# Using Management Center for Cisco Security Agents 4.5.1

Revised: March 10, 2008

**Corporate Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-78-16728

# CONTENTS


**Preface** xiii

- Audience xiii
- Conventions xiv
- Obtaining Documentation xv
  - World Wide Web xv
  - Ordering Documentation xv
  - Documentation Feedback xv
- Obtaining Technical Assistance xvi
  - Cisco.com xvi
  - Technical Assistance Center xvii
- Obtaining Additional Publications and Information xviii

CHAPTER 1 **Overview** 1-1

- What Cisco Security Agent Does 1-1
  - The Lifecycle of an Attack 1-2
- How Cisco Security Agents Protect Against Attacks 1-3
- Deployment Overview 1-4
  - Network Architecture 1-5
  - Cisco Security Agent Architecture 1-6
- Preparing a Security Policy 1-9
  - Configuring Rule Modules and Policies 1-9
- Communicating over Secure Channels 1-10
- Distributing Policy Updates 1-10

Configuration Road Map 1-10

CHAPTER 2 **Management Center for Cisco Security Agents Administration 2-1**

Overview 2-1

Management Center for Cisco Security Agents Description 2-2

Browser Requirements 2-2

About Management Center for Cisco Security Agents 2-3

Accessing Management Center for Cisco Security Agents 2-4

Role-Based Administration 2-6

Administrator Preferences 2-6

Using Audit Trail 2-11

Using Management Center for Cisco Security Agents 2-12

Creating, Saving, and Deleting Data 2-26

Using the Correct Syntax 2-28

CHAPTER 3 **Configuring Groups and Managing Hosts 3-1**

Overview 3-1

Grouping Hosts Together 3-2

Mandatory Group Enrollment 3-3

Configuring Groups 3-3

Managing Agent Kits 3-7

Creating Agent Kits 3-8

Agent Registration 3-17

Scripted Agent Installs and Uninstalls 3-18

Registration Control 3-18

Modifying Agent Kits 3-19

Managing Hosts Using CSA MC 3-21

Viewing General Host Statuses with CSA MC 3-21

Viewing All Hosts Managed by CSA MC 3-21
Viewing Host Details 3-22
Searching for Hosts 3-28
Deleting Hosts 3-30
Changing Host Memberships in Groups 3-31
Distributing Software Updates 3-39
Configuring Scheduled Software Updates 3-41
Software Updates in a Distributed Configuration 3-45

CHAPTER 4 Building Policies 4-1
Overview 4-1
Developing a Security Policy 4-3
About Rules 4-6
Combining Policies 4-7
Policy Components 4-9
Rules: Action Options and Precedence 4-9
Rules: Action Definitions 4-10
Rules: Manipulating Precedence 4-13
Monitoring Access 4-14
Querying the User 4-15
Caching Responses 4-18
Building Policies and Rule Modules 4-19
Configure a Policy 4-19
Configuring Rule Modules 4-22
Setting State Conditions 4-24
System State Sets 4-25
User State Sets 4-30
Adding Rules to a Rule Module 4-32
Filtering the Rules Display 4-36

Copying Rules between Modules 4-36
Comparing Configurations 4-39
Merging or Copying Rule Modules 4-41
View Change History 4-41
Explanation of Rules 4-42
Consistency Check 4-43
Rules Common to Windows and UNIX 4-44
Agent Service Control 4-44
Agent UI Control 4-48
Application Control 4-52
Connection Rate Limit 4-56
Data Access Control 4-60
File Access Control 4-64
Network Access Control 4-69
Windows Only Rules 4-74
Clipboard Access Control 4-74
COM Component Access Control 4-76
File Version Control 4-79
Kernel Protection 4-84
NT Event Log 4-87
Registry Access Control 4-90
Service Restart 4-93
Sniffer and Protocol Detection 4-96
UNIX Only Rules 4-99
Network Interface Control 4-99
Resource Access Control 4-102
Rootkit / kernel Protection 4-104
Syslog Control 4-107
Attaching Rule Modules to Policies 4-111
Attaching Policies to Groups 4-112

Using Test Mode 4-114
Generating Rule Programs 4-118

CHAPTER 5 Using System Correlation Rules 5-1
Overview 5-1
Event Correlation and Heuristics 5-2
System API Control Rule 5-3
Network Shield Rule 5-7
Buffer Overflow Rule 5-14
Email Worm Protection Rule Module 5-18
Installation Applications Policy 5-19
Global Events 5-20
Correlation 5-21

CHAPTER 6 Using Application Classes 6-1
Overview 6-1
About Application Classes 6-2
Processes Created by Application Classes 6-2
Removing Processes from Application Classes 6-2
Shell Scripts and Application Classes 6-3
Built-in Application Classes 6-4
Built-in Configurable Application Classes 6-7
Configuring Static Application Classes 6-9
Dynamic Application Classes 6-13
Defining Dynamic Classes 6-14
Configuring Dynamic Application Classes 6-15
Configure an Application-Builder Rule 6-18
Configure a Rule Using a Dynamic Application Class 6-22
Create New Application Classes from Rule Pages 6-23

Application Class Management 6-24

CHAPTER 7 **Configuring Variables 7-1**

Overview 7-1

Where Variables are Used 7-2

Display only Show All mode Option 7-3

COM Component Sets 7-3

COM Component Extract Utility 7-6

Data Sets 7-7

File Sets 7-10

Network Address Sets 7-15

Network Services 7-18

Registry Sets 7-21

Query Settings 7-25

Localized Language Version Support 7-29

CHAPTER 8 **Event Logging and Alerts 8-1**

Overview 8-1

The Event Log 8-2

Reading Event Details 8-6

Reading Packet Details 8-6

Event Monitor 8-7

Event Log Management 8-8

How Logging Works 8-12

Verbose Logging 8-13

Logging and Query User Rules 8-13

About the Event Management Wizard 8-14

Creating an Exception Rule 8-16

Creating a Logging Exception Rule 8-22
Perform a Behavior Analysis 8-25
Event Sets 8-27
Third Party Access to Events 8-32
Configuring Alerts 8-34
Generate an Alert Log File for Third Party Applications 8-41

CHAPTER 9 **Generating Reports 9-1**
Overview 9-1
Types of Reports 9-2
Viewing Reports 9-2
Generating Reports 9-3
Events by Severity 9-3
Events by Group 9-5
Host Detail 9-6
Policy Detail 9-8
Group Detail 9-9
About the ActiveX Crystal Report Viewer 9-10

CHAPTER 10 **Using Management Center for Cisco Security Agents Utilities 10-1**
Overview 10-1
Start and Stop Server Service 10-2
Start and Stop Agent Service 10-2
Backing Up Configurations 10-3
Restoring Backup Configurations 10-6
Database Maintenance (Free Up Disk Space on CSA MC ) 10-8
Using the COM Extract Utility 10-9

Manual Agent Data Filter Installation 10-10
Exporting and Importing Configurations 10-14
View Import History 10-19
Cisco Security Agent Posture Plug-in for CTA 10-20

