figure 3-5 Agent Status



Management server : Stormcenter

Registration date : 3/10/2003 3:29:45 PM

Last poll time : 3/14/2003 1:33:24 PM

Last download time : 3/10/2003 3:30:01 PM

Software Update: Update available

Security: Enabled

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

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 Search** page. Click the **Find** button to view all registered hosts. (All is the default search setting.) Or narrow your search to active or inactive hosts by selecting the appropriate radio button. You can also enter text in the Find edit field to search for a particular host.

- 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 Policy

This section provides brief instructions for configuring and distributing a policy to Cisco Security Agents. For a full discussion of rules 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 access control rules 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.

For this example, we will configure a file access control rule that protects systems from a known email virus. Cisco Security Agent heuristics catch email viruses such as ILOVEYOU (used in this example). These VBS files are detected, correlated across systems, and quarantined by CSA MC for up to one hour. 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 policy, do the following.

Step 1 Move the mouse over **Configuration** in the menu bar and select **Policies** from the drop-down list that appears. The policy list view appears.

Step 2 Click the **New** button to create a new policy. You are prompted to select whether this is a Windows or a UNIX policy. For this example, click the Windows button. This takes you to the Policy configuration page. See Figure 3-6.

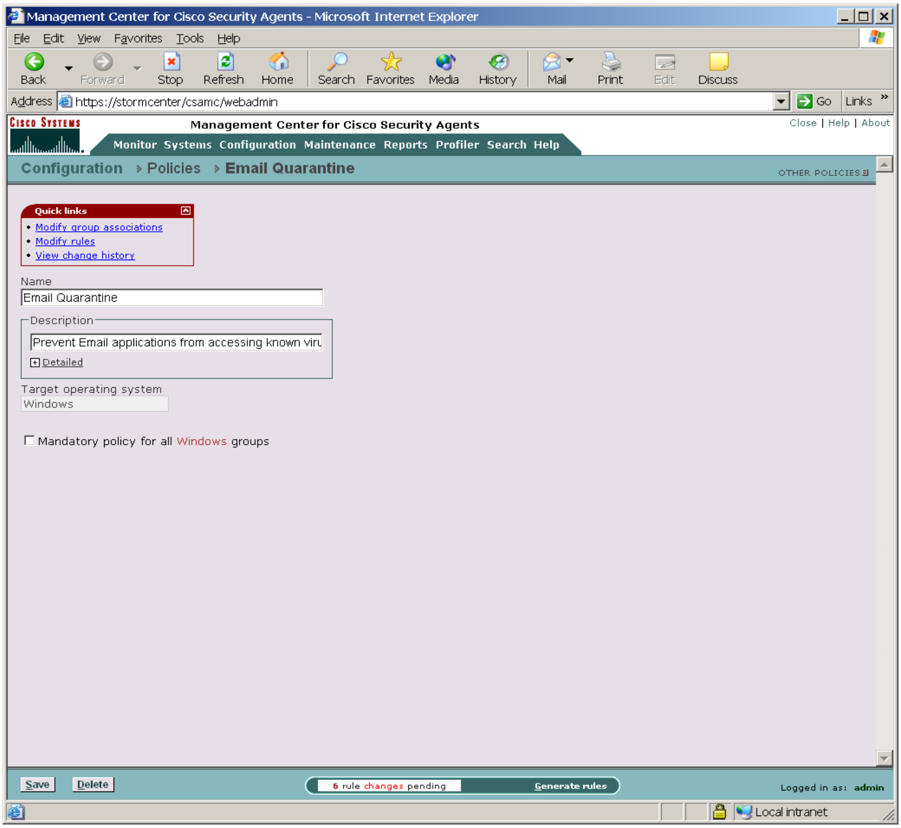
Step 3 In the policy configuration view, enter the **Name** *Email Quarantine*. Note that names are case insensitive, must start with an alphabetic character, can be up to 64 characters long. Spaces are also allowed in names.

Step 4 Enter a **Description** of your policy. We'll enter *Prevent email applications from accessing known viruses*.

Step 5 Click the **Save** button.

Now we add our file access rule to this policy.

Figure 3-6 Policy Creation View



Management Center for Cisco Security Agents - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Mail Print Edit Discuss
Address https://stormcenter/csamc/webadmin
Go Links
Cisco Systems
Management Center for Cisco Security Agents
Close | Help | About
Monitor Systems Configuration Maintenance Reports Profiler Search Help
Configuration > Policies > Email Quarantine
OTHER POLICIES
Quick links
Modify group associations
Modify rules
View change history
Save Delete
6 rule changes pending
Generate rules
Logged in as: admin
Local intranet

Name
Email Quarantine

Description
Prevent Email applications from accessing known viru
Detailed

Target operating system
Windows

☐ Mandatory policy for all Windows groups

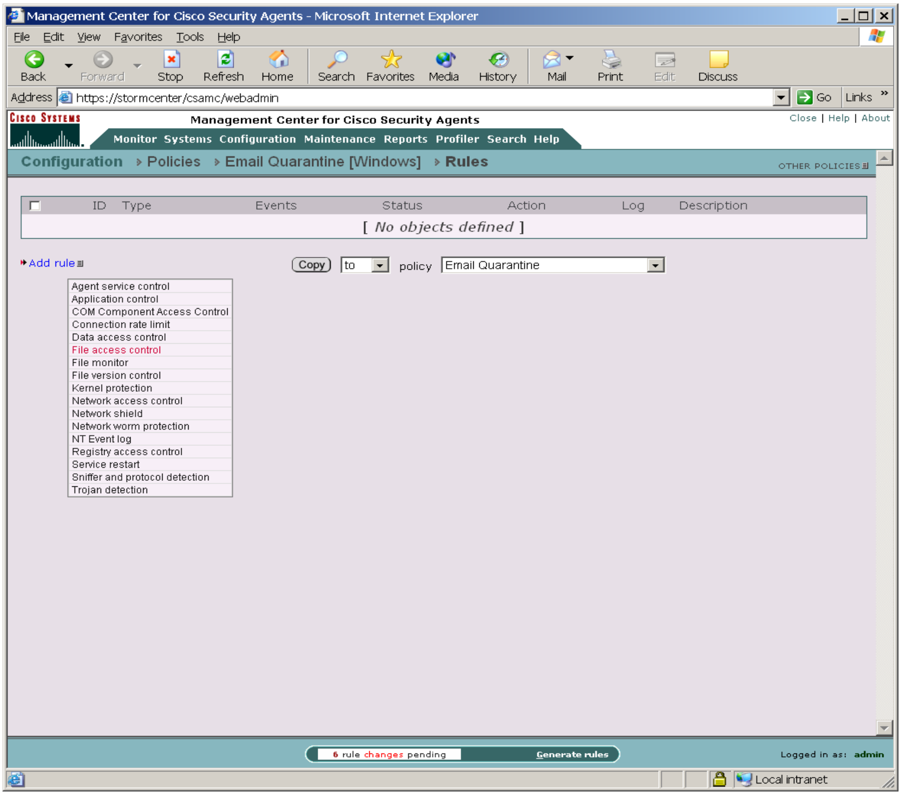
Create a File Access Control Rule

Step 1 From the Policy configuration page (Figure 3-6), 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 3-7). This takes you to the configuration page for this rule.

Figure 3-7 Add Rules to Policy



Management Center for Cisco Security Agents - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Mail Print Edit Discuss
Address https://stormcenter/csamc/webadmin
Go Links
Cisco Systems
Management Center for Cisco Security Agents
Close | Help | About
Monitor Systems Configuration Maintenance Reports Profiler Search Help
Configuration › Policies › Email Quarantine [Windows] › Rules
OTHER POLICIES
Add rule
Copy to policy Email Quarantine
Agent service control
Application control
COM Component Access Control
Connection rate limit
Data access control
File access control
File monitor
File version control
Kernel protection
Network access control
Network shield
Network worm protection
NT Event log
Registry access control
Service restart
Sniffer and protocol detection
Trojan detection
6 rule changes pending
Generate rules
Logged in as: admin
Local intranet

□	ID	Type	Events	Status	Action	Log	Description
[*No objects defined*]							

Step 4 In the File access control rule configuration view (see Figure 3-8), 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** 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:

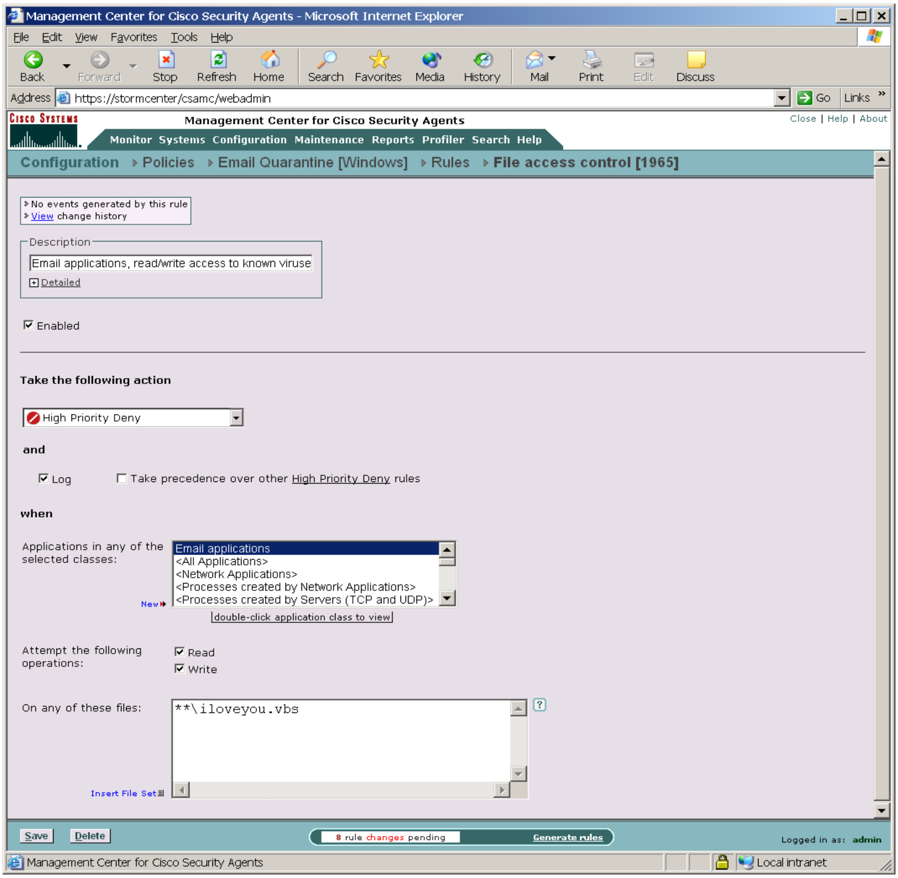
```
        **\iloveyou.vbs
```

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 attach our policy to the group we created earlier.

Figure 3-8 File Access Control Rule



Management Center for Cisco Security Agents - Microsoft Internet Explorer

Address https://stormcenter/csamc/webadmin

Management Center for Cisco Security Agents

Configuration › Policies › Email Quarantine [Windows] › Rules › File access control [1965]

No events generated by this rule
View change history

Description: Email applications, read/write access to known viruse

☑ Enabled

Take the following action: High Priority Deny

and

☑ Log ☐ Take precedence over other High Priority Deny rules

when

Applications in any of the selected classes:
- Email applications
- <All Applications>
- <Network Applications>
- <Processes created by Network Applications>
- <Processes created by Servers (TCP and UDP)>

Attempt the following operations: ☑ Read ☑ Write

On any of these files: **\iloveyou.vbs

8 rule changes pending

Logged in as: admin

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.

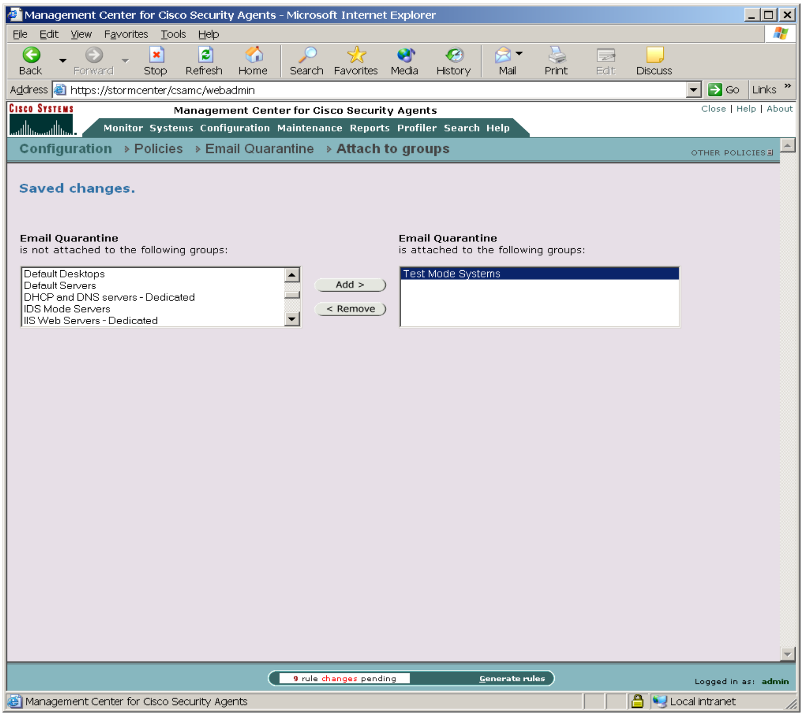
Step 2 From the group list view, click the link for the group you want to attach the policy to. This brings you to that group's edit view.

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 3-9).

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 3-9 Attach Policy to Group


Management Center for Cisco Security Agents - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Mail Print Edit Discuss
Address https://stormcenter/csamc/webadmin
Go Links
Cisco Systems
Management Center for Cisco Security Agents
Close | Help | About
Monitor Systems Configuration Maintenance Reports Profiler Search Help
Configuration › Policies › Email Quarantine › Attach to groups
OTHER POLICIES
Add >
< Remove
9 rule changes pending
Generate rules
Logged in as: admin
Management Center for Cisco Security Agents
Local intranet

Saved changes.