CHAPTER 11 **Using Cisco Security Agent Analysis** 11-1
What is Analysis 11-1
The Application Deployment Investigation Process 11-3
Reporting Categories 11-3
Turning Application Deployment Investigation On 11-4
Configure Group Settings 11-4
Configure Product Associations 11-7
Associate Unknown Applications 11-12
About Data Management 11-14
Generating Application Deployment Reports 11-16
AntiVirus Installations Report 11-17
Installed Products Report 11-20
Unprotected Hosts Report 11-23
Unprotected Products Report 11-25
Product Usage Report 11-27
Network Data Flows Report 11-30
Network Server Applications Report 11-34
Viewing Reports 11-37
Exporting Reports 11-38
What is Application Behavior Investigation 11-38
How Application Behavior Investigation Works 11-39
The Application Behavior Investigation Process 11-39
Behavior Analyses 11-40
Creating, Saving, and Cancelling Analysis Data 11-40

Configure a Behavior Analysis Investigation 11-42
Start Behavior Analysis 11-47
Importing the Rule Module 11-50
Application Behavior Reports 11-52
Report Components 11-53
Working with Reports 11-57
The Behavior Analysis Rule Module 11-58
Reviewing the Rule Module 11-59
Behavior Analysis Methodology 11-59

CHAPTER 12 **Policy Definition Guidelines** 12-1
Overview 12-1
Analyzing Applications 12-2
Configuring Policies—The Methodology 12-3
General Server Policy 12-5
Sample Web Server Policy 12-6
Combined General Server and Sample Web Server Policies 12-8

CHAPTER 13 **Third Party Product Integration** 13-1
Overview 13-1
Cisco VPN Client Support 13-2
Cisco Security Monitor Integration Support 13-2
netForensics Integration Support 13-2
Check Point™ OPSEC™ Integration 13-3
Configuration Prerequisites 13-3
Integration Configuration 13-4

APPENDIX A **Cisco Security Agent Overview** A-1

Overview A-1

Downloading and Installing A-2

Network Shim Optional A-7

The Agent User Interface A-10

Turn Agent Security Off A-22

Installing Software Updates on Agents A-23

Installing the Solaris Agent A-24

UNIX Agent csactl Utility A-27

Installing the Linux Agent A-29

APPENDIX B **System Components** B-1

Overview B-1

CSA MC Components B-2

Agent Components B-4

APPENDIX C **Open Source License Acknowledgements** C-1

OpenSSL/Open SSL Project C-1

License Issues C-1

Apache license C-4

TCL license C-6

Perl License: C-7

libpcap C-7

CMU-SNMP Libraries C-8

Open Market Inc., Fastcgi license C-8

CGIC License C-10

Mozilla 1.xx (libcurl) C-10

# Preface

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

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

## Audience

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

# Conventions

This manual uses the following conventions.

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

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

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

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

# Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

## World Wide Web

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

http://www.cisco.com

Translated documentation is available at this URL:

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

## Ordering Documentation

Cisco documentation is available in these ways:

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

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

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

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

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

## Documentation Feedback

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

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

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

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

We appreciate your comments.

# Obtaining Technical Assistance

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

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

## Cisco.com

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

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

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

http://www.cisco.com

# Technical Assistance Center

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

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

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

## Cisco TAC Web Site

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

http://www.cisco.com/tac

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

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

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

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

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

## Cisco TAC Escalation Center

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

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

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

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

# Obtaining Additional Publications and Information

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

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

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

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

  http://www.ciscopress.com

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

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

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

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

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

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

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

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


# Overview

## What Cisco Security Agent Does

Cisco Security Agents provides intrinsic, distributed security to your enterprise by deploying agents that defend against the proliferation of attacks across networks and systems. These Cisco Security Agents enforce a set of policies provided by Management Center for Cisco Security Agents and selectively applied to system nodes by the network administrator.

Operating under the direction of assigned policies, Cisco Security Agents provide strong system resource protection, tying together the auditing and control of multiple system and network resources.

This section contains the following topics.


- The Lifecycle of an Attack, page 1-2
- How Cisco Security Agents Protect Against Attacks, page 1-3
- Deployment Overview, page 1-4
- Network Architecture, page 1-5
- Cisco Security Agent Architecture, page 1-6
- Preparing a Security Policy, page 1-9
- Configuring Rule Modules and Policies, page 1-9
- Communicating over Secure Channels, page 1-10
- Distributing Policy Updates, page 1-10
- Configuration Road Map, page 1-10

# The Lifecycle of an Attack

When your network is targeted for attack, an assault is typically launched in a series of steps. Each step of an attack often depends upon the previous step being successful. Table 1-1 displays the common evolution of an attack.

*Table 1-1 Lifecycle of an Attack*

| Attack Action | Network Manifestation |
|---|---|
| Probe | • ping server IP addresses<br>• run traceroute on IP addresses<br>• sniff passwords<br>• impersonate mail users |
| Penetrate | • email attachments<br>• Java applets and ActiveX controls<br>• buffer overflows<br>• backdoors and trojans |
| Persist | • weaken security settings<br>• install new services |
| Propagate | • email<br>• Internet connections<br>• IRC<br>• FTP<br>• infected file shares |
| Paralyze | • reformat disks<br>• destroy or corrupt data<br>• drill security holes<br>• crash computers<br>• consume work cycles<br>• steal confidential data |

# How Cisco Security Agents Protect Against Attacks

The Cisco Security Agent differs from anti-virus and network firewall software in that it doesn't prevent users from accessing technologies they require. It assumes that users are going to put their systems at risk by making use of a wide range of Internet resources. Keeping this in mind, Cisco Security Agents install and work at the kernel level, controlling network actions, local file systems, and other system components, maintaining an inventory of what actions may be performed on the system itself. This way, malicious system actions are immediately detected and disabled while other actions are permitted. Both actions take place transparently, without any interruption to the user.

If an encrypted piece of malicious code finds its way onto a system via email, for example, as it attempts to unexpectedly execute or alter Cisco Security Agent-protected system resources, it is immediately neutralized and a notification is sent to the network administrator.

Cisco Security Agents use policies which network administrators configure and deploy to protect systems. These policies can allow or deny specific system actions. Cisco Security Agents must determine whether an action is allowed or denied before any system resources are accessed and acted upon.

Specifically, rule policies enable administrators to control access to system resources based on the following parameters:

- What resource is being accessed.
- What operation is being invoked.
- Which application is invoking the action.

The resources in question may be either system resources or network resources such as mail servers.

When any system actions that are controlled by specific rules are attempted and allowed or denied accordingly, a system event is logged and sent to the administrator in the form of a configurable notification such as email, pager, or custom script.

# Deployment Overview

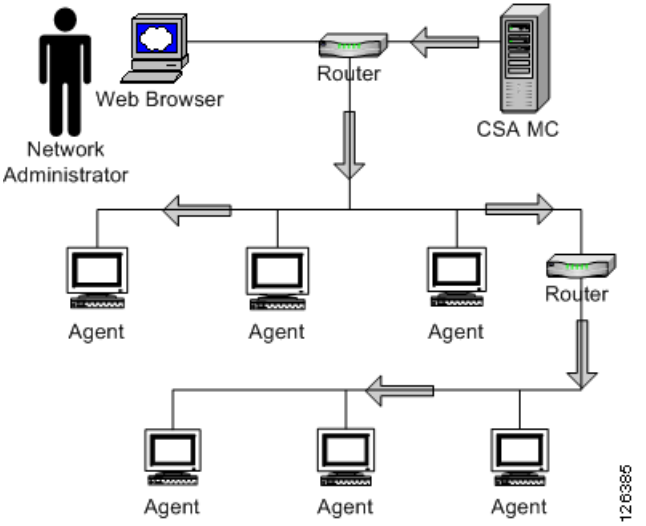
Management Center for Cisco Security Agents contains two components:

- CSA MC—installs on designated Windows 2000 systems and includes a configuration database server and a web-based user interface.
- Cisco Security Agent (the agent)—installs on server and desktop systems across your enterprise network.

Using CSA MC, you assemble your network machines into specified groups and then attach security policies to those groups. All configuration is done through the web-based user interface and then deployed to the agents.

The network example shown in Figure 1-1 illustrates a basic deployment scenario. CSA MC software is installed on a system which maintains all policy and host groups. The administration user interface is accessed securely using SSL (Secure Sockets Layer) from any machine on the network that can connect to the server and run a web browser. Use the web-based interface to deploy your policies from CSA MC to agents across your network.

***Figure 1-1 Policy Deployment***



# Network Architecture

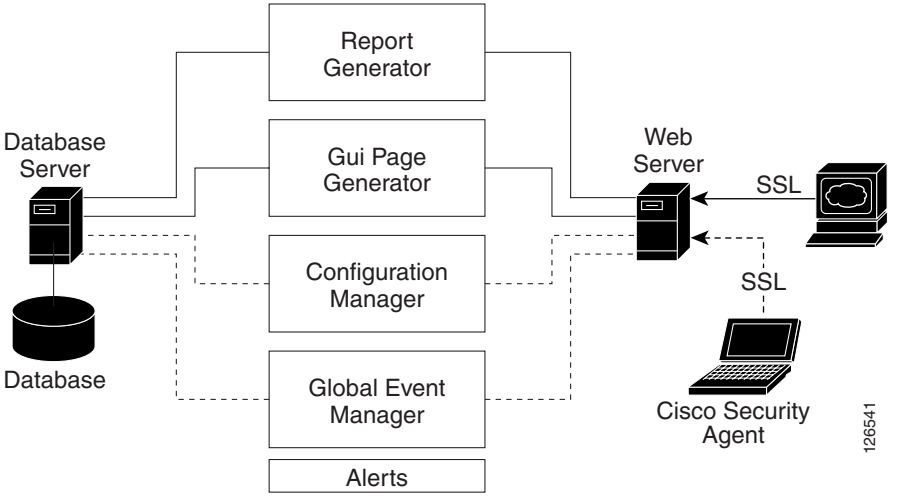
The CSA MC architecture model consists of a central management center which maintains a database of policies and system nodes, all of which have Cisco Security Agent software installed on their desktops and servers.

Agents register with CSA MC. CSA MC checks its configuration database for a record of the system. When the system is found and authenticated, CSA MC deploys a configured policy for that particular system or grouping of systems.

The Cisco Security Agent software now continually monitors local system activity and polls to the CSA MC at configurable intervals for policy updates. It also sends triggered event alerts to the CSA MC's global event manager. The global event manager examines system event logs and, based on that examination, may trigger an alert notification to the administrator or cause the agent to take a particular action.

**Note** See Appendix B, "System Components" for detailed information on product architecture.

*Figure 1-2 CSA MC Architecture*




# Cisco Security Agent Architecture

The Cisco Security Agent software installs locally on each system node and intercepts operations of that system. A network application interceptor sits at the application level and intercepts all application operations. Other Cisco Security Agent mechanisms intercept network traffic, file actions, and system registry actions while the rule/event correlation engine controls all agent mechanisms watching for any events that trigger an agent policy. See Figure 1-3.

*Figure 1-3 Cisco Security Agent Software Architecture (Windows)*

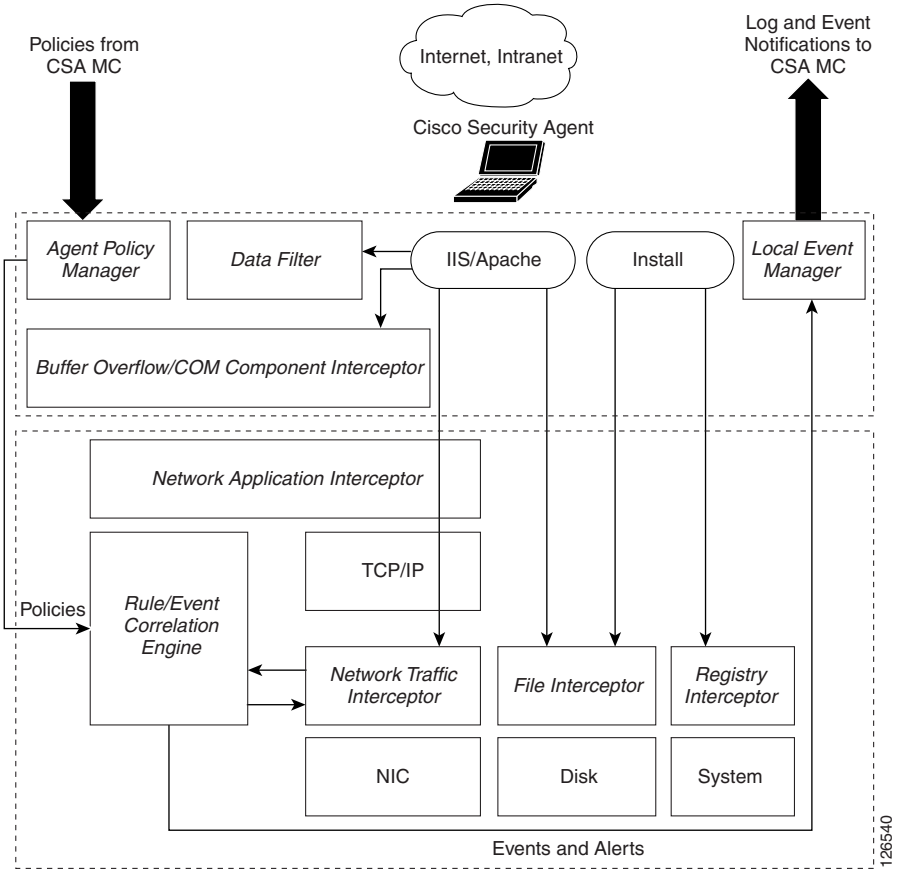
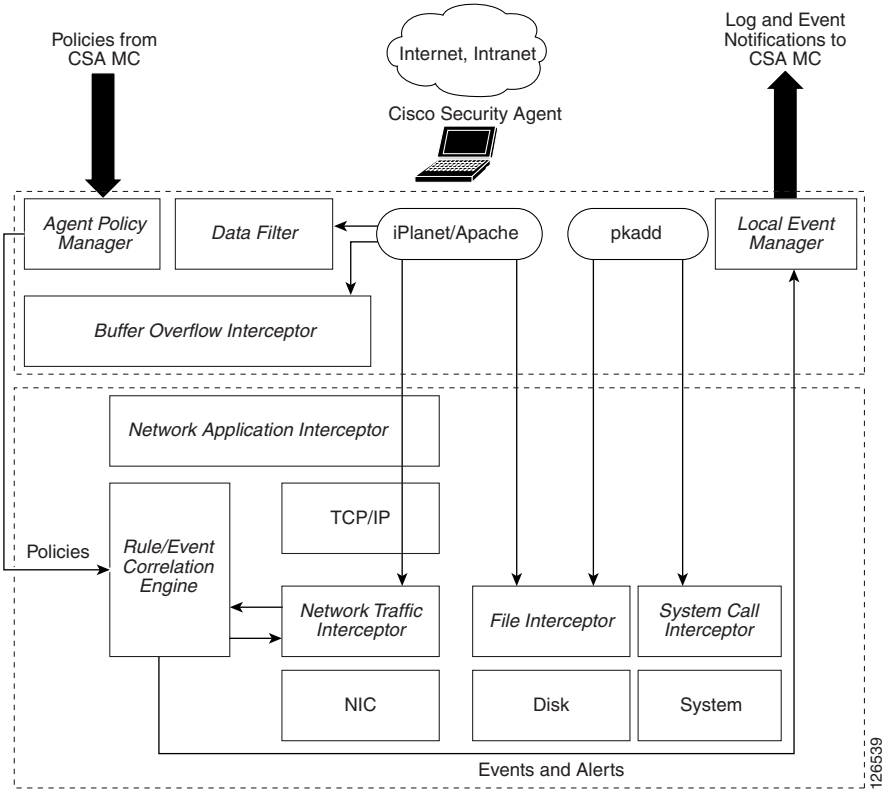