Email Quarantine
is not attached to the following groups:

Default Desktops
Default Servers
DHCP and DNS servers - Dedicated
IDS Mode Servers
IIS Web Servers - Dedicated

Email Quarantine
is attached to the following groups:

Test Mode Systems

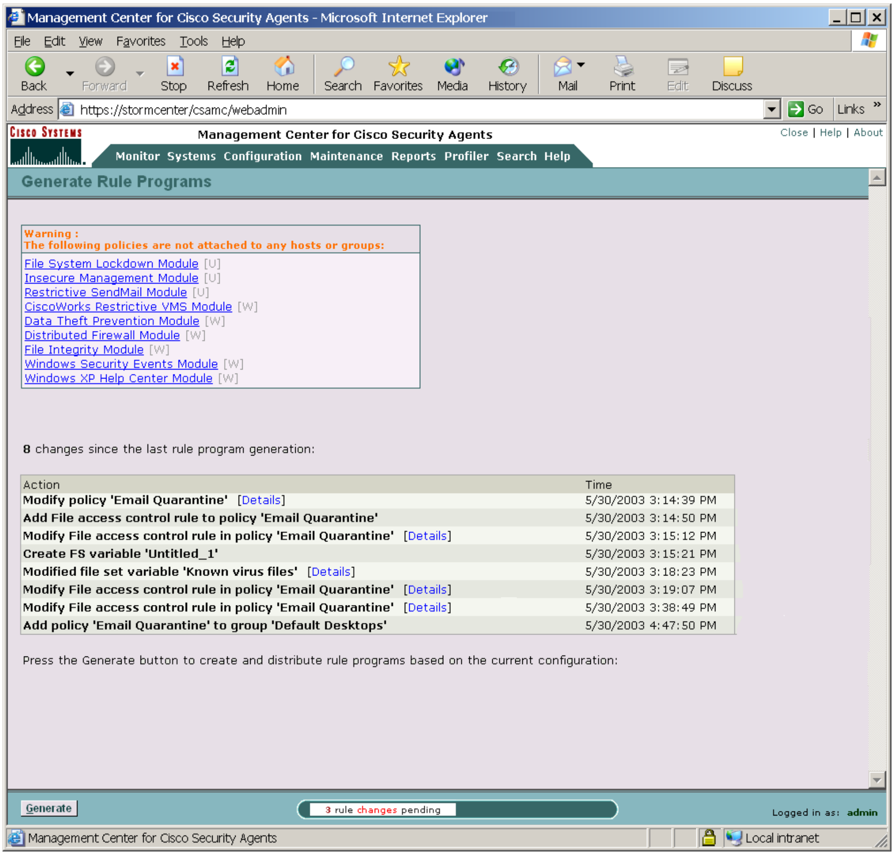
Generate Rule Programs

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 3-10).

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 3-10 Generate Rule Programs


Management Center for Cisco Security Agents - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Mail Print Edit Discuss
Address https://stormcenter/csamc/webadmin
Go Links
Cisco Systems
Management Center for Cisco Security Agents
Close | Help | About
Monitor Systems Configuration Maintenance Reports Profiler Search Help
Generate
3 rule changes pending
Logged in as: admin
Management Center for Cisco Security Agents
Local intranet

Generate Rule Programs

Warning :
The following policies are not attached to any hosts or groups:

File System Lockdown Module [U]
Insecure Management Module [U]
Restrictive SendMail Module [U]
CiscoWorks Restrictive VMS Module [W]
Data Theft Prevention Module [W]
Distributed Firewall Module [W]
File Integrity Module [W]
Windows Security Events Module [W]
Windows XP Help Center Module [W]

8 changes since the last rule program generation:

Action	Time
Modify policy 'Email Quarantine' [Details]	5/30/2003 3:14:39 PM
Add File access control rule to policy 'Email Quarantine'	5/30/2003 3:14:50 PM
Modify File access control rule in policy 'Email Quarantine' [Details]	5/30/2003 3:15:12 PM
Create FS variable 'Untitled_1'	5/30/2003 3:15:21 PM
Modified file set variable 'Known virus files' [Details]	5/30/2003 3:18:23 PM
Modify File access control rule in policy 'Email Quarantine' [Details]	5/30/2003 3:19:07 PM
Modify File access control rule in policy 'Email Quarantine' [Details]	5/30/2003 3:38:49 PM
Add policy 'Email Quarantine' to group 'Default Desktops'	5/30/2003 4:47:50 PM

Press the Generate button to create and distribute rule programs based on the current configuration:

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 every 10 minutes, by default, to retrieve policies. It may take up to 10 minutes for your agent to receive the generated policy. You can shorten or lengthen this polling time in the Group configuration page.

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 both the Windows and UNIX agents. (This information, with some additional details, also appears in a similarly titled Appendix A in the User Guide.)

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

This section contains the following topics.

- Downloading and Installing, page A-2
- The Cisco Security Agent User Interface, page A-5
- Installing the UNIX Agent, page A-10

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>/csamc/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>/csamc/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

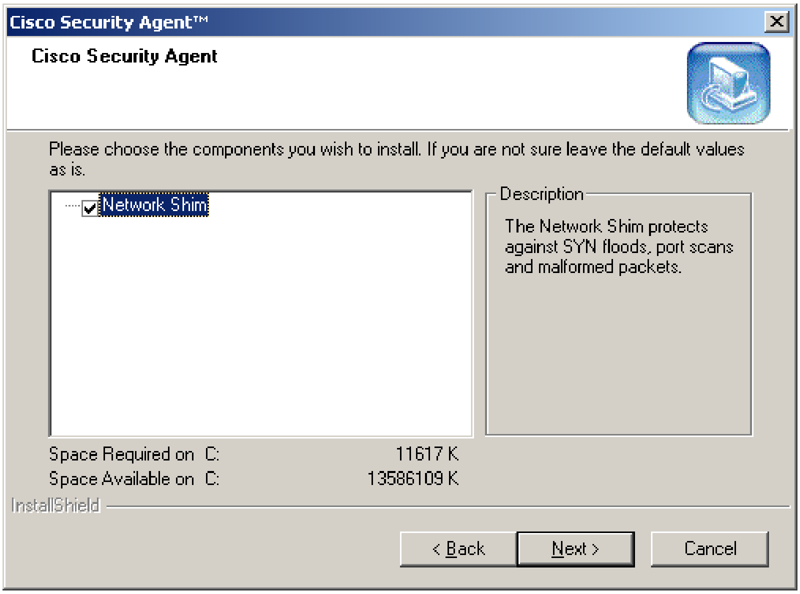
In some circumstances, you may not want users to enable the network shim on their systems as part of the agent installation. For example, if users have VPN software or a personal firewall installed on their systems, the network shim's Portscan detection, SYN flood protection, and malformed packet detection capabilities may be in conflict with VPNs and personal firewalls. (There are no conflicts with the Cisco VPN client, Release 4.0.)

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 (on Windows). 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 mentioned in the previous paragraph are not enabled.

Figure A-1 Optional Network Shim (Windows)



Please choose the components you wish to install. If you are not sure leave the default values as is.

☑ Network Shim

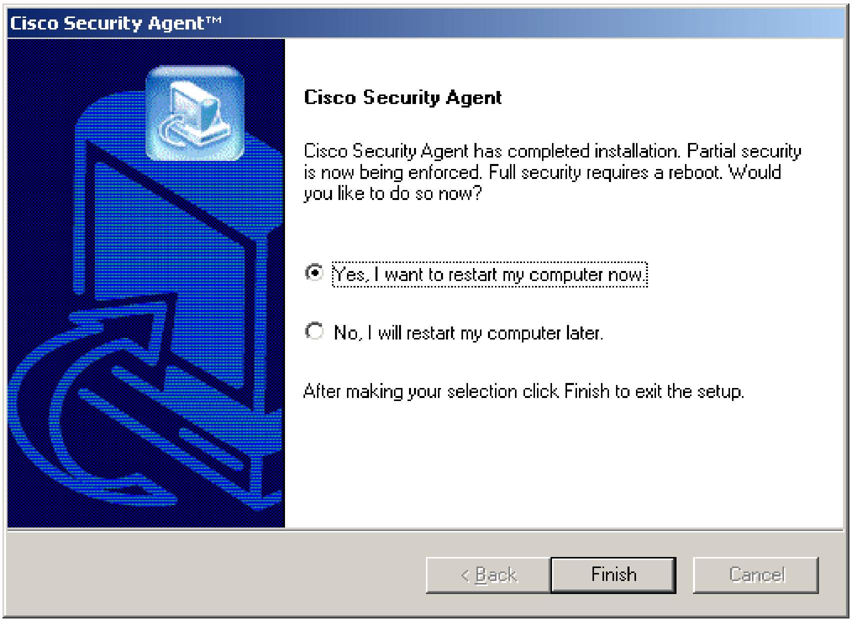
Description

The Network Shim protects against SYN floods, port scans and malformed packets.

Space Required on C: 11617 K
Space Available on C: 13586109 K

Once users install agents on their systems, they can optionally perform a reboot (if Automatic 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.

Figure A-2 Optional Agent Reboot



Cisco Security Agent

Cisco Security Agent has completed installation. Partial security is now being enforced. Full security requires a reboot. Would you like to do so now?

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

After making your selection click Finish to exit the setup.

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.
- Buffer overflow protection (located on the Trojan page for Windows) is only enforced for new processes.
- Data access control rules are not applied until the web server service is restarted.
- COM component access control rules are not applied until the system is rebooted.

UNIX agents, when no reboot occurs after install, the following caveats exist:

- 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.
- 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.

Note By default, agents poll in to CSA MC every 10 minutes for policy updates (unless you change this value in the Groups configuration view).

The Cisco Security Agent User Interface

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

Note If **No user interaction** (available on Windows groups only) is enabled for the system group, no agent UI appears on the end user system. See Configuring Groups, page 3-3 of the User Guide for details.

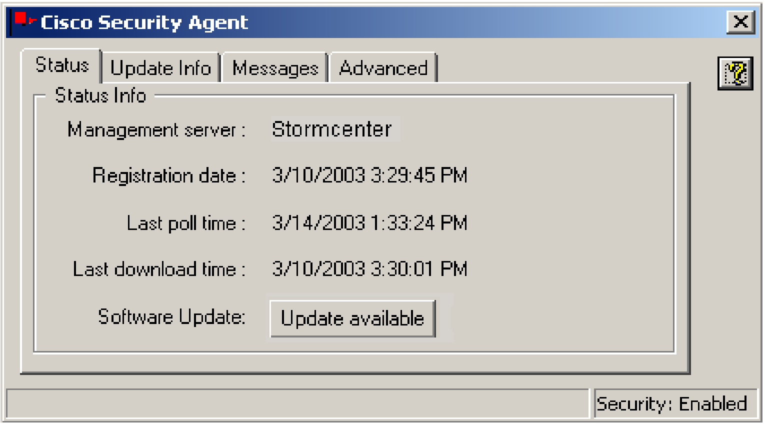
To open the Cisco Security Agent user interface on Windows systems, users can double-click on the flag icon in their system trays. The user interface opens on their desktop. It contains four tabs. Most fields are read-only.

Status tab: This tab provides the following information (see Figure A-3).

- The name of the CSA MC with which this agent is registered.
- The date and time the agent registered with CSA MC.
- The date and time when the agent last polled CSA MC (data is not downloaded each time the agent polls).

- The date and time the agent last downloaded data from CSA MC.
- Lets users know if there is a software version update available for their agent (see the User Guide for details).

Figure A-3 Agent Status Tab



Management server : Stormcenter

Registration date : 3/10/2003 3:29:45 PM

Last poll time : 3/14/2003 1:33:24 PM

Last download time : 3/10/2003 3:30:01 PM

Software Update: Update available

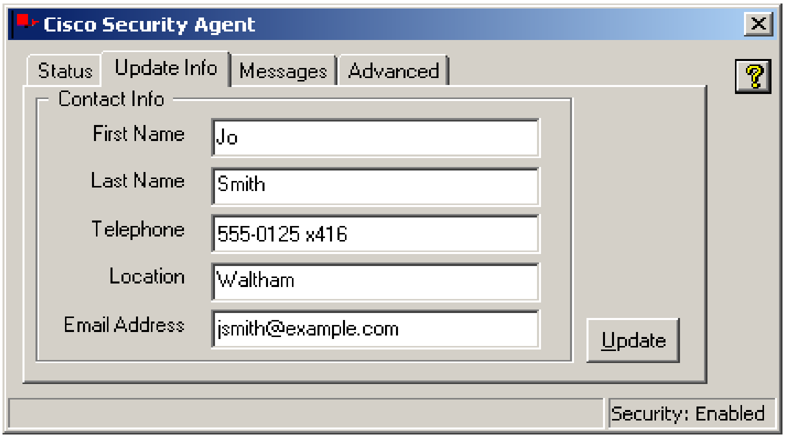
Security: Enabled

Note Viewable from all tabs, on the bottom of the agent UI, is a Security status field. This status lets the user know if security is enabled or disabled. They can change this status (if allowed by the administrator) from the agent pulldown menu.

Update Info tab: This tab provides the following information (see Figure A-4).

- Contact information, including user name, telephone number, location, and email address. Users enter this information here and click the Update button. CSA MC receives this contact data and you can now quickly locate a user if the agent indicates that there is a problem.

Figure A-4 Agent Update Info Tab



Contact Info

First Name: Jo

Last Name: Smith

Telephone: 555-0125 x416

Location: Waltham

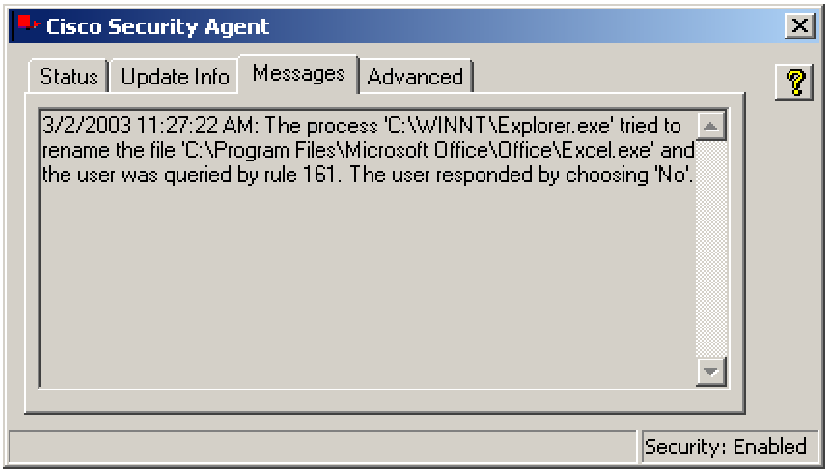
Email Address: jsmith@example.com

Security: Enabled

Messages tab: This tab provides the following information (see Figure A-5).

- When an agent denies a system action, a message informing the user of this event is placed in the Messages field. Note that a line of text in the Status tab informs the user that there are messages present. Click the Messages tab to view them.

Figure A-5 Agent Messages Tab



3/2/2003 11:27:22 AM: The process 'C:\WINNT\Explorer.exe' tried to rename the file 'C:\Program Files\Microsoft Office\Office\Excel.exe' and the user was queried by rule 161. The user responded by choosing 'No'.

Events are also stored in the NT event log on the agent system.

Note When a policy is triggered on an agent system and a message appears in the Messages tab, the flag icon in the system tray *waves*. This waving continues until the user opens the agent GUI and clicks on the Messages tab.

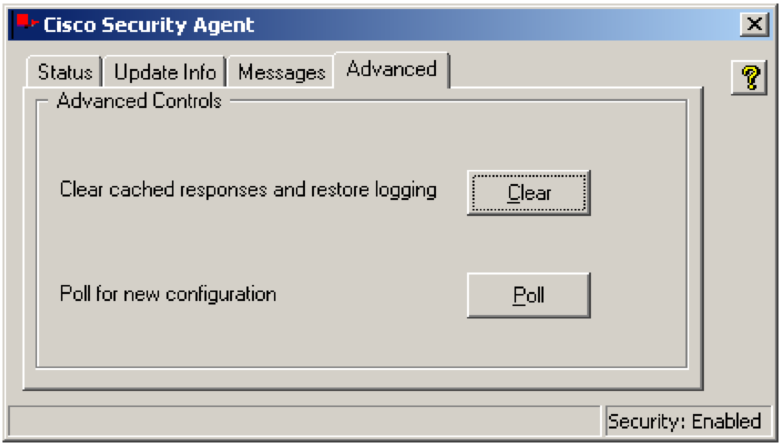
Advanced tab: This tab provides the following information (see Figure A-6).