*Figure 1-4 Cisco Security Agent Software Architecture (UNIX)*



# Preparing a Security Policy

You should have a carefully planned corporate security policy in place before you attempt to configure Management Center for Cisco Security Agents. You must understand exactly what network resources and services you want to protect in order to adequately scale a set of policies that safeguard those valuable organizational resources. A corporate security policy should allow the user community to easily access required resources, while protecting that community from the dangers those open resources can represent.

To help achieve this goal, CSA MC ships with a variety of rule templates and pre-configured security modules and policies. The policies you configure and deploy become the foundation of your security policy.

## Configuring Rule Modules and Policies

A policy is a collection of rule modules. A rule module is a collection of rules. The rule module acts as the container for these rules while the policy serves as the unit of attachment to groups. Machines with similar security needs are grouped together and assigned one or more policies that specifically target the needs of the group.

When you are creating rules for your rule modules, targeting the needs of machine groupings is central to your overall security plan. You can base these security needs on various criteria. For example, the concerns you have for your web servers may require you to group them separately from your mail servers based on the types of policies each set of servers require. Therefore, you could place your web servers into a common group, create rules that protect those servers from having their cgi files and html files written to (for example), and then attach the policy that contains these rules to the web servers group.

When first configuring and deploying policies, you should put them into Test Mode (from the Group or Rule Module pages). In Test Mode, the policies are not "live." The Cisco Security Agent will not deny any action or operation even if an associated policy says it should be denied. Instead, the agent will permit the action but log an event when a deny or query rule is triggered and when an allow rule with logging enabled is triggered. This helps you to understand the impact of deploying a policy on a host before enforcing it.

# Communicating over Secure Channels

All communications between the Management Center for Cisco Security Agents server system and systems accessing the browser-based user interface are protected using SSL (Secure Sockets Layer). Administrator authentication is also provided via the required entry of a username and password to authenticate and initiate each management session. Additionally, communications between the management server and the agents are passed over SSL.

See the Installation Guide for information on importing certificates and connecting securely over SSL.

# Distributing Policy Updates

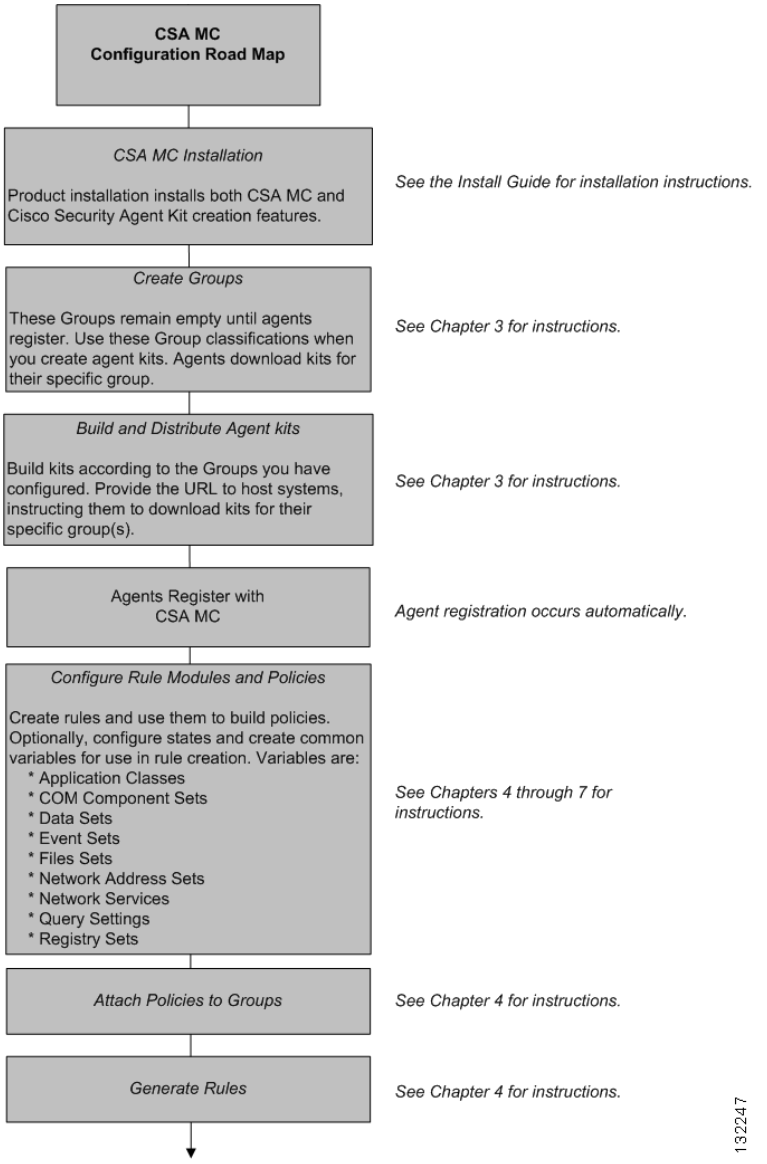
At configurable time intervals, Cisco Security Agents on the network poll in to CSA MC to check for updated rule sets. See Chapter 3, "Configuring Groups and Managing Hosts" for details.