When the agent logs an event with CSA MC, it remembers that event for an hour and does not log it again (even if the event occurs again) until that hour time frame has expired. This is to prevent the logfile from filling too quickly. The same applies to Query User pop-up messages (see the User Guide for details). Once the user has answered a pop-up query, the system remembers the answer and responds automatically, not prompting the user with another query pop-up.

The Advanced tab on the agent lets the user clear the cache and re-enable logging.

- Clicking the **Clear** button tells the system to clear all cached responses and display a Query User pop-up box when the event in question occurs again. Clicking Clear also tells the system to clear its memory of all logged events (causing events to once again produce log messages if they occur).
- Clicking the **Poll** button forces the agent to poll in to CSA MC. This way, the agent receives any rule changes immediately. It will stop fast polling after the first successful configuration request. If the first attempt is unsuccessful, the agent will attempt to poll 2 more times. This is useful if new rules are being deployed and tested.

Figure A-6 Agent Advanced Tab



Uninstall Windows Cisco Security Agent

To uninstall the Cisco Security Agent, do the following:

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

Installing the UNIX 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 UNIX 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-Server_4.0.0.15-setup.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) 4.0.0.15
```

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/csamanager 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) 4.0.0.15
```

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, and file access control rules only apply to newly opened files. (This functionality becomes available the next time the system is rebooted.)

The agent installs into the following directory:

```
/opt/CSCOcsa
```

Caution If you are upgrading the UNIX 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 UNIX 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 service control 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 service control** in the User Guide for details on this rule type.

The shipped mandatory UNIX policy, "Secure Management Module," 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.

APPENDIX B

Evaluating the Cisco Security Agent

Overview

This section is meant for users evaluating the Cisco Security Agent 4.0. It is designed to help you understand the product design goals for the Cisco Security Agent 4.0, as well as how to use the Cisco Security Agent to establish a proactive security solution for your mission-critical business applications.

This evaluator's section is recommended for any user who wishes to install the Cisco Security Agent for the purpose of reviewing and evaluating the product. It contains a recommended set of tests that allows evaluators to put the product through its paces, by running a broad range of real-world tests and observing the output. Additional configuration information is available (the CSA MC Install Guide and the CSA MC User Guide) for a more wide scale deployment.

After reading through this appendix, you should be familiar with the capabilities offered by the Cisco Security Agent, and have "hands on" experience installing, configuring, and managing the product.

This section contains the following topics.

Evaluation Instructions

This section of the document describes five distinct and concrete steps that you can take to see the power and ease of use that the Cisco Security Agent offers. Each of these steps stands by itself, but build sequentially on one another. Performing each of these steps in sequence will provide a very complete, in-depth analysis and demonstration of the product.

Test 1: Agents are managed from the same console as Firewalls, Network IDS, and VPN devices

The Cisco Security Agent is managed from the Cisco Works platform (specifically, the VPN and Security Management application). This application also lets you manage PIX Firewalls, Cisco VPN concentrators, and Cisco Secure IDS appliances and blades. Centralizing security management functions lets you get more capability from the same set of trained administrators.

Other resources you might want to get:

- *Installing Management Center for Cisco Security Agents*, found on the product CD.
- *Using Management Center for Cisco Security Agents*, found on the product CD.

What you need to do this test:

- A computer to install CiscoWorks Common Services and CSA MC software on. CSA MC is supported on Microsoft Windows 2000 server, with Service Pack 3 installed. Note that if only a few agents will be installed during these tests, it can be installed on Microsoft Windows 2000 Professional.
- One or more computers to install Cisco Security Agent agents on. For this test, it is recommended that Microsoft Windows server or desktop computers are used (either Windows NT 4.0, Windows 2000, or Windows XP). We will test UNIX agents in a later step.

- A computer that you can use to attack the Cisco Security Agent protected systems. You may or may not want to do this, but this document offers some recommendations on tools you can use to attack your computers. Note that some tools run under Windows, while others run under Linux. You may need two computers, or one that will boot either Operating System.
- IP communications between these systems. Communications between agents and servers use secure HTTP (port 443). It is helpful to have access to the Internet to download exploits to exercise the Cisco Security Agent's protection as well.
- An evaluation software license key from Cisco. You will need to get an evaluation key from Cisco to install agents to protect systems.

Things to keep in mind:

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

Step 1. Install the Management Center for Cisco Security Agents

Place the CiscoWorks (VPN and Security Management) CD in the CD drive of the computer that will be CSA MC. If you have CD autorun enabled in the computer, the installation start screen will display automatically. You must install both CiscoWorks **Common Services** and **Managing Cisco Security Agents**.

The Managing Cisco Security Agents installation will prompt you for standard information like directories to use to install the software. It will also install and configure the database (Microsoft SQL Server Desktop Engine).

Tip If you already have Microsoft SQL Server 2000 with Service Pack 3 installed on the CSA MC computer, CSA MC will configure and use that, rather than install the desktop engine. While CSA MC will happily use SQL Server 2000, SQL Server version 7 is not supported. The CSA MC installation will abort, and tell you that you need to uninstall SQL 7.

Caution You have to be logged on as administrator to install the agent kits.

Caution If you don't have a key, agents will not register with the Manager. You can request an evaluation key which will ensure that agents work normally.

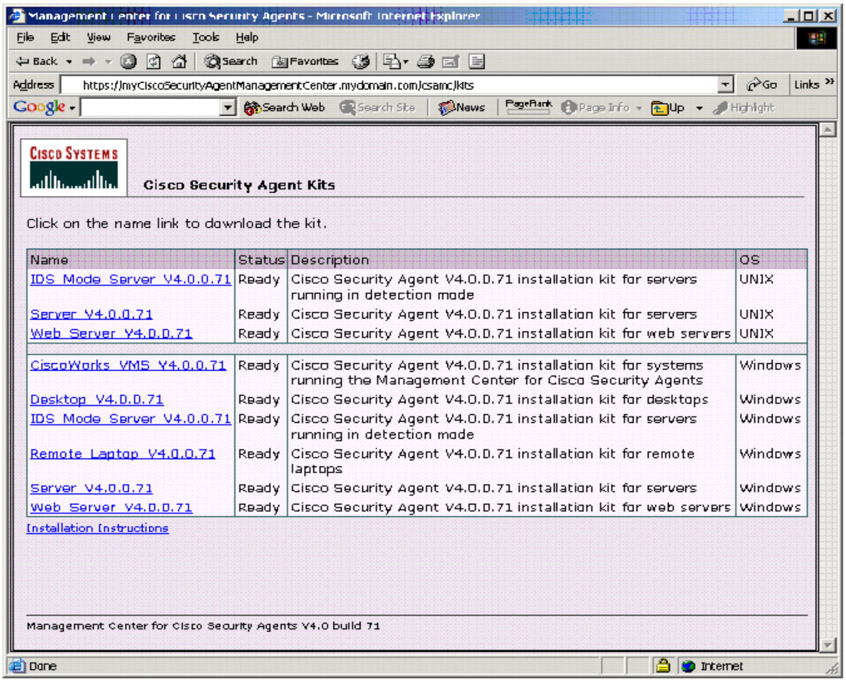
Step 2. Install Agent Kits on the computers you want to protect

Now you need to log into the Windows desktop or server computer(s) that you want to protect. The easiest way to install agent kits is to use a web browser to directly retrieve the kit from CSA MC. Since CSA MC uses a web server for remote access, and since the agent kits are small, you can easily download and install the appropriate kit on the remote computer.

In your browser, type the URL of the CSA MC computer, e.g. `https://myCSA MC.example.com/csamc/kits`. If you do not have DNS configured, you will need to type CSA MC's IP address in the browser URL window, e.g. http://10.0.1.17. You can use either Internet Explorer or Netscape browsers to do this. Note that this is a secure web page—using an "https" URL.

Figure B-1 shows you the Agent Kits web page. While you could choose to log in to CSA MC via CiscoWorks via the main web page (http://myCSA MC.example.com), let's leave that for later. Cisco Security Agent allows you to protect agent computers without even logging in, so let's go straight to installing agent software. Click on the button that says "Agent Kits".

Figure B-1 Getting Agent Kits Page


Management Center for Cisco Security Agents - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://myCiscoSecurityAgentManagementCenter.mydomain.com/csamc/kits
Go Links
Google Search Web Search Site News PageRank Page Info Up Highlight
Cisco Systems
Done
Internet

Cisco Security Agent Kits

Click on the name link to download the kit.

Name	Status	Description	OS
IDS Mode Server V4.0.0.71	Ready	Cisco Security Agent V4.0.0.71 installation kit for servers running in detection mode	UNIX
Server V4.0.0.71	Ready	Cisco Security Agent V4.0.0.71 installation kit for servers	UNIX
Web Server V4.0.0.71	Ready	Cisco Security Agent V4.0.0.71 installation kit for web servers	UNIX
CiscoWorks VMS V4.0.0.71	Ready	Cisco Security Agent V4.0.0.71 installation kit for systems running the Management Center for Cisco Security Agents	Windows
Desktop V4.0.0.71	Ready	Cisco Security Agent V4.0.0.71 installation kit for desktops	Windows
IDS Mode Server V4.0.0.71	Ready	Cisco Security Agent V4.0.0.71 installation kit for servers running in detection mode	Windows
Remote Laptop V4.0.0.71	Ready	Cisco Security Agent V4.0.0.71 installation kit for remote laptops	Windows
Server V4.0.0.71	Ready	Cisco Security Agent V4.0.0.71 installation kit for servers	Windows
Web Server V4.0.0.71	Ready	Cisco Security Agent V4.0.0.71 installation kit for web servers	Windows

Installation Instructions

Management Center for Cisco Security Agents V4.0 build 71

There are three types of agent kits that are automatically generated during the CSA MC installation:

- Servers. The security policy for these kits is optimized for server-class machines, running server-class applications. These kits provide the protection that you would want on most, if not all, of your servers. There is a different agent kit for UNIX and Windows servers—UNIX agent kits are on the top of the screen, and Windows agent kits are on the bottom. You can choose to install the agent kit in IDS Mode (it will alert you but will not block any actions), by clicking on the "IDS Mode Server" kit.
- Desktops. This is the agent kit that is optimized to protect Windows desktop computers running desktop applications. These kits provide the protection that you would want on most, if not all, of your desktops. Note that this agent kit is offered only for Windows computers.
- Cisco Works VMS. This agent kit is optimized to protect the CiscoWorks VPN and Security Management System (VMS), which hosts CSA MC. Cisco strongly recommends that you install this agent kit on every CSA MC.

Right now, you'll want to click on the appropriate agent kit (server or desktop) that you want to install. It's fine to run the install straight from CSA MC, or you can save the agent kit locally and run it from the local hard drive. Note that no interaction is required during the installation—the agent automatically does all local setup, and automatically registers itself with CSA MC.

Tip There's no need to distribute encryption keys to the agents. The agent kit contains everything that the agent needs to securely communicate with CSA MC. Since it uses the SSL encryption capability that your Operating System contains, you probably have strong encryption installed already.

Tip When you're done installing the agent kit, you'll have to reboot. The reason for this is that Cisco Security Agent hooks many different locations in the kernel. You'll only need to do this once. If you like, you can change this so that agent kit installation does not require a reboot.

Congratulations! A Cisco Security Agent is now protecting your computer. Now, let's test it. The best way to test it is to attack it.

Step 3. Attack your system

The proof of any security product is in how well it protects. The Cisco Security Agent is designed to provide unmatched protection "out of the box", without any configuration being required. However, testing this requires that you actually try to attack the computer.

There are many tools available on the Internet that you can find to test your security. Table B-1 lists a small selection of reputable sites that we believe offer high caliber tools for this purpose.

Each of these tools performs a different task, and is used for a different purpose. The following sections show the purpose for each of the tools (i.e. what the tool does when the Cisco Security Agent is not protecting the target), and the expected outcome when the Cisco Security Agent is protecting the target.

Step 3a. Scanning with nmap

nmap is a tool used to identify which devices are present on a network, and what Operating System and services they are running—indeed, the name stands for **N**etwork **M**apper. nmap works by sending a series of network probes to the target; the fact that the target responds identifies that it is there (and also which ports it is running), and the pattern of error messages returned identifies the OS. nmap is surprisingly accurate in identifying targets. It is frequently used at the initial stage of an attack or investigation, to determine what systems might respond to an attacker's exploits.

Table B-1 Tools To Test Cisco Security Agent protection

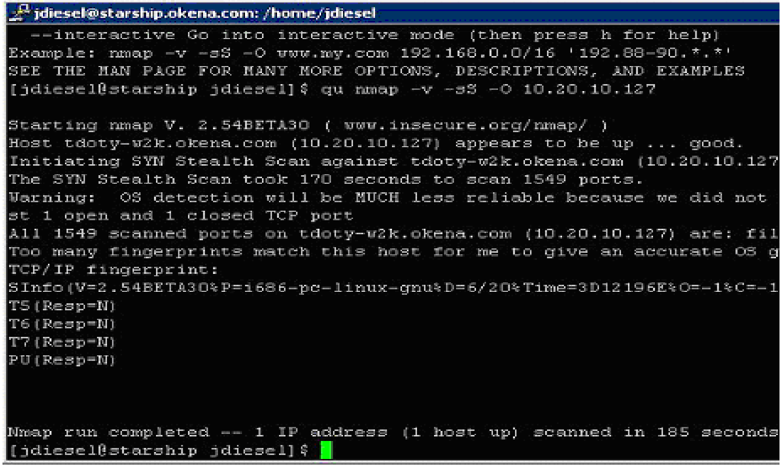
Tool	Site	Comments
nmap	http://www.insecure.org/	Most sophisticated network mapping and discovery tool. Does an excellent job of identifying the Operating System of the target device. Very commonly encountered.
Nessus	http://www.nessus.org/	A free, Linux-based, Open Source vulnerability scanner. Contains a very large list of current exploits for both UNIX and Windows systems.

Table B-1 Tools To Test Cisco Security Agent protection (continued)

Tool	Site	Comments
Windump	http://windump.polito.it/	High quality, free network packet and password capture tool. Windows version of UNIX tcpdump.
Etherpeek	http://www.wildpackets.com/	Good commercial packet sniffer.
Silentlog	http://packetstorm.decepticons.org/Win/SilentLog.zip	Keystroke logger with source code.
Pwdump2	http://razor.bindview.com/tools/files/pwdump2.zip	Allows encrypted password hashes to be dumped, even if the Windows 2000 system is protected (running SYSKEY).
Firehole	http://keir.net/firehole.html	Personal Firewall testing tool that uses DLL Injection.
netcat	http://www.atstake.com/research/tools/	Among other features, can act as a remote login server on any port.
Command Shell	%Systemroot%\system32\cmd.exe (Windows) /bin/sh (UNIX)	Lets you run commands from a command line.

Expected outcome of nmap scans against Cisco Security Agent-protected systems: nmap is unable to identify the target operating system of systems running the default server or default desktop policies. nmap scans will appear to hang while its security tests timeout. nmap scans against systems not protected by Cisco Security Agent will report results very quickly. Figure B-2 shows a screenshot of an nmap scan against a Windows system protected by Cisco Security Agent.

Figure B-2 Scanning a Windows system with nmap



```
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
[jdiesel@starship jdiesel]$ qu nmap -v -sS -O 10.20.10.127

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Host tdoty-w2k.okena.com (10.20.10.127) appears to be up ... good.
Initiating SYN Stealth Scan against tdoty-w2k.okena.com (10.20.10.127
The SYN Stealth Scan took 170 seconds to scan 1549 ports.
Warning:  OS detection will be MUCH less reliable because we did not
st 1 open and 1 closed TCP port
All 1549 scanned ports on tdoty-w2k.okena.com (10.20.10.127) are: fil
Too many fingerprints match this host for me to give an accurate OS g
TCP/IP fingerprint:
SInfo(V=2.54BETA30%P=i686-pc-linux-gnu%D=6/20%Time=3D12196E%O=-1%C=-1
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)



Nmap run completed -- 1 IP address (1 host up) scanned in 185 seconds
[jdiesel@starship jdiesel]$ 
```

Caution Disabling the Cloak System option (enabled by default in the Default Server and Default Desktop policies) will allow nmap to gather much more information.

Step 3b. Scanning with Nessus

Nessus is an Open Source vulnerability scanner that runs on a Linux computer. It makes network connections to remote systems and runs many hundreds of security tests against them. Nessus is one of the few scanners that relies extensively on exploits to determine vulnerability—it typically does not rely on any "banner" information passed back from the remote service (e.g. "Sendmail 8.8.2 ready"), but instead actually tries to break into the service.

Nessus is well regarded in the security industry, and is frequently updated with new tests. It is frequently used to perform network security audits.

Expected outcome of Nessus scans against Cisco Security Agent-protected systems: Nessus will not detect any vulnerabilities in systems running the default server or default desktop policies. Nessus status screens will be blank, and its reports will show no vulnerability information. Nessus scans against systems not protected by Cisco Security Agent will typically report large numbers of "holes", "warnings", or "notes".

Caution Disabling the Cloak System option (enabled by default in the Default Server and Default Desktop policies) will allow Nessus to gather much more information.

Step 3c. Capturing packets with Windump or dsniff

Packet capture programs are sometimes referred to as packet "sniffers", after the popular Sniffer™ product sold by Network Associates. These utilities are used for a wide range of uses, from legitimate network troubleshooting to the much more shady password theft.

Windump is a Windows version of the popular tcpdump packet capture and analysis utility. Since it uses the tcpdump data format, add-on utilities that process tcpdump logs will also process Windump logs. This makes Windump a useful and popular packet capture utility. Dsniff is another popular packet capture program.

Expected outcome of running Windump on Cisco Security Agent-protected systems: Cisco Security Agent detects applications that perform unusual interactions with the NIC (more specifically, with the NDIS interface in Windows or with streams in UNIX). These events will be intercepted either at boot time (Windows) or in real-time (UNIX).

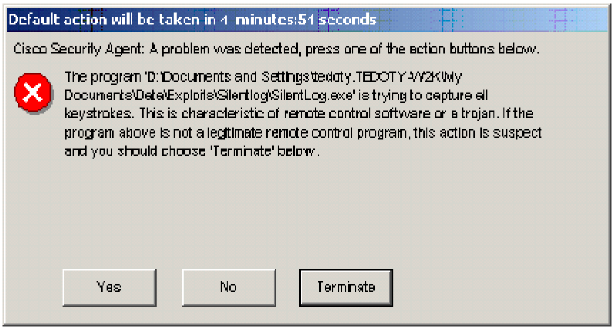
Tip Since Windump interfaces with the NIC at boot time, you'll have to reboot the computer after installing Windump if you want to test Cisco Security Agent's capabilities.

Step 3d. Capturing keystrokes with Silentlog

Silentlog is a "keystroke logger" program that silently captures all keyboard input and logs them to a file. Attackers often install keystroke loggers to capture passwords entered by users. Many Trojan horse programs include keystroke logging as a feature.

Expected outcome of running SilentLog on Cisco Security Agent-protected systems: Cisco Security Agent will generate a message saying that an attempt is being made to capture all keystrokes. The user will be able to select "Yes" (allow this action to take place), "No" (block this action but let the program continue to run), or "Terminate" (terminate the application that caused this event). By default, Cisco Security Agent will terminate the application trying to capture keystrokes if no selection is made within 5 minutes. Figure B-3 shows this message box.

Figure B-3 User queried about keyboard sniffing



Default action will be taken in 4 minutes:51 seconds

Cisco Security Agent: A problem was detected, press one of the action buttons below.

The program 'D:\Documents and Settings\tedoty.TEDOTY-W2K\My Documents\Data\Exploits\Silentlog\SilentLog.exe' is trying to capture all keystrokes. This is characteristic of remote control software or a trojan. If the program above is not a legitimate remote control program, this action is suspect and you should choose 'Terminate' below.

Tip You can install SilentLog anywhere, on any drive, under any name. You could, for example, install it under the name IEXPLORE.EXE (the name used by the Internet Explorer web browser). What is important to the Cisco Security Agent is not the name, but the action that the application takes.

Tip Some programs trap keyboard input as part of their normal operations. The AOL Instant Messenger and Yahoo Messenger instant messenging clients are two examples of this.

Step 3e. Hijacking applications via overwriting memory or via DLL Injection

A popular attack program that tries to steal passwords from the Windows registry is PWDUMP2. PWDUMP2 tries to overwrite a table used by the Local Security Authority subsystem (lsass.exe) to grant itself privilege to access the passwords. These hashes are then analyzed by password cracking routines like Crack, l0phtcrack, or John the Ripper.

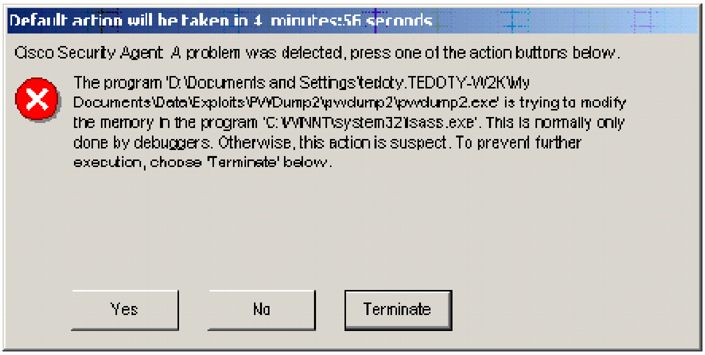
Another attack method involves tricking another application into executing your code. Common software routines are stored in collections called libraries. Microsoft Windows provides a built-in ability to load these libraries as required—this capability is called *Dynamically Linked Libraries*, and is abbreviated DLL. One form of attack is to insert (or "inject") a new and malicious DLL into a running application. This attack is called "DLL Injection."

Another application that uses DLL injection is FIREHOLE, which is used to test whether personal firewall applications can "leak"—whether applications can make unauthorized outgoing connections.

Expected outcome of running PWDump2 or Firehole on Cisco Security Agent-protected systems: The Cisco Security Agent detects applications that try to overwrite a different application's memory, or that inject code into other running applications. As with our keyboard sniffing example, the user will see a pop-up box that identifies the application and asks whether the user wants to let this activity occur, block the application, or terminate the offending application. Figure B-4 shows this dialog box. Note that while Figure B-4 shows the result of running PWDump2, you would see a similar message if you used Firehole.

Tip There are very few legitimate programs that use this technique. If you see activity like this—especially from downloaded programs—you should be extremely suspicious.

Figure B-4 User queried about DLL injection activity



Default action will be taken in 4 minutes:56 seconds

Cisco Security Agent A problem was detected, press one of the action buttons below.

The program 'D:\Documents and Settings\teddty.TEDDTY-W2K\My Documents\Data\Exploits\PWDump2\pwdump2\pwdump2.exe' is trying to modify the memory in the program 'C:\WINNT\system32\lsass.exe'. This is normally only done by debuggers. Otherwise, this action is suspect. To prevent further execution, choose 'Terminate' below.

Step 3f. Replacing critical portions of the Operating System (rootkit attacks)

One of the classic attacks against UNIX systems (dating from the 1980s or before) was to replace critical Operating System (OS) binaries. For example, the routine used by most UNIX systems to authenticate users during login is the program /bin/login. Replacing this program with a different one that stores the passwords in a secret file is the classic subversion attack against UNIX.

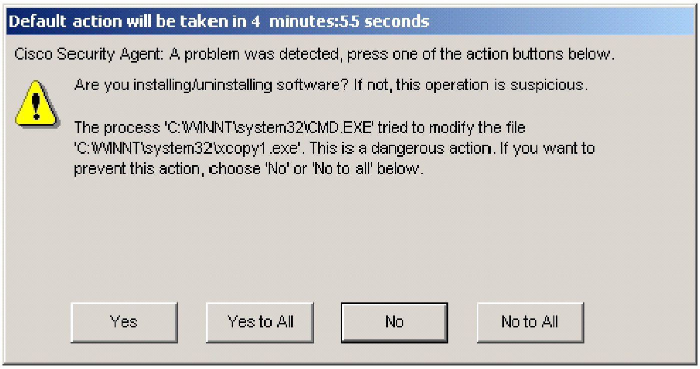
Windows stores many of these routines in the SYSTEMROOT, which is typically found in the directory C:\WINNT\SYSTEM32. Not only are there executable routines here, but DLL libraries as well.

Many malicious programs attempt to modify or replace these programs. For our example, you can use a command shell (MS DOS Prompt) to manually replace or copy files. You can run a command shell from the start menu by selecting "Run" and typing "cmd.exe" in the dialog box. In the command shell, type "CD %SYSTEMROOT%" and then "cd system32" to change to your OS directory.

All executables and libraries in this directory are protected. For testing purposes, we will use a relatively unimportant one, XCOPY. Rather than deleting it, we will simply copy it to another filename. At the command prompt, type "copy xcopy.exe xcopy1.exe". When you see the query message, choose "No".

Expected outcome of OS replacement attacks against Cisco Security Agent-protected systems: You will see a query popup asking whether this activity is desired. As with other queries of this type, you can allow, deny, or terminate the activity. Figure B-5 shows this query.

Figure B-5 User queried about OS replacement activity



Default action will be taken in 4 minutes:55 seconds

Cisco Security Agent: A problem was detected, press one of the action buttons below.

Are you installing/uninstalling software? If not, this operation is suspicious.

The process 'C:\WINNT\system32\CMD.EXE' tried to modify the file 'C:\WINNT\system32\xcopy1.exe'. This is a dangerous action. If you want to prevent this action, choose 'No' or 'No to all' below.

Caution In this example, we tried a trivial modification of the OS. You can try to actually delete critical files like SYSTEM.EXE or LSASS.EXE, and the Cisco Security Agent will protect you. However, you should make sure that Cisco Security Agent is in protection mode (in other words, you are not in "IDS Mode"—sometimes called "Test Mode"), and that you are running the default protection policy (either Default Servers or Default Desktops). If you have disabled the Cisco Security Agent, deleting or replacing these files will damage the Operating System.

Tip There are times when users will want to add executables or DLLs to the system32 directory—for example, when installing device drivers. Query messages will allow users to install drivers, but prevent silent malicious installation of attack programs. That is why the query box asks if the user is installing software. Query messages are configurable by the security administrator—if you don't want to give your users the ability to make security decisions, these rules can be configured to silently block the activity.

Step 3g. Unknown servers listening on high-number ports (backdoors)

A popular way to be able to connect to other systems is via an application listening (acting as a network server) on hard-to-find high number ports. If the attacker knows that he can connect to port 53,962, it is unlikely that most security defenses will be watching for this type of attack. Backdoor programs like this are included in most Trojan Horse applications.

netcat is a utility that can be used for many purposes, such as connecting to applications across the network and sending arbitrary data streams to it. It also provides the ability to listen (act as a server) on any port that you like (we've chosen port 23000 in the example below).

```
nc -l -p 23000 -t -e cmd.exe
```

Attackers would start a netcat listener on a high level port, and then use netcat (or Telnet) on a remote system to connect to the listener:

```
telnet target.ip.address 23000
```

Expected outcome of unknown servers running on Cisco Security Agent-protected systems: The remote login session will be unable to connect to the netcat listener. The attacker may see a "Connection refused" message.

Caution Connecting to yourself—for example, "telnet localhost 23000"—will not trigger Cisco Security Agent. As it turns out, many applications use this internal localhost address to communicate. Cisco Security Agent does not block traffic that is both generated and received locally. You have to try to break into the netcat backdoor remotely.

Key Point: Notice that until you actually run some attacks, the Cisco Security Agent is very quiet. This is by intention: if your security system requires a lot of attention when you are not being attacked, all it is doing is making more work for you. The Cisco Security Agent is designed not only to stop attacks, but also to provide a very low number of alerts for you to manage.

Test 1 Summary

We saw several key points in this test:

1. Agents are managed from the same console as Firewalls, Network IDS, and VPN devices. The same Management platform can consolidate management of several security products.
2. The Cisco Security Agent protects against a large number of attacks with the default policies. There is no need to customize security policies to get protection.
3. The Cisco Security Agent does not generate a large number of alerts. Unless you attack it, it will not give you many alerts that you have to manage.

Test 2: Protection is proactive—Stops the unknown attack

The Cisco Security Agent differs substantially from traditional Host-based security products, in that it contains no signatures. Rather, it focuses on behavior, and blocks malicious or undesired behavior. By focusing on behavior, new and previously unknown attacks can be detected and blocked.

No new tests will be performed in this section—instead, we will analyze what happened in the tests we just ran, and determine that Cisco Security Agent protection will proactively stop undesired behavior.

What you need to do this test:

- The CSA MC used in the previous test. The Cisco Security Agent agent(s) reported all malicious activity to CSA MC. We will analyze these alerts in this test.
- A computer to connect to CSA MC. The CSA MC user interface is provided in a Web Browser. You need a computer with a browser to access the CSA MC's user interface. Both Internet Explorer (5.x or higher) and Netscape (6.2) are supported. Note that you can use a browser on CSA MC itself to connect to its user interface.

Step 1. Connect to CSA MC's URL using the web browser

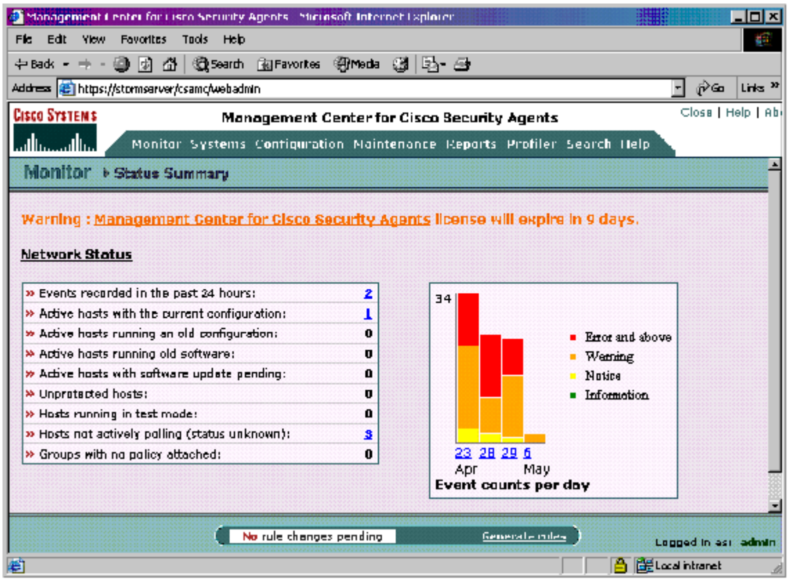
Using your browser, connect to CSA MC. If you are using a browser on the CSA MC computer, you can use the URL http://localhost. If you are using a browser on another computer, you will need to use a URL with CSA MC's domain name or IP address.