When a rule is triggered on a system, the agent sends its event notifications to CSA MC. CSA MC identifies the agent, examines the event notifications presented by the agent and correlates this information.

# Configuration Road Map

There are several elements you must configure to create policies that are distributed to the agents. First, you must configure host groups and create Cisco Security Agent kits. After the agents are installed on systems throughout your network, they register with CSA MC. Then, they are automatically placed into their assigned groups. When you generate rules, agents receive the policies intended for them. Refer to the following CSA MC configuration roadmap in Figure 1-5.

*Figure 1-5 CSA MC Configuration Road Map*




# Management Center for Cisco Security Agents Administration

## Overview

Management Center for Cisco Security Agents supports editing of the database by multiple administrators. Administrators must identify themselves and authenticate to CiscoWorks before they can access any CSA MC configuration data.

CSA MC's web-based user interface provides secure access to the database from anywhere on the network. All changes to the database are logged. The logged information includes a summary description of the modification, the time the changes were made, and the identity of the administrator who made the changes.

This section contains the following topics.


- Management Center for Cisco Security Agents Description, page 2-2
- Browser Requirements, page 2-2
- About Management Center for Cisco Security Agents, page 2-3
- Accessing Management Center for Cisco Security Agents, page 2-4
- Administrator Preferences, page 2-6
- Role-Based Administration, page 2-6
- Using Audit Trail, page 2-11
- Using Management Center for Cisco Security Agents, page 2-12
- Creating, Saving, and Deleting Data, page 2-26

- Using the Correct Syntax, page 2-28

# Management Center for Cisco Security Agents Description

The Management Center for Cisco Security Agents (CSA MC) is a web-based user interface which can be accessed from the CiscoWorks user interface on any machine connected to the Internet and running a web browser. Through CSA MC, administrators configure all aspects of Management Center for Cisco Security Agents.

## Browser Requirements

The browser you use to access CSA MC through CiscoWorks must meet the following requirements.

Internet Explorer:

- Version 6.0 or later
- You must have cookies enabled. This means using a maximum setting of "medium" as your Internet security setting. Locate this feature from the following menu, Tools>Internet Options. Click the Security tab.
- JavaScript must be enabled.

Netscape:

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

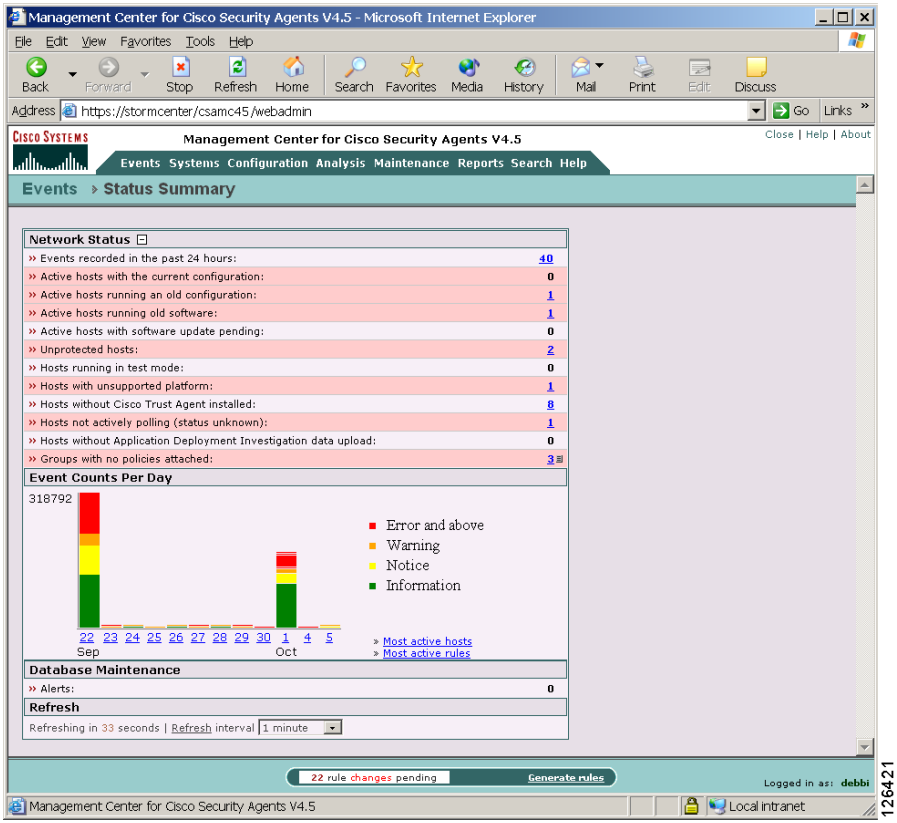
**Note** SSL must be enabled on the CiscoWorks user interface to access CSA MC. Enable SSL in CiscoWorks from the Server Configuration drawer. Select **Administration>Security Management>Enable/Disable SSL**. Click **Enable** in the right pane. You may have to restart both the CiscoWorks and CSA MC services for this change to take effect.

# About Management Center for Cisco Security Agents

All Cisco Security Agent policies are configured and deployed through the CSA MC web-based user interface. CSA MC also provides a reporting tool, letting you generate reports with varying views of your network enterprise health and status. Providing an HTML web-based user interface enables an administrator to access CSA MC from any machine connected to the Internet and running a web browser.

CSA MC provides a menu bar for easy navigation among the configurable administrator task items. Configurable items are displayed in drop-down menus that appear when you move the mouse over a category in the menu bar. When you select an item, the properties and status for that item are displayed.

*Figure 2-1 CSA MC Status View*




# Accessing Management Center for Cisco Security Agents

You access CSA MC from the CiscoWorks user interface. An initial administrator account was created as part of the CiscoWorks installation process. After that administrator account is entered to log in to CiscoWorks, you do not need to log in to CSA MC again.

- To access CSA MC locally select **Start > Programs > CiscoWorks > CiscoWorks**. Log in to 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 user interface, the **Security Agents V4.5** item is located in the **VPN/Security Management Solution** drawer. Expand the **Management Center** or the **Administration>Management Center** folder. (If you have upgraded from version 4.0.x, you may see both a **Security Agent V4.5** and a **Security Agents** item here.)

**Note** To launch CSA MC from CiscoWorks, the CiscoWorks user interface must have SSL enabled. Refer to *Installing Management Center for Cisco Security Agents 4.5* for detailed information.

# Role-Based Administration

CSA MC can have multiple administrators, all with secure access to configuration data. 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 CiscoWorks 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 CiscoWorks 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 CiscoWorks roles listed in the first two bullets enabled, this provides administrators with read access to the entire CSA MC database. Administrators with Monitor privileges can also create reports, alerts, and event sets.

**Caution** To restrict administrator privileges, the administrator(s) in question must first register with CSA MC. This registration occurs the first time the administrator logs in to CSA MC.