CSA MC runs under the Cisco Works management framework. This allows you to manage all of your Cisco security products from a single platform, using the same access method. For example, you can configure and monitor both your Cisco Security Agent host-based protection as well as your Cisco Secure IDS network-based protection from the same Cisco Works server.

Click the "Login" button, and type the user name and password that you defined when you installed CSA MC. Note that your browser may notify you that it does not recognize CSA MC’s web server certificate. This is normal, since CSA MC creates a unique certificate when it is installed. You can import the cert into your browser, but for now, it is fine to ignore this.

After selecting "VPN/Security Management Solution," "Management Center," and "Security Agent" in CiscoWorks, you will see the CSA MC Status Summary screen shown in Figure B-6.

Figure B-6 CSA MC Status Summary Screen


Management Center for Cisco Security Agents - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://stormserver/csamc/webadmin
Go Links
Cisco Systems
Management Center for Cisco Security Agents
Close | Help | Ab
Monitor Systems Configuration Maintenance Reports Profiler Search Help
Monitor ▸ Status Summary
34
Error and above
Warning
Notice
Information
23 28 29 6
Apr May
Event counts per day
Generate rules
Logged in as: admin
Local intranet

Warning : Management Center for Cisco Security Agents license will expire in 9 days.

Network Status

» Events recorded in the past 24 hours:	2
» Active hosts with the current configuration:	1
» Active hosts running an old configuration:	0
» Active hosts running old software:	0
» Active hosts with software update pending:	0
» Unprotected hosts:	0
» Hosts running in test mode:	0
» Hosts not actively polling (status unknown):	3
» Groups with no policy attached:	0

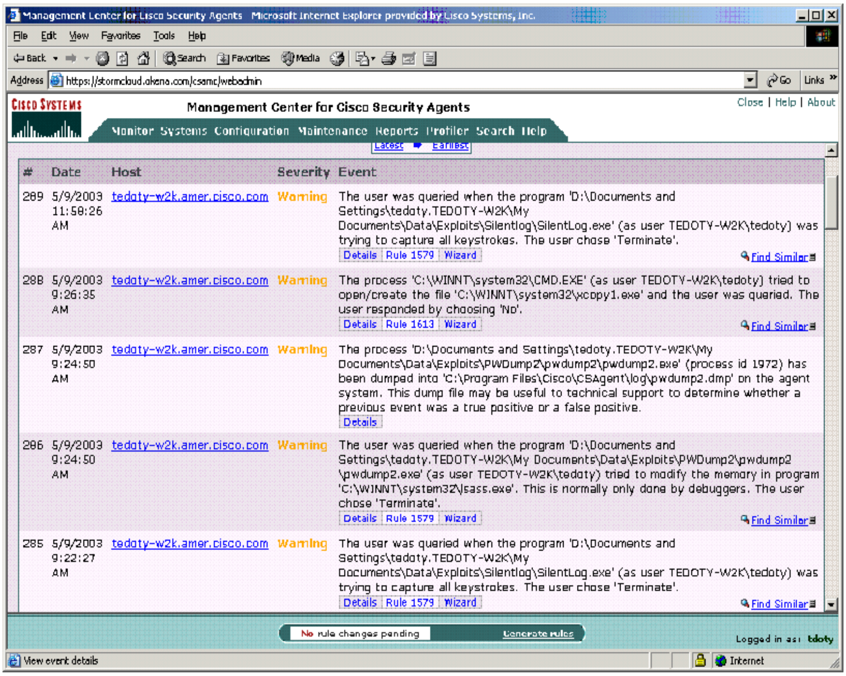
No rule changes pending

Step 2. Open the Event Log

The color coded Bar Graph contains a quick summary of the number and severity of the alerts that CSA MC has received. As we can see, in this example, there are several high severity events. Clicking on the red portion of the bar takes us directly to the Event Log screen that provides a detailed breakdown of the events for each Severity Level, as shown in Figure B-7.

The Event Log shows all of the alerts that were received by CSA MC. Some of these may be pop-up query messages that the user saw; others may relate to events that end users never saw. Note that if the alert is from a user query message, the alert will specify which action the user took (Allow, Deny, or Terminate).

Figure B-7 The E vent Log Screen


Management Center for Cisco Security Agents Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://stormcloud.okena.com/csamc/webadmin
Go Links
Cisco Systems
Management Center for Cisco Security Agents
Close | Help | About
Monitor Systems Configuration Maintenance Reports Profiler Search Help
Latest Earliest

#	Date	Host	Severity	Event
289	5/9/2003 11:58:26 AM	tedoty-w2k.amer.cisco.com	Warning	The user was queried when the program 'D:\Documents and Settings\tedoty.TEDOTY-W2K\My Documents\Data\Exploits\Silentlog\SilentLog.exe' (as user TEDOTY-W2K\tedoty) was trying to capture all keystrokes. The user chose 'Terminate'. Details Rule 1579 Wizard Find Similar
288	5/9/2003 9:26:35 AM	tedoty-w2k.amer.cisco.com	Warning	The process 'C:\WINNT\system32\CMD.EXE' (as user TEDOTY-W2K\tedoty) tried to open/create the file 'C:\WINNT\system32\xcopy1.exe' and the user was queried. The user responded by choosing 'No'. Details Rule 1613 Wizard Find Similar
287	5/9/2003 9:24:50 AM	tedoty-w2k.amer.cisco.com	Warning	The process 'D:\Documents and Settings\tedoty.TEDOTY-W2K\My Documents\Data\Exploits\PWDump2\pwdump2\pwdump2.exe' (process id 1972) has been dumped into 'C:\Program Files\Cisco\CSAgent\log\pwdump2.dmp' on the agent system. This dump file may be useful to technical support to determine whether a previous event was a true positive or a false positive. Details
286	5/9/2003 9:24:50 AM	tedoty-w2k.amer.cisco.com	Warning	The user was queried when the program 'D:\Documents and Settings\tedoty.TEDOTY-W2K\My Documents\Data\Exploits\PWDump2\pwdump2\pwdump2.exe' (as user TEDOTY-W2K\tedoty) tried to modify the memory in program 'C:\WINNT\system32\lsass.exe'. This is normally only done by debuggers. The user chose 'Terminate'. Details Rule 1579 Wizard Find Similar
285	5/9/2003 9:22:27 AM	tedoty-w2k.amer.cisco.com	Warning	The user was queried when the program 'D:\Documents and Settings\tedoty.TEDOTY-W2K\My Documents\Data\Exploits\Silentlog\SilentLog.exe' (as user TEDOTY-W2K\tedoty) was trying to capture all keystrokes. The user chose 'Terminate'. Details Rule 1579 Wizard Find Similar

Look at the alert generated when we ran PWDUMP2. You'll see an alert that says something like the following:

The user was queried when the program 'C:\Documents and Settings doty\Data\Products\PWDump2\pwdump2\pwdump2.exe' (as user TEDOTY-W2Kedoty) tried to modify the memory in program 'C:\WINNT\system32\lsass.exe'. This is normally only done by debuggers. The user chose 'Terminate'.
[Details] [Rule 1579] [Wizard]

Key Point: Notice that the activity was denied. The rule did not alert us about an attack that possibly was under way and that we might want to look into. Rather, the attack was intercepted and terminated. The alert is interesting for the administrator only in a historical sense—there is no need to have a room full of security operators watching consoles, looking for things to turn red. Even if the agent cannot communicate with the console, the system will be protected with the last policy that the agent received.

Tip There are not 1579 rules that ship with the Cisco Security Agent product. Rules are renumbered for each product release to ensure that rules are always unique (in other words, to ensure that you are always running the latest rule). Typically, the default policies for servers and desktops contain 30 to 40 rules.

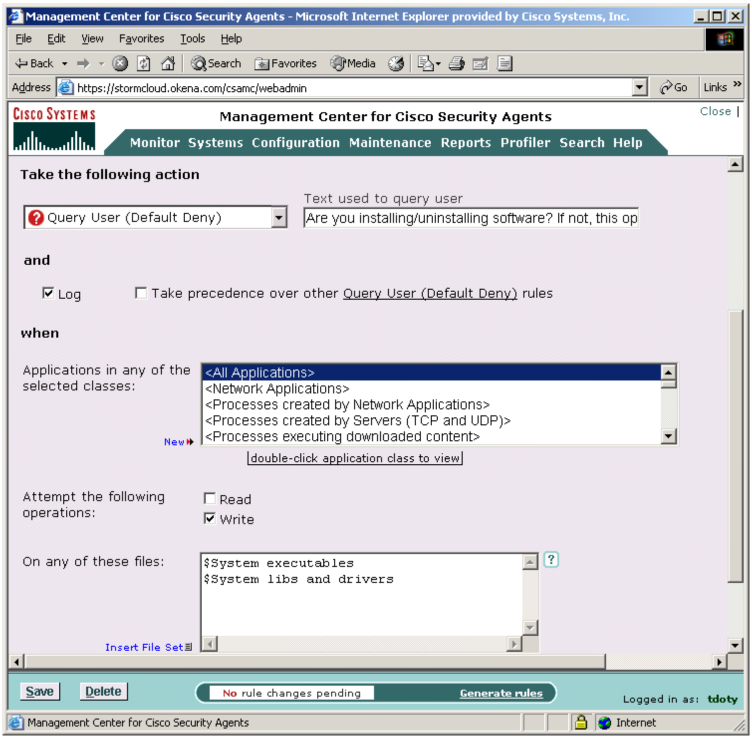
Step 3. Click through to the rule that caused this alert

Now let's look at why we couldn't copy the XCOPY.EXE program. You'll see an alert that says something like the following:

The process 'C:\WINNT\System32\cmd.exe' (as user CISCO-MAdoty) tried to open/create the file 'C:\WINNT\system32\xcopy1.exe' and the user was queried. The user responded by choosing 'No'.
[Details] [Rule 1613] [Wizard]

Let's take a look at rule 1613, which controls this activity. Click on the link to the rule, which will display the actual rule (shown in Figure B-8).

Figure B-8 The Rule Screen


Management Center for Cisco Security Agents - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://stormcloud.okena.com/csamc/webadmin
Go Links
Cisco Systems
Management Center for Cisco Security Agents
Close
Monitor Systems Configuration Maintenance Reports Profiler Search Help
New
Insert File Set
Save Delete
No rule changes pending
Generate rules
Logged in as: tdoty
Management Center for Cisco Security Agents
Internet

Take the following action

Query User (Default Deny)

Text used to query user: Are you installing/uninstalling software? If not, this op

and

☑ Log ☐ Take precedence over other Query User (Default Deny) rules

when

Applications in any of the selected classes:

- <All Applications>
- <Network Applications>
- <Processes created by Network Applications>
- <Processes created by Servers (TCP and UDP)>
- <Processes executing downloaded content>

double-click application class to view

Attempt the following operations:

☐ Read
☑ Write

On any of these files:

```
$System executables
$System libs and drivers
```

Note that we can tell several things from the rule screen:

- The user will be queried as to whether the activity is allowed or not.
- If the user doesn't make a selection, the default action will be that the activity is blocked.
- The rule will trigger when any application trying to write system executables, system libraries, or drivers.

Tip Note that we have a couple pre-defined variables here: System Executables and System libs and drivers. Cisco has predefined these to relate to the specific files of these types for the various Operating Systems that the Cisco Security Agent supports. These variables can be examined and modified if desired, but there is typically no need to do so.

Key Point: What is important to note here is that most of the rules that we've caused to trigger are very generic in nature. Rather than a signature to look for a particular executable file, the rules look for types of activity that are not desired. What is important is not that cmd.exe (or a particular version of cmd.exe) that tried to modify a system executable; as you can see from the rule, any application trying to overwrite the Operating System will trigger exactly the same reaction. The application could be a web browser that is executing malicious mobile code, or an email client program that executes a malicious attachment, or a web server attacked by a remote exploit. Since all applications are effected by this rule, the system is protected against all manner of attacks against the Operating System binaries.

Tip One result of this is that there is typically little or no need to have a specific security policy for an individual application. The default policies for desktops and servers provide broadly-based security coverage that applies to all applications that run on the system.

This ability to block attacks based on behavior, rather than signatures, is the reason that we say that Cisco Security Agent is Proactive.

Test 2 Summary

We saw several key points in this test:

- The Cisco Security Agent stops attacks. All Cisco Security Agent alerts are of the form "I saw this activity which violates your policy, so I stopped it". By the time the security administrator sees the alert on CSA MC, the activity has already been stopped. The Cisco Security Agent does not provide Intrusion Detection, it provides Intrusion Prevention.
- The Cisco Security Agent protects against attacks that it has never seen before, because the protective rules target malicious activity, not particular offending programs or network traffic. Any application that behaves in a way proscribed by the rules will be detected, and the activity stopped. Even applications that have never been seen before—or perhaps not even created when the rule was defined—will be controlled.

Test 3. The Cisco Security Agent is easy to customize

Now that we've seen the "out of the box" proactive protection that the Cisco Security Agent can provide, let's see what is required to tune the default server and desktop policies to fit your local security environment. Since the rules are easily configured via a "point and click" interface, this will be relatively straightforward.

Tip You will typically only do this to adapt the default policies to your environment. While every environment is a little different, there should be no reason to change many rules to get an exact fit. There is also little need for most people to create custom policies, or policies for most applications—the broad protection provided by the default policies will protect all applications running on a system.

What you need to do this test:

- The CSA MC used in the previous test. We will modify some of the rules that caused alerts in the first test.
- A computer to connect to CSA MC. Remember, you can use a browser on CSA MC itself to connect to its user interface.
- A computer running the Cisco Security Agent to test the customized policy. We will repeat Step 3f from Test 1. It's best to use the same computer that you used in Test 1, but any computer running the same policy will work, too.

Step 1. Connect to the CSA MC's URL using the web browser, and go to the Event Log screen

Using your browser, connect to CSA MC. Log in with the username and password you entered when installing the CiscoWorks software, and open up CSA MC from the "VPN/Security Management Solution".

If you didn't start there on login, select "Event Log" from the "Monitor" menu. You should see a screen that looks like the one we saw in Figure B-7. You should see an alert from the time you tried to copy XCOPY.EXE to a different name in the system32 directory.

In the last test, we just looked at the rule that stopped this. Now let's modify the rule.

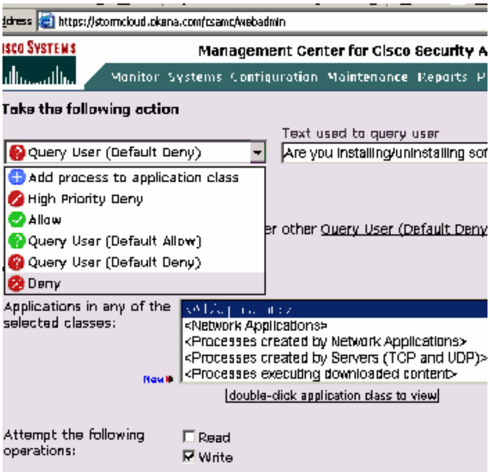
Step 2. Jump to the rule

This step is just like step 3 in the previous test. To view the rule, click on the link to the rule in the alert. We saw this rule earlier in Figure B-8.

Let's assume that our environment is a little different. We do not want users to be able to install drivers or update the Operating System—perhaps our IT organization takes care of all driver and hotfix installation. Because the default policy allows the user to decide whether to do this (via the query pop-up messages), the default doesn't quite fit the way we work.

Let's change the rule to prohibit the action, rather than querying the user. Click the pull-down menu for the rule action and select "Deny", as shown in Figure B-9. We need to save the rule by clicking "Save" on the lower left hand side of the window. Congratulations—you've adapted a rule to your environment.

Figure B-9 Customizing a Rule


ddress https://stormcloud.okana.com/csamc/webadmin
isco Systems
Management Center for Cisco Security A
Monitor Systems Configuration Maintenance Reports H

Take the following action

Query User (Default Deny)

- Add process to application class
- High Priority Deny
- Allow
- Query User (Default Allow)
- Query User (Default Deny)
- Deny

Text used to query user: Are you installing/uninstalling sof

er other Query User (Default Deny

Applications in any of the selected classes:

<Network Applications>
<Processes created by Network Applications>
<Processes created by Servers (TCP and UDP)>
<Processes executing downloaded content>

New
double-click application class to view

Attempt the following operations:

□ Read
☑ Write

Tip Notice that we could have also chosen "High Priority Deny", which would have accomplished the same thing.

Step 3. Deploy the rule

While we've successfully changed the rule, we need to get it distributed to the agents. Updating large numbers of agents can be a daunting challenge with many security products. Fortunately, the Cisco Security Agent makes this easy.

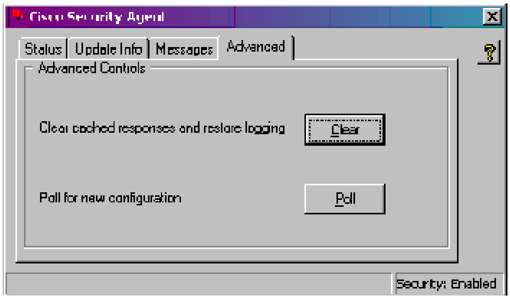
First, we need to regenerate the rule. This causes CSA MC to build a policy update package for every agent that uses the particular rule. Click "Generate", which you find in the middle of the bottom of the current screen. What you'll see is a screen that describes the change you are about to make. This is to give you a chance to change your mind before deploying changes to your running policies, and to verify that all the changes are what you want (you could have several rule changes generated all at the same time). Let's assume that we do in fact want to make this change. Go ahead and click "Generate" again.

You will see a few messages about what the CSA MC does when it generates the rule. There really isn't anything you need to do here, and this usually only takes a few seconds.

That's it! CSA MC has built updates for all agents that need them. As soon as the agent polls in, it will automatically get the modified policy and start enforcing it. Your agent will poll in after the default interval of 10 minutes. You can hurry this along by clicking on the red flag icon in the task bar of the system that is running the agent.

This opens up the local Cisco Security Agent GUI. Selecting the "Advanced" tab shows you the window in Figure B-10.

Figure B-10 Using the Cisco Security Agent local UI to poll



Clicking "Poll" causes the agent to poll immediately. Now you should have the updated policy running on your agent.

Key Point: Updating large numbers of agents has traditionally been the hardest part of managing security. While security policies tend to change slowly, each change typically required a considerable amount of "Leg Work" to deploy. The Cisco Security Agent is designed to completely eliminate policy update work—once rules are generated, the policy deploys itself.

Step 4. Repeat the attack from Test 1, Step 3f

This step was where we tried to copy an executable into the system32 directory. That time, we say a pop-up message asking whether this was OK. This time, all we get is an "Access is denied" message in our command shell. CSA MC has a new alert, but there was no end-user query.

Tip You will notice that the task bar flag icon on the system where the attack took place is now waving. This is to attract the attention of the end user, who can view the local alerts (but not modify the security policy). If you want, you can configure a group of agents so that the flag icon is hidden from the end user, and no pop-up query messages are generated. Since some organizations prefer not to make security products visible to users, this is easily configured.

Step 5. The Tuning Wizard helps automate policy tuning, and the optional "Profiler" product investigates alerts

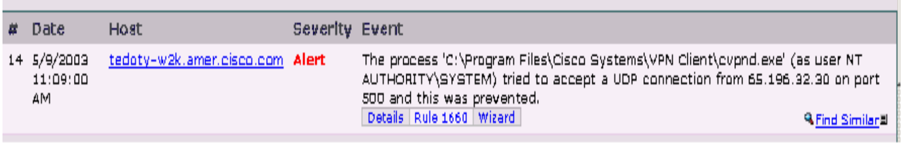
CSA MC contains a tuning wizard that automates the process of adapting Cisco Security Agent policies to local environments. The optional Cisco Security Agent Profiler product also will investigate application behavior to investigate alerts that you do not understand.

Tip Profiler will also create entirely new policies that control applications, based on how the application behaves in your environment. You can use this not only to investigate unknown activity that you see, but to create custom security policies for high-value applications.

Caution Profiler is a separately license component of CSA MC. You don't have to do anything to get the Profiler installed—it is automatically installed with CSA MC. You do have to install a license key to enable Profiler functionality.

You will find that many of the alerts in the Event Log have a "click-through" option: "[Wizard]". The wizard helps you customize policies to allow events that are normal or expected in your environment. It walks you through the process of deciding if this is normal, whether it is normal for one system or more systems, and how you would like the policy to be updated. It analyzes your current policies and makes recommendations as to the most sensible manner of making the update. At the end of the process, it makes the appropriate changes for you. Figure B-11 shows an alert with a link to the wizard.

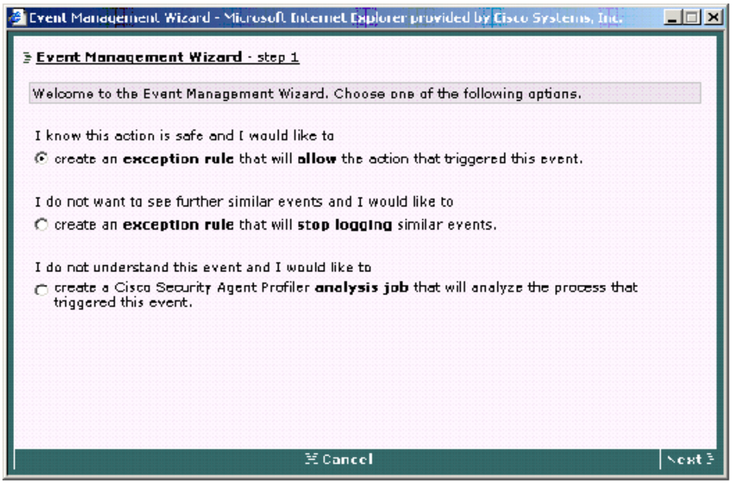
Figure B-11 An alert with a link to the Profiler policy wizard



#	Date	Host	Severity	Event
14	5/9/2003 11:09:00 AM	tedoty-w2k.amer.cisco.com	Alert	The process 'C:\Program Files\Cisco Systems\VPN Client\cvpnd.exe' (as user NT AUTHORITY\SYSTEM) tried to accept a UDP connection from 65.196.32.30 on port 500 and this was prevented. Details Rule 1660 Wizard Find Similar

Let's take a closer look at this alert. It seems that a VPN client wants to accept incoming network connections from the VPN concentrator. This is blocked by the Default Desktop policy, which does not allow desktop applications to act as network servers. Users haven't complained that the application isn't working correctly, but it is hard to know precisely what the impact to the application might be. Let's tune the policy to allow this behavior.

Figure B-12 The Tuning Wizard



Event Management Wizard - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Event Management Wizard - step 1

Welcome to the Event Management Wizard. Choose one of the following options.

I know this action is safe and I would like to
● create an **exception rule** that will **allow** the action that triggered this event.

I do not want to see further similar events and I would like to
○ create an **exception rule** that will **stop logging** similar events.

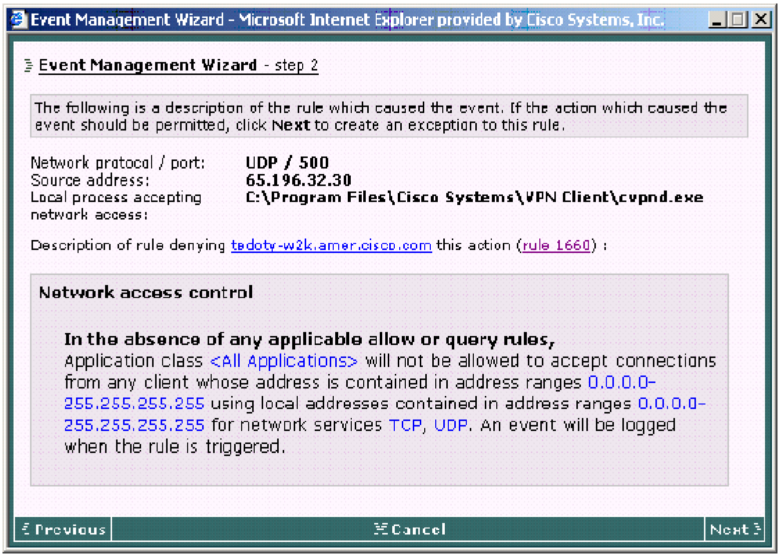
I do not understand this event and I would like to
○ create a Cisco Security Agent Profiler **analysis job** that will analyze the process that triggered this event.

Clicking the **Wizard** link brings up the first screen of the wizard, shown in Figure B-12. The wizard first provides the administrator with a decision point, since there are three mutually exclusive ways to tune your security policy to handle this type of event:

1. If this application is known to be safe in this environment—and a VPN client communicating with a VPN concentrator is almost certainly safe—you want to update your policy to let this activity occur in the future. If you select this option, the wizard guides you through the process of modifying the policy to allow this activity. By allowing behavior that you know to be safe to occur, you will eliminate future occurrences of this event.
2. If the application is trying to do something that you don't want to occur, but that you don't want to be notified about, you want to update your policy to disable logging/alerting for this event. For example, if a (possibly mis-configured) print server keeps trying to connect to one of your other servers, an agent may block and alert this activity. Assuming that this is activity you want blocked, you will find your event log filling up with a large number of these alerts, as the mis-configured server repeatedly tries to connect. Having the rule keep blocking the activity, but disabling logging, may be appropriate for situations like this.
3. If you don't know whether the action is safe, the wizard can set up a Profiler analysis job to observe the application and report on what it does. This will give you enough information to decide whether to allow the activity or to keep blocking it.

After taking a closer look at the VPN application, let's assume that this activity is low risk. We can also anticipate that this is something that is likely to occur frequently, and that not blocking this activity may result in more efficient operation. If there is a vulnerability in the VPN application—for example, perhaps a buffer overflow—the Default Desktop policy will still offer protection from attack. Therefore, let's use the wizard to change the policy. We will make sure that we've selected the radio button labeled "create an exception rule". Clicking the **Next** button brings up the next screen of the Wizard, shown in Figure B-13.

Figure B-13 The Policy Tuning Wizard



Event Management Wizard - Microsoft Internet Explorer provided by Cisco Systems, Inc.
Event Management Wizard - step 2

The following is a description of the rule which caused the event. If the action which caused the event should be permitted, click **Next** to create an exception to this rule.

Network protocol / port: **UDP / 500**
Source address: **65.196.32.30**
Local process accepting network access: **C:\Program Files\Cisco Systems\VPN Client\cvpnd.exe**

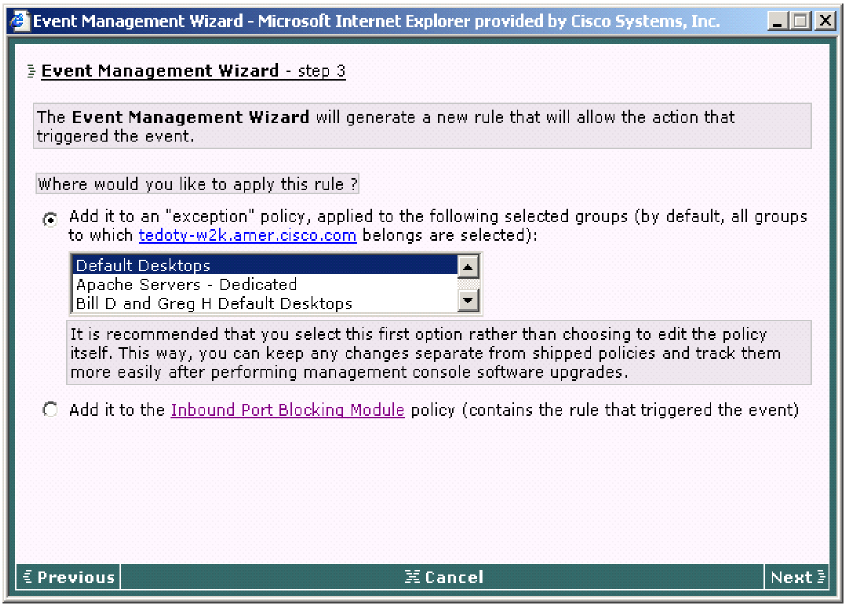
Description of rule denying tedoty-w2k.amer.cisco.com this action (rule 1660) :

Network access control

In the absence of any applicable allow or query rules,
Application class <All Applications> will not be allowed to accept connections from any client whose address is contained in address ranges 0.0.0.0-255.255.255.255 using local addresses contained in address ranges 0.0.0.0-255.255.255.255 for network services TCP, UDP. An event will be logged when the rule is triggered.

This screen shows the action that was blocked, and gives a description of the rule that blocked it. If you want, you can click through to the rule itself like we did in Test 2, but for now, let's just click **Next** to go to the next screen, shown in Figure B-14.

Figure B-14 Deciding how to update the policy



Event Management Wizard - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Event Management Wizard - step 3

The **Event Management Wizard** will generate a new rule that will allow the action that triggered the event.

Where would you like to apply this rule ?

● Add it to an "exception" policy, applied to the following selected groups (by default, all groups to which tedoty-w2k.amer.cisco.com belongs are selected):

Default Desktops
Apache Servers - Dedicated
Bill D and Greg H Default Desktops

It is recommended that you select this first option rather than choosing to edit the policy itself. This way, you can keep any changes separate from shipped policies and track them more easily after performing management console software upgrades.

○ Add it to the Inbound Port Blocking Module policy (contains the rule that triggered the event)

The wizard now shows your options on how to update the policy. One way is to actually change the policy module—the building block used by one or more policies—that contains this rule (in this case, the "Inbound Port Blocking Module"). Notice, however, that in this case the wizard recommends creating an "Exception" policy that will be included in the groups of systems that are affected. The group affected here (in other words, the group that contains the agent that generated the alert) is the Default Desktops group.