**Note** To view or edit your CiscoWorks administrator profile, in the CiscoWorks user interface, select **Server Configuration>Setup>Security>Modify My Profile.**

# Administrator Preferences

In addition to the role-based administration created through CiscoWorks, you can set CSA MC-specific administrator preferences. As a CSA MC administrator, you can select to view configuration items for all operating systems or to view only those for a particular operating system. If you leave the default of "All" configuration items at the top of item list pages, you must then select an operating

system when you configure items such as policies, groups, and agent kits. If you are only configuring or deploying policies to UNIX systems, it is likely that you will only want to see those items. The same holds true if you are deploying policies to only Windows systems.

By selecting Maintenance>Admin Preferences in CSA MC, you can set global administrator preferences (see Figure 2-3). This way, you do not have to choose an operating system, for example, on each configuration page. Using Admin Preferences, you can configure preferences for each administrator registered with CSA MC.

Additional global administrator preferences are:

- **Remember last page visited**—Select this check box to have the management center display the last page you visited during your last session when you next log in. (This can be useful if the management center times out due to inactivity during a session.)
- **Always use Show All mode** If you have hidden configuration items **by selecting** the Display only in Show All mode check box for variables and application classes, selecting this check box for your admin preference causes all hidden items to appear in list pages and selection boxes. When you select the "Display only in Show All mode" check box for a configuration item, the only way to have the item reappear is to select the Always use Show All mode check box for your admin preference and then all hidden items will also appear. Note that you can click "Show All" in rule pages to temporarily display hidden items for that rule page.

**Note** The Display only in Show All mode feature in configuration pages makes configuring CSA MC policies easier by paring down configuration items to only those you use most. CSA MC ships with pre-configured administrator preferences you can use to turn various features on and off depending upon when you prefer a basic or advanced view of the product. See Pre-Configured Admin Preferences, page 2-9, for details.

- **Always show expanded configuration views** To simplify product configuration, several management center pages, especially rule pages, contain fields that are not automatically displayed. In place of these fields is a + symbol signifying that the field is present and can be configured by clicking on the + symbol to expand it. If the field in question has a configuration setting (either an explicit setting or a default setting such as

<none> or <all>) the configured setting is displayed textually beside the plus sign. The fields that are not expanded by default are considered fields that are used less often and are not shown in order to streamline the page and the configuration tasks.

Once a field is expanded manually on a page, you cannot collapse it again until you refresh the page. To always display all fields on all pages, select the **Always show expanded configuration views** check box as an Admin Preference.

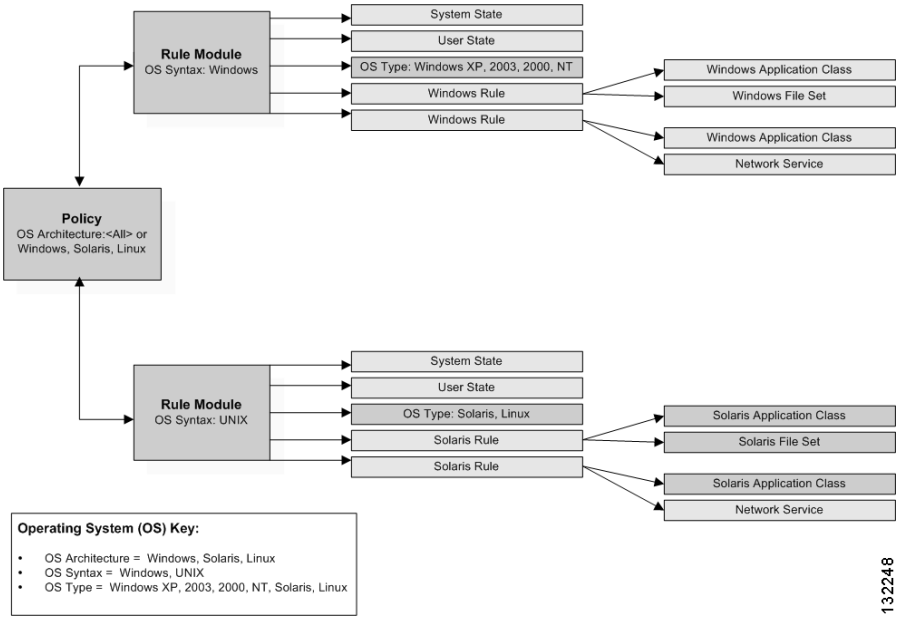
Once you have configured administrator preferences, you must select one or more administrators to which these preferences are assigned in the **Apply these preferences to the following selected administrators** selection box. To apply different sets of preferences to different administrators, you must configure several Admin Preferences and assign them appropriately.

Operating system designation requirements and their granularity vary for different configuration items. Refer to the following chart and diagram for an overview of how and where operating systems designations are made.

***Table 2-1 Operating System Naming Conventions***

| OS Naming Conventions | Available OS Options |
|---|---|
| OS Architecture | Windows, Solaris, Linux |
| OS Syntax | Windows, UNIX |
| OS Type | Windows All, Windows XP, Windows 2003, Windows 2000, Windows NT, UNIX All, Linux, Solaris |

*Figure 2-2 Example: Operating System Specifications*



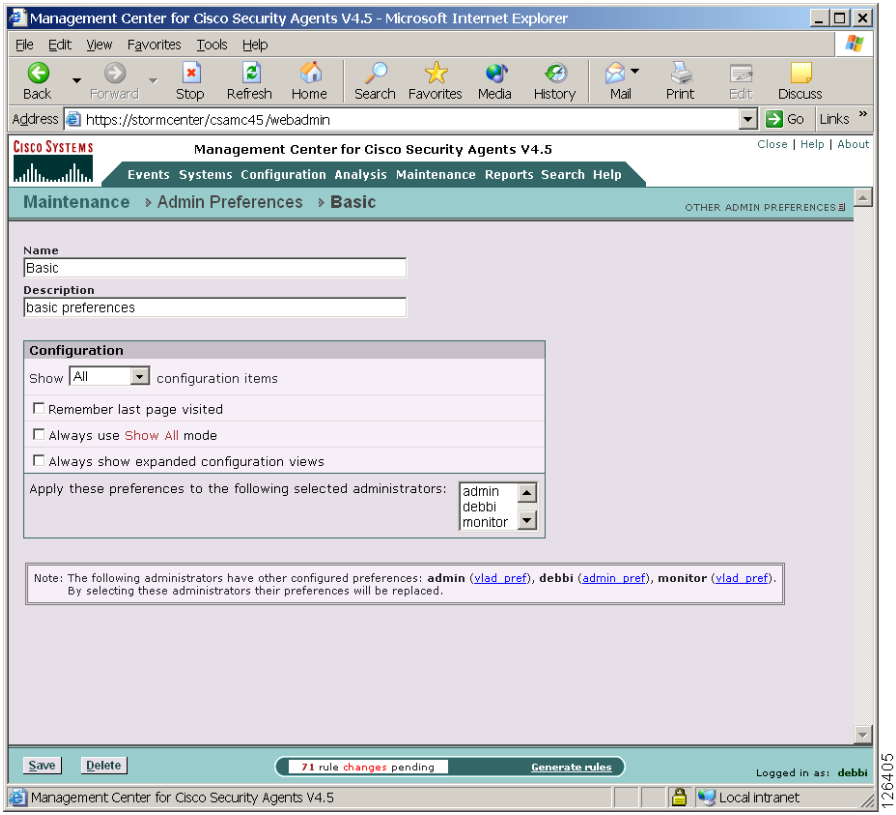

## Pre-Configured Admin Preferences

CSA MC ships with several pre-configured administrator preferences that you can choose if the default preferences do not meet your needs. By default, the administrator created automatically by the CiscoWorks installation is also the "Basic Administrator" preference included here. See Figure 2-3. The preferences shipped with CSA MC are as follows:

- Basic Administrator—Causes all UNIX and Windows items that are not marked as hidden to be displayed. Items that are marked "Display only in Show All mode" are not displayed and less frequently used configuration fields are collapsed. This is the implicit (not selected) preference assigned to the administrator created by the CiscoWorks installation. If you select a preference in the Admin Preferences window, to return to the implicit preference, you can either deselect all other preferences or select the Basic Administrator preference.