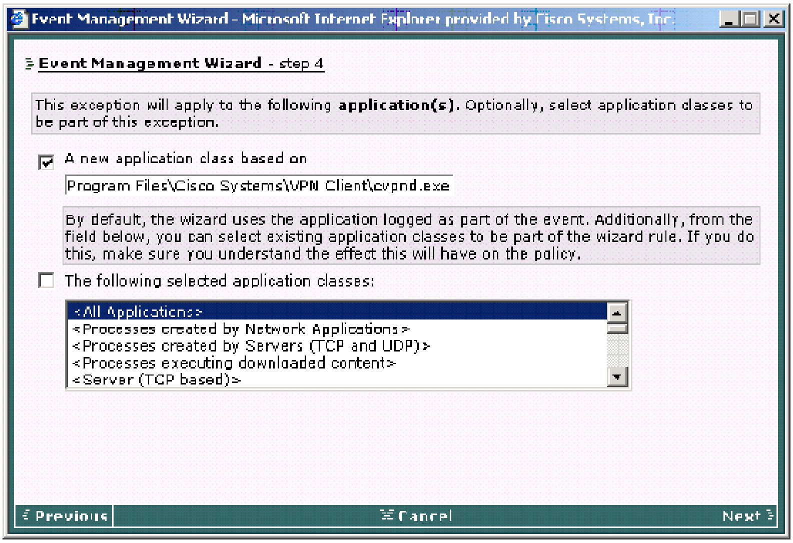
Tip This is actually the best way to tune most rules. There are a couple of reasons why. First, by collecting these "exceptions" in separate policy modules, you can easily see how you've customized your policies. If you changed a number of existing rules in a number of policies, it would be difficult or impossible to reconstruct later. Second, when you upgrade to a new release, the default policies might change, but your exception policy modules will be preserved untouched. This means that tuning your policies by using this exception policy module approach will be easier for you to understand and maintain in the future.

For now, let's take this approach. Click **Next** to continue.

The wizard now asks whether this exception applies only to the application in question—the application that caused the rule to block the action—or whether it applies to other types of applications. Note that Cisco Security Agent has a large number of applications that it knows about (applications that use the network, etc), and these are displayed in the wizard. However, the wizard recommends that the exception be applied more strictly—only to the Blackberry application itself. Click **Next**.

The wizard will now ask you which applications this exception rule will be applied to, as shown in Figure B-15. While you can choose to have a rule apply to one of the many built-in application sets (actually referred to as "classes"), or to all applications, the wizard will suggest that you make exceptions specific to the particular application causing the alert. This is the best approach for our VPN client, so we will let the wizard create a new application class for our VPN client. We're almost done, so click **Next** to go to the last step.

Figure B-15 Selecting the appropriate applications



Event Management Wizard - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Event Management Wizard - step 4

This exception will apply to the following **application(s)**. Optionally, select application classes to be part of this exception.

☑ A new application class based on

Program Files\Cisco Systems\VPN Client\cvpnd.exe

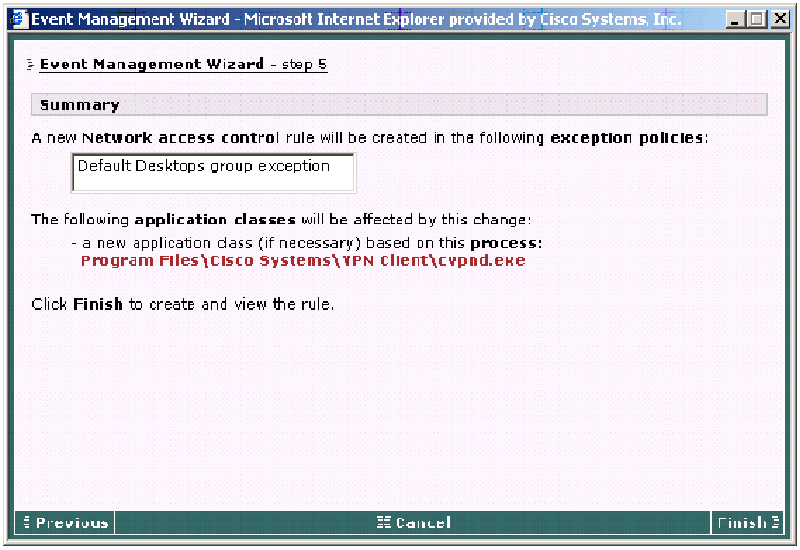
By default, the wizard uses the application logged as part of the event. Additionally, from the field below, you can select existing application classes to be part of the wizard rule. If you do this, make sure you understand the effect this will have on the policy.

☐ The following selected application classes:

<All Applications>
<Processes created by Network Applications>
<Processes created by Servers (TCP and UDP)>
<Processes executing downloaded content>
<Server (TCP based)>

The wizard now shows a summary (Figure B-16) of what you've decided to do. If you click **Finish**, the wizard builds or updates the appropriate policies. You'll have to click the **Generate Rules** button on CSA MC to update the live policies, and agents will get the updated policies the next time they poll in. If you click **Cancel** in the wizard, it discards your changes before committing them.

Figure B-16 Summary of policy changes


Event Management Wizard - Microsoft Internet Explorer provided by Cisco Systems, Inc.
Event Management Wizard - step 5
Summary

A new **Network access control** rule will be created in the following **exception policies**:

Default Desktops group exception

The following **application classes** will be affected by this change:

- a new application class (if necessary) based on this **process:**
Program Files\Cisco Systems\VPN Client\cvpnd.exe

Click **Finish** to create and view the rule.

Tip Profiler's analysis capability is very useful for forensics investigation. If your Network IDS reports traffic to a particular high-numbered port on a host, you can use Profiler to analyze what application is listening on that port and what it does. Profiler collects and summarizes all resource access requests that the application makes. It can even build a policy to "sandbox" the application, if you like. This ability to closely investigate mysterious applications can greatly speed up the security administrator's ability to identify undesired activity.

Key Point: While tuning policies to your environment is not a complex task, automation allows lower-level administrators to be effective in updating policies. Because the wizard guides the process, policies are updated sensibly. Using the wizard ensures that policies remain well-structured and maintainable over time.

Test #3 Summary

We saw several key points in this test:

1. The Cisco Security Agent is simple to customize. The CSA MC UI provides hotlinks to the pertinent rules, making it easy to identify which rules need modification to fit your local policy.
2. CSA MC provides a wizard to make customization even easier. The wizard helps automate more complex customization tasks, so that even junior level security administrators can quickly and sensibly adapt the Cisco Security Agent policies to their environment.

Test 4. The Cisco Security Agent runs on UNIX as well as Windows

So far, we've been doing all of our testing on Windows systems. Now let's see how the Cisco Security Agent performs in a heterogeneous Windows and UNIX environment.

What you need to do this test:

- The CSA MC used in the previous tests. We will do some testing on a Solaris system.
- A computer Sunning Solaris. Cisco Security Agent supports Solaris 8 systems.
- A computer to connect to CSA MC. Remember, you can use a browser on CSA MC itself to connect to its user interface. You can also use a Netscape 6.2 browser on the Solaris computer to connect to CSA MC.

Step 1. Install Agent Kits on UNIX computer

You'll need to log into the Solaris computer(s) that you want to protect. The easiest way to install agent kits is to use a Netscape web browser to directly retrieve the kit from CSA MC, just like we did on Windows computers in Test 1.

Tip There is a GNU utility called wget that will download an agent kit from CSA MC, when run from a command line. Systems that do not have web browsers, or where installation is desired to be scripted will find this utility handy. You can find a compiled wget Solaris 8 binary at http://www.sunfreeware.com/sol8right.html.

Tip You can also save the Solaris agent kit on a server, and use FTP to distribute it to your target computer.

Caution Unlike Windows systems, The Cisco Security Agent does not offer a "Default Desktops" agent kit for Solaris. It is assumed that all Solaris systems are servers, so only a "Default Servers" agent kit is provided by default. Note that the "IDS Mode Server" agent kit is also available for Solaris systems. As with the equivalent kit for Windows servers, this will alert, but not block activity.

In your browser, type the URL of the CSA MC computer, just like you did in Test 1. The Solaris agent kit is not an InstallShield executable—rather, it is a Solaris package. You install the agent kit just like you install any other Solaris package.

Caution Just like you need to be logged in with administrator privilege to install the agent kit on Windows computers, you have to be logged in as root to install the agent kit on Solaris computers.

We'll assume that you've used a Netscape browser to download the agent kit to your Solaris system. Once it's downloaded, you need to extract the files from the tar archive:

```
# tar xf CSA-Server_V4.0.0.76-setup.tar
```

The installation will be familiar to any Solaris system administrator: you use pkgadd to install the agent:

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

Caution While pkgadd installs and configures the agent, you will need to either reboot or kill and restart running processes for the agent to begin protecting the system. The reason is that the while the agent doesn't replace any portions of the Operating System, it intercepts calls to the OS in a number of places, but this interception is effected when the process starts running.

Step 2. Attack your system

Just like we did in Test 1, we need to attack the Solaris system to see how the Cisco Security Agent provides protection. You can use many of the tools discussed earlier.

Step 2a. Scanning with nmap or Nessus

Just as port scans are used against Windows targets, they are used against UNIX targets.

Expected outcome of Nessus or nmap scans against Cisco Security Agent-protected systems: Because the Solaris Operating System works very differently from Windows, the results of scanning your Solaris system are different then when you scanned your Windows system. Because the Solaris inetd process services all incoming connections (before handing them off to the appropriate service), nmap and Nessus will report that the Solaris system has a number of open ports. This will be true even if Cisco Security Agent is blocking incoming connections from the scanning host. While it may seem surprising that blocked ports are reported as open, this is an artifact of the way UNIX handles network connections—in fact, this is exactly what is seen when using other security tools like TCP Wrappers or xinetd.

Tip The Cisco Security Agent will report all port scans to CSA MC. CSA MC will also correlate these reported portscan events with similar events received from other agents to detect distributed port scans (port scans where many systems are scanned at the same time).

Tip Unlike TCP Wrappers, Cisco Security Agent provides centralized control of which systems will be blocked. If you like, you can even define "Hosts.Allow" and "Hosts.Deny" variable names to hold allowed or blocked systems, and enforce this globally. Unlike TCP Wrappers, you can also centrally control which applications are allowed to accept connections. For example, you could globally prohibit the use of Telnet to prevent the sending of unprotected passwords over the network.

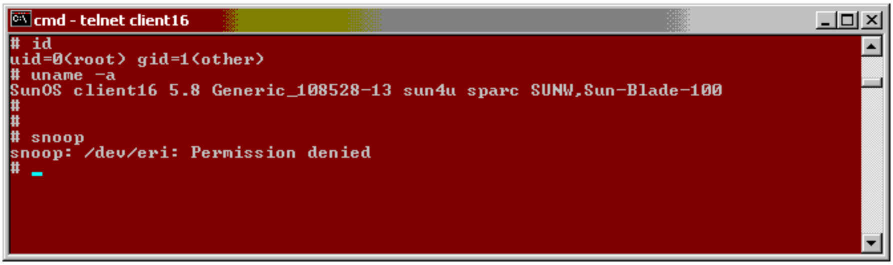
Tip If you use the Solaris system as the scanning computer, the Cisco Security Agent prevents the execution of both nmap and Nessus. Since both nmap and Nesus send many non-standard packets, they need to communicate directly with the network interface. The Cisco Security Agent prohibits this, so these applications will not run on a system protected by the Cisco Security Agent. If you try, you will get a message similar to the following generated by nmap (note how nmap is confused, and thinks that you are scanning localhost):

```
Starting nmap V. 2.54BETA28 ( www.insecure.org/nmap/ )
pcap_open_live: /dev/eri: Permission denied
There are several possible reasons for this, depending on your
operating system:
LINUX: If you are getting Socket type not supported, try modprobe
af_packet or recompile your kernel with SOCK_PACKET enabled.
*BSD: If you are getting device not configured, you need to
recompile your kernel with Berkeley Packet Filter support. If
you are getting No such file or directory, try creating the
device (eg cd /dev; MAKEDEV <device>; or use mknod).
SOLARIS: If you are trying to scan localhost and getting
'/dev/lo0: No such file or directory', complain to Sun. I don't
think Solaris can support advanced localhost scans. You can
probably use "-P0 -sT localhost" though.
```

Step 2b. Capturing packets with snoop

One of the first things that an attacker tries once he gains access to a UNIX system is to start a packet sniffer to capture passwords that are sent across a network. While there are many sniffer programs available, they all cause the NIC to change into "promiscuous" mode (i.e. receive and decode all packets seen on the network, not just those addressed to the system itself). For the purpose of this test, we've used snoop, a packet sniffer which comes bundled with Solaris.

Figure B-17 Capturing packets with a packet sniffer



```
# id
uid=0(root) gid=1(other)
# uname -a
SunOS client16 5.8 Generic_108528-13 sun4u sparc SUNW,Sun-Blade-100
#
#
# snoop
snoop: /dev/eri: Permission denied
# _
```

Expected outcome of packet sniffing against Cisco Security Agent-protected systems: The Cisco Security Agent Default Server policy prevents the NIC from changing into promiscuous mode. Different programs will handle the "access denied" OS signal differently, but Figure B-17 shows the result when snoop is run. Note that the user trying to run snoop is root. Root normally has unrestricted access to all system resources; this example shows that even the root account can be prevented from performing dangerous tasks.

Step 2c. Installing a backdoor on a high-numbered port

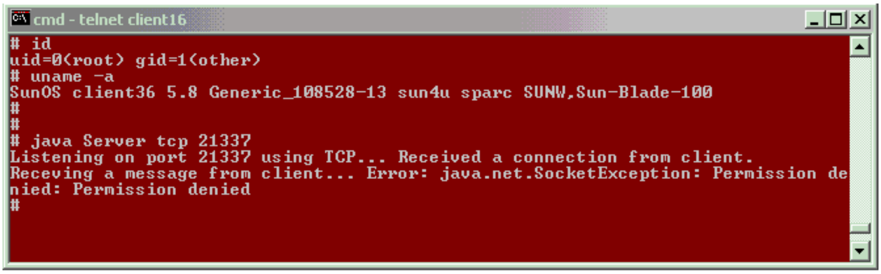
One of the most popular utilities for running backdoor services is netcat. As we saw earlier, you can use netcat to run a backdoor Telnet-like service on any port you like with the following command (this example causes netcat to listen on port 23000):

```
    nc -l -p 23000 -t -e /bin/sh
```

Unfortunately for our testing purposes (but good for security), we've seen that netcat won't even run on a Solaris system protected by the Cisco Security Agent, because it tries to hook directly into the NIC streams interface. Therefore, we have to use a different program to test the Cisco Security Agent. We chose to write a small Java program to do this, because Java is widely available (especially on Solaris systems). Also, many people know how to write small Java programs, so the number of potential attackers who can do this is large.

Expected outcome of running backdoor programs against Cisco Security Agent-protected systems: While the program may start up and believe that it is listening for incoming connections, (Figure B-18 shows us running a backdoor on port 21337), the Cisco Security Agent Default Server policy will prevent the remote client from connecting to the backdoor program.

Figure B-18 Running a backdoor program



```
# id
uid=0(root) gid=1(other)
# uname -a
SunOS client36 5.8 Generic_108528-13 sun4u sparc SUNW,Sun-Blade-100
#
#
# java Server tcp 21337
Listening on port 21337 using TCP... Received a connection from client.
Receving a message from client... Error: java.net.SocketException: Permission de
nied: Permission denied
#
```

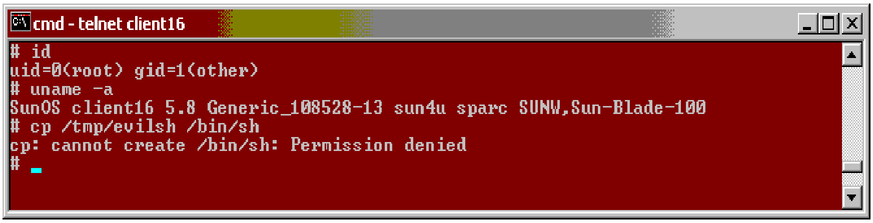
Tip The Java source code for this backdoor is listed at the end of this appendix.

Step 2d. Overwriting the Operating System (rootkit attacks)

As we said earlier, replacing critical Operating System (OS) binaries is one of the classic computer attacks. Any command shell (/bin/sh, /bin/csh) will let you try to replace critical system binaries.

Expected outcome of running backdoor programs against Cisco Security Agent-protected systems: As shown in Figure B-19, we attempted to overwrite the command shell program /bin/sh with one of our own, /tmp/evilsh. As you can see from the example, the Cisco Security Agent Default Server policy prevented this even though we were logged in as root.

Figure B-19 Trying to Trojan the Operating System binaries



```
# id
uid=0(root) gid=1(other)
# uname -a
SunOS client16 5.8 Generic_108528-13 sun4u sparc SUNW,Sun-Blade-100
# cp /tmp/evilsh /bin/sh
cp: cannot create /bin/sh: Permission denied
#
```

Key Point: The Cisco Security Agent offers the ability to secure UNIX and Windows systems, whether they are desktops (Windows) or servers (Windows or UNIX). This simplifies training, reduces the number of console systems that are required to manage security, and eliminates the need for data consolidation between products.

Test 4 Summary

We saw several key points in this test:

1. The Cisco Security Agent protects UNIX systems. Just like we did with Windows, we deployed agents that protected a Solaris system.
2. The Cisco Security Agent manages UNIX and Windows agents from a single console. CSA MC lets you control both Windows and UNIX systems from a single management point.

Summary

Congratulations! There's a lot to see in any new product, and we've seen a lot during our evaluation of the Cisco Security Agent. While any introduction can only cover the highlights, we've seen several key points:

1. Agents are managed from the same console as Firewalls, Network IDS, and VPN devices. The same management platform can consolidate management of several security products.
2. The Cisco Security Agent protects against a large number of attacks with the default policies. There is no need to customize security policies to get protection, or even to log into CSA MC.

3. The Cisco Security Agent does not generate a large number of alerts. Unless you attack it, it will not give you many alerts that you have to manage.
4. The Cisco Security Agent stops attacks. All Cisco Security Agent alerts are of the form "I saw this activity which violates the policy you specified, so I stopped it". By the time the security administrator sees the alert on CSA MC, the activity has already been stopped. The Cisco Security Agent does not provide Intrusion Detection, it provides Intrusion Prevention.
5. The Cisco Security Agent protects against attacks that it has never seen before, because the protective rules target malicious activity, not particular offending programs or network traffic. Any application that behaves in a way proscribed by the rules will be detected, and the activity stopped. Even applications that have never been seen before—or perhaps not even created when the rule was defined—will be controlled.
6. The Cisco Security Agent is simple to customize. The CSA MC GUI provides hotlinks to the pertinent rules, making it easy to identify which rules need modification to fit your local policy.
7. CSA MC provides a wizard to make customization even easier. The wizard helps automate more complex customization tasks, so that even junior level security administrators can quickly and sensibly adapt the Cisco Security Agent policies to their environment.
8. The Cisco Security Agent protects UNIX systems. Just like we did with Windows, we deployed agents that protected a Solaris system.
9. The Cisco Security Agent manages UNIX and Windows agents from a single console. CSA MC lets you control both Windows and UNIX systems from a single management point.

Frequently Asked Questions

How does the Cisco Security Agent integrate with the kernel of my Windows system?

The Cisco Security Agent uses the same interfaces that are currently used by anti-virus and personal firewall software manufacturers. These interfaces include file system filter drivers and the Network Driver Interface Specification (NDIS).

What is the performance impact incurred by running the Cisco Security Agent?

> Because the Cisco Security Agent does not scan packets for content (unlike AV and IDS products) the performance impact is less than 1-2%.

Do I need to replace any system programs?

> Because the Cisco Security Agent intercepts system calls at the operating system level, there is no need to replace any system programs.

What is the impact to Cisco Security Agent when a new service pack is released?

> Like all software companies, the Cisco will perform a thorough QA process to maintain currency with the latest Microsoft issued patches and service packs that will interact with the Cisco Security Agent software.

What is the impact of the Cisco Security Agent to newly installed executables on a system?

> Provided that the new software does not change the behavior of existing the Cisco Security Agent protected applications, there is no expected impact.

Do I need to develop policies in order to start using the Cisco Security Agent?

> The Cisco Security Agent ships with 'out of the box' agent kits and policies for default desktop and server systems. This makes the Cisco Security Agent immediately useful for securing your environment. Most organizations start with these policies, because they are designed to stop malicious activity. It also ships with a number of default policies for popular Microsoft applications such as IIS, SQL Server, and Office, for use by organizations that want to implement policy-based control over application behavior. These can be supplemented by new, user-defined policies as a the Cisco Security Agent implementation proceeds in scope.

What administrative overhead accompanies the Cisco Security Agent policy development and deployment?

> The Cisco Security Agent application-centric policies are easy to deploy because they don't need to be assigned to the user population, only to hosts; they can be simply evaluated without impacting production environments, through the use of test mode; and they can be disseminated simply through the enterprise by using host groups and agent polling.

What Sort Of Correlation Does the Cisco Security Agent Provide?

The Cisco Security Agent utilizes real-time correlation at both the agent and the global level. This provides greater accuracy for decision-making at the agent level and enables security to be dynamically adapted across the enterprise in reaction to events that occur on distributed hosts. The Cisco Security Agent real-time correlation enables the following functionality: Correlation of network scans (ping scans and port scans) Correlation and dynamic quarantining of files based on email worm events Correlation of OS events from host event logs Correlation of events received from AV scanners (files can be added to the Cisco Security Agent dynamic quarantine list).

Do Cisco Security Agent Default Policies Help With System Hardening?

Buffer Overflow protection, port scan detection, network worm protection, and Trojan detection are pre-configured rules that you can add to your policies in the same way you add other rules. These are basic system hardening features that should be applied in most cases.

How Does the Cisco Security Agent Protect Against Buffer Overflows?

When malicious code attempts to overrun buffers, the Cisco Security Agent can detect and prevent the accessing of system functions by code executing in data or stack space. This functionality was the key to preventing notorious buffer overrun attacks like Code Red and Nimda. Note that the Cisco Security Agent provides automatic protection to all applications from both Stack and Heap overflow attacks.

How Do Cisco Security Agent Policies Protect My Applications Against SYN Floods?

SYN floods results in half open connections on the server. An abundance of half open states on a server can prevent legitimate connections from being established. The Cisco Security Agent policies help to prevent the proliferation of half open states. You should apply SYN flood protection to servers within your enterprise, keeping them up and running and able to provide resources should a SYN flood attack occur.

How Do Cisco Security Agent Policies Protect My Applications Against Port Scans?

Using port scan protection in a policy causes the intelligent agent on a system to log an event when an attempt is made to scan the system for an open port. This can warn you if someone is mapping out your system in preparation for an attack. The intelligent agent also gathers information on the source IP addresses perpetrating a scan and it reveals the source address of the latest scan attempt. If scans are detected across several machines, the Cisco Security Agent correlates against these events and generates an additional event to warn of this correlation.

How Do Cisco Security Agent Policies Protect Against The Propagation Of Network Worms?

When a worm of this type is received through email and executed by unsuspecting users, it generally attempts to send copies of itself to all entries in the email address book of the user. In doing this, the worm modifies registry keys, writes its own script files, and modifies existing files. When this type of suspicious activity is detected, the intelligent agent queries the user, informing the user of this activity. When the user elects to stop the system action on the desktop where the worm was received, the network worm is prevented from propagating itself. The pre-configured Cisco Security Agent network worm protection rule also correlates a series of suspicious events across multiple machines.

How Do Cisco Security Agent Policies Protect My Applications Against Trojan Horses?

The included Trojan detection rule lets you enable several different types of Trojan detection. Trapping of keystrokes by network applications. (Detect and prevent applications that attempt to capture system keystrokes.) Accessing memory owned by other applications (Detect and prevent applications that attempt to interfere with the memory space of other applications.) Stealing local passwords (Detect and prevent applications that attempt to steal local system passwords.) Downloading and invoking executable file. (Detect and prevent applications that download executables and immediately attempt to execute them. This is a type of buffer overrun attack that takes the form of and email attachment executable file) Downloading and invoking ActiveX controls (Detect and prevent malicious applications acting like a Web browser).

Java code for backdoor program

The following Java application test illustrates what an attacker might use as a "back door" on a server.

Please note the following:

- This program is provided as an example only, and is not supported.
- To run the program you need to have Java Runtime Environment (JRE) installed on your machine. You can download it from http://java.sun.com/. Note that most Solaris builds include this by default.
- To run the executable you would execute this from the command line (note that this is case sensitive; you must type "Server" and not "server"):

  # java Server [protocol] [port] ===>CASE SENSITIVE!, so you must type "Server" and not "server"

  example:

  ```
  # java Server tcp 25000
  ```
  "Whenever in doubt of the arguments, just execute it without any arguments to get the usage statement.

```
/**  Server.java
 *   Version: 1.0
 *   Author: Veronika
 *  Date: 4/01/02
 */
import java.io.*;
import java.net.*;
import java.util.*;

/**
 * This program takes 2 command line arguments from the user
 * 1.Protocol to be used:  TCP or UDP
 * 2.Port number: 0 to 65,535
 *
 *
 * The server listens on a port and protocol specified by the
user listening
 * for a client connection.  Once client connected, it
receives and displays
```

```
 * a text message that the client sent.
 *
 */

public class Server
{
                 private final static int MINPORT = 0;
   private final static int MAXPORT = 65535;

   public static void main (String[] args) throws Exception
   {
       String protocol;  // protocol
       int port;         // port number

       //extract and authenticate command line arguments
       try
       {
          protocol=args[0];
          port=Integer.parseInt(args[1]);


           //Check protocol name specified for invalid name
           if (protocol.equalsIgnoreCase("TCP"))
             tcpConnect(port);
           else
             if (protocol.equalsIgnoreCase("UDP"))
                udpConnect(port);
              else
              {
                 System.out.println("Error: Invalid protocol
name used!");
                 System.out.println("Exiting...");
                System.exit(0);
              }

          //check port number in range
          if (port < MINPORT || port > MAXPORT)
          {
             System.out.println("Error: Port number is out of
range!");
             System.out.println("Exiting...");
             System.exit(0);
          }
       }catch (Exception e)
```

```
        {
            System.out.println("Usage: Server [protocol]
[port]");
             System.out.println("Where - [protocol] TCP or UDP
only");
            System.out.println("      - [port] is the port
number from 0 to 65,535");
            System.out.println("Example: Server TCP 80 ");
            System.exit(0);
        }
    }//end of main

    public static void tcpConnect(int port)
    {
        String message;

        try{
             //create a TCP socket for the client to 'knock' on
            ServerSocket listenSocket = new ServerSocket(port);
            System.out.print("Listening on port " + port + "
using TCP... ");
            do //loop waiting for a connection from client
            {
                Socket connectionSocket=listenSocket.accept();
                System.out.println("Received a connection from
client.");

                //establish in/out streams
                BufferedReader inFromClient=new
BufferedReader(new
InputStreamReader(connectionSocket.getInputStream()));
                DataOutputStream outToClient=new
DataOutputStream(connectionSocket.getOutputStream());

                //read the message from client
                System.out.print("Receving a message from
client... ");
                message=inFromClient.readLine();
                System.out.println("Done.");

                //print message received from client
                System.out.print("FROM CLIENT: ");
                System.out.println(message);
                //close the connection
                System.out.print("Closing connection to client...
");
                connectionSocket.close();
                System.out.println("Done");
            } while (true);
        }catch(Exception e)
        {
            System.out.println("Error: " + e);
        }


    }//end of tcpConnect
    public static void udpConnect(int port)
    {
        try{
            //create a UDP socket to listen on
            DatagramSocket serverSocket = new
DatagramSocket(port);
            System.out.println("Listening on port " + port + "
using UDP.");

            byte[] receiveData = new byte[1024];
             while(true)
            {
                DatagramPacket receivePacket = new
DatagramPacket(receiveData, receiveData.length);

                //receive a packet from client
                System.out.print("Waiting for a datagram
packet...");
                serverSocket.receive(receivePacket);
                System.out.println("Received.");

                //extract message received from client
                String message = new
String(receivePacket.getData());
                System.out.println("FROM CLIENT: " + message);

            }//end of while
        }catch (Exception e)
        {
                System.out.println("Error: " + e);
            }
        }

    } // end of server class
```

Third Party Copyright Notices

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

Openssl license

Copyright © 1998-2000 The OpenSSL Project. All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgement:
   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

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

SSLEAY license

Copyright © 1995-1198 Eric Young (eay@cryptsoft.com)
All rights reserved.

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

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

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

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

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

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

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

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

Apache license

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

TCL license

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

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

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

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

GOVERNMENT USE: If you are acquiring this software on behalf of the U.S. Government, the Government shall have only “Restricted Rights” in the software and related documentation as defined in the Federal Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you are acquiring the software on behalf of the Department of Defense, the software shall be classified as “Commercial Computer Software” and the Government shall have only “Restricted Rights” as defined in Clause 252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the authors grant the U.S. Government and others acting in its behalf permission to use and distribute the software in accordance with the terms specified in this license.

Perl License

Larry Wall's Copyright Notice Distributed with Perl. Copyright © 1989, 1990, 1991, Larry Wall. All rights reserved. This program is distributed in the hope

That it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR PARTICULAR PURPOSE.

To get the standard perl source distribution, go to http://www.cpan.org.

libwww License

This product contains software developed by libwww: W3C's implementation of HTTP can be found at: http://www.w3.org/Library/ Copyright © 1994-2000 World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National De Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. This program is distributed under the W3C's Software Intellectual Property License. This program is distributed in the hope that it will be useful, but WITHOUT WARRANTY; without even an implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See W3C License hhttp://www.w3.org/Consortium/Legal/for more details.

This product includes computer software created and made available by CERN. Copyright © 1995 CERN.

libpcap

This product contains software derived from libpcap.

Copyright (c) 1988, 1989, 1990, 1991, 1993, 1994, 1995, 1996
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that: (1) source opcode distributions retain the above copyright notice and this paragraph in its entirety, (2) distributions including binary opcode include the above copyright notice and this paragraph in its entirety in the documentation or other materials provided with the distribution, and (3) all advertising materials mentioning features or use of this software display the following acknowledgement: ``This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.'' Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

CMU-SNMP Libraries

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

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

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

Open Market Inc., Fastcgi license

This product contains software developed by Open Market Inc.

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

CGIC License

Basic License

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

Mozilla 1.xx (libcurl)

The curl and libcurl are dual-licensed under the MPL and the MIT/X-derivative licenses. This software is licensed under an MIT/X-derivative license as shown here:

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2001, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

INDEX