- Basic UNIX Administrator—Causes all unhidden UNIX items to be displayed. Items that are marked “Display only in Show All mode” are not displayed and less frequently used configuration fields are collapsed.
- Basic Windows Administrator—Causes all unhidden Windows items to be displayed. Items that are marked “Display only in Show All mode” are not displayed and less frequently used configuration fields are collapsed.
- Advanced Administrator—Causes all items to be displayed. All configuration fields are expanded.
- <Admin Access Control>—Administrators with configure privileges can use this global built-in preference to restrict administrators with monitor privileges from viewing specified groups by using the **Define Group Restrictions** feature. By clicking the <Admin Access Control> link and then selecting administrators and selecting groups, you are indicating that the selected administrators can only view items pertaining to the groups they are allowed to view. If an administrator is not permitted access to a group, that administrator cannot view any items related to the group, including events, policies, and application classes (unless those configuration items are also used by groups they are allowed to see.) You can configure several access control settings from this page.

*Figure 2-3 Administrator Preferences*




# Using Audit Trail

Accessible from the Reports drop-down list in the menu bar, the Audit Trail page displays a list of changes administrators have made to the CSA MC database. These changes are displayed according to the following information:

- The change itself.
- The type of change (configuration category: policies, file sets, groups, and so on).
- The date and time the change was made.

- The administrator who made the change.

Click the **Change Filter** link to edit the audit trail viewing parameters according to the following:

- Start date (enter date parameters using the same formats as in the Event Log).
- End date.
- The administrator who made the changes.
- The change type (configuration category: policies, file sets, groups, and so on).
- The number of changes to display per viewing page.

# Using Management Center for Cisco Security Agents

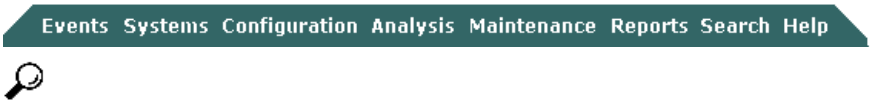
The sections in this chapter describe the various components you should understand in order to configure Cisco Security Agents using CSA MC.

## Menu Bar

The menu bar at the top of CSA MC provides links to all configuration pages and list views. Arrows indicate that there are subcategories for which you can choose from those top-level main items (see Figure 2-4). These subcategories appear when you move the mouse over the main item itself.

When you select an item from the menu bar, the list view page for that item appears.

*Figure 2-4 Menu Bar*

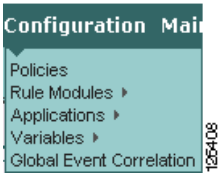



The configuration options available from each menu bar item are as follows.

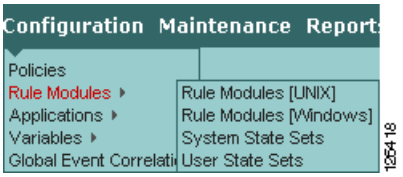
**Events**—The Events drop-down list provide tools for viewing and managing system status and log files. You can also set alerts and alert parameters from here. (See Chapter 8, "Event Logging and Alerts".)


**Systems**—The items available from the Systems drop-down list let you configure the groups which agent host systems are placed into when they register with CSA MC. You can also deploy new agent kits and software updates for agents from this menu option. (See Chapter 3, "Configuring Groups and Managing Hosts".)

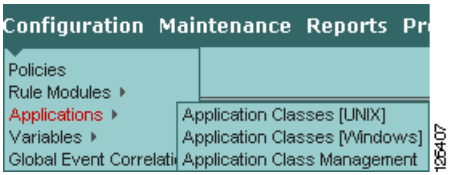
**Configuration**—The items available from the Configuration drop-down list provide you with the pages you will need to configure your policies for agents. This list provides links to the rule pages you use to develop your policies, as well as links to application classes and variables. (See Chapter 4, "Building Policies")



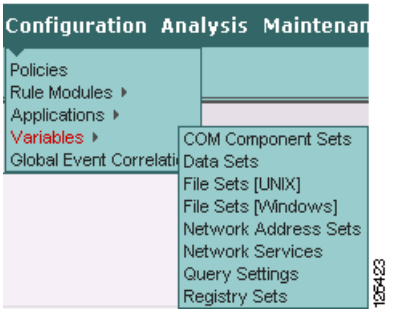
**Configuration>Rule modules**—System state sets and User state sets are accessible from the cascading Rule Modules menu that appears when you move your mouse over that item in the Configuration drop-down list. (See Chapter 4, "Building Policies")




**Configuration>Applications** are accessible from the cascading menu that appears when you move your mouse over the Applications item in the Configuration drop-down list. (See Chapter 6, "Using Application Classes")




**Configuration>Variables**, such as file sets and network addresses, which are the building blocks for policies, are accessible from the cascading menu that appears when you move your mouse over the Variables item in the Configuration drop-down list. (See Chapter 7, "Configuring Variables".)




**Analysis**—The items in the Analysis menu are for diagnostic and investigative purposes, separate from general CSA MC configuration. Use these menu options to analyze application behavior and to investigate all resources being used across

your enterprise with the purpose of securing these applications and resources using CSA MC Policies. (See Chapter 11, "Using Cisco Security Agent Analysis")


**Maintenance**—The items available from the Maintenance drop-down list let you import and/or export configuration files, backup your database configuration and enter your license key. When you move your mouse over the Export/Import item, you can select further options from the cascading menu that appears. (See Administrator Preferences, page 2-6, available from this menu item, as well.)


**Reports**—The items available from the Reports drop-down list let you generate reports by various categories such as event severity level, by the group(s) that generated the event and by individual host systems. (See Chapter 9, "Generating Reports".)

**Search**—Use the selections available from the Search drop-down list to search for a specific configuration item in the CSA MC database. You can limit your search to Hosts, Groups, Policies, Rules, Rule Modules, Variables, Application Classes, or All. Each option has its own criteria by which you can search.


## Using Search

Once you select a category to search on from the Search drop-down list, enter all or part of the name of the item for which you are searching in the Find field. (See Figure 2-5.)

To further control your search, select one or more of the following check boxes.

- Show references—Select this check box to also display configuration items which reference the name being searched for. Clicking on the referenced item in the right column lets you access the configuration(s) using the string value.
- Search on description—Select this check box to search for the string value in Description fields.
- Search all fields—Select this checkbox to search all database fields (including Description fields) for the string value.

You can limit Results per page by entering a value in the corresponding field. (25 is the default). Click the **Find** button. Results are displayed as links. Click the item link to go to its configuration view.

**Note** The search page does not search the event database.

(Use the Delete button to remove found items from the database. Once an item is deleted here, it cannot be recovered.)

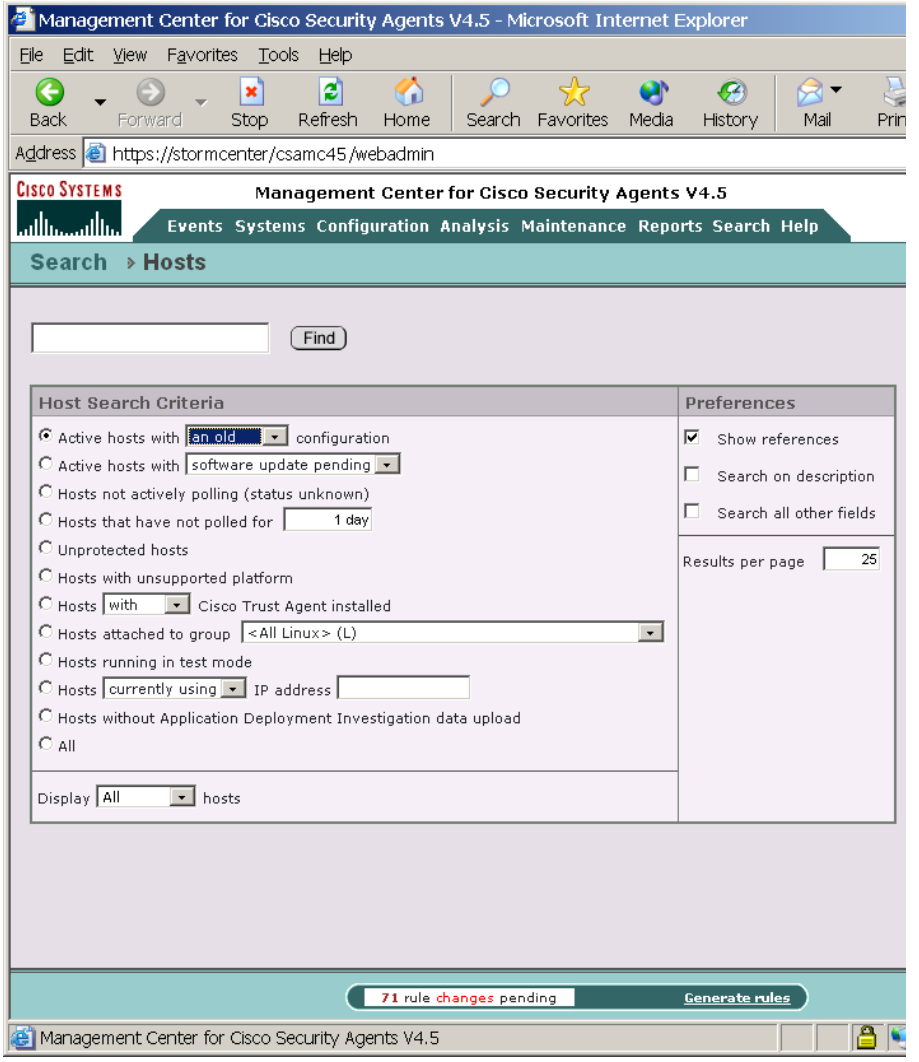
- Replace—From the Search menu, Policies, Variables, and Application Classes allow you to perform a search and replace on items. Once you've selected a category from the Search menu, you can click the Replace link to access a pop-up box. In that box, you select references to an item and replace it where it appears with another item that you select. For example, you may want to replace all references to a certain variable across the system. Selecting the Preview checkbox allows you to see where all references will be replaced before you actually do the replacement.

The Hosts search page lets you search for hosts based on several criteria. For example, you can search for hosts that are not actively polling or that are unprotected. Unprotected hosts are not members of any group or are members of a group that has no policies

You can also search for hosts according to those with "old rule sets", "the latest rule set", "old (outdated) software", "those with pending software updates", "hosts not actively polling" see Not active hosts for details on this item, "hosts that have not polled in for a specified time".

See Viewing Host Details, page 3-22 for more information on Hosts.

*Figure 2-5 Search Feature*



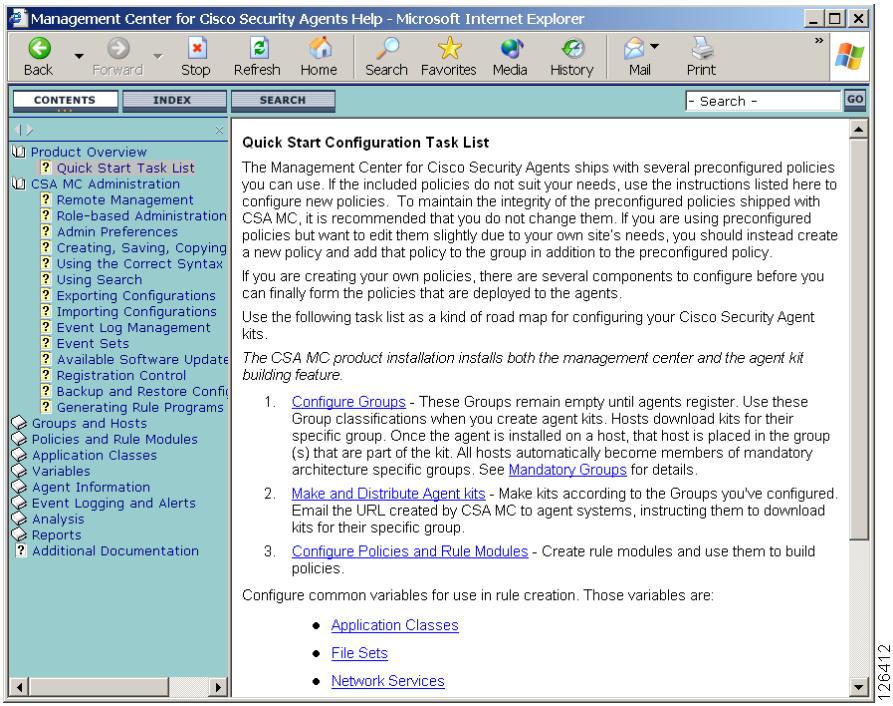

## Using Help

**Help**—In addition to this configuration guide, CSA MC provides online help. When you click Help on the far right of the menu bar, you can select Online Help

or you can click a link for the Technical Support web site. When you select Online help, a new browser window opens. This window contains help information on the configuration item from which you have accessed the help. To view help on other topics, click the corresponding topic link in the Contents frame of the help window.


**Note** You can also access Quick Help for fields that have question marks beside them. Quick Help provides information for specific text fields.

*Figure 2-6 Main Help System*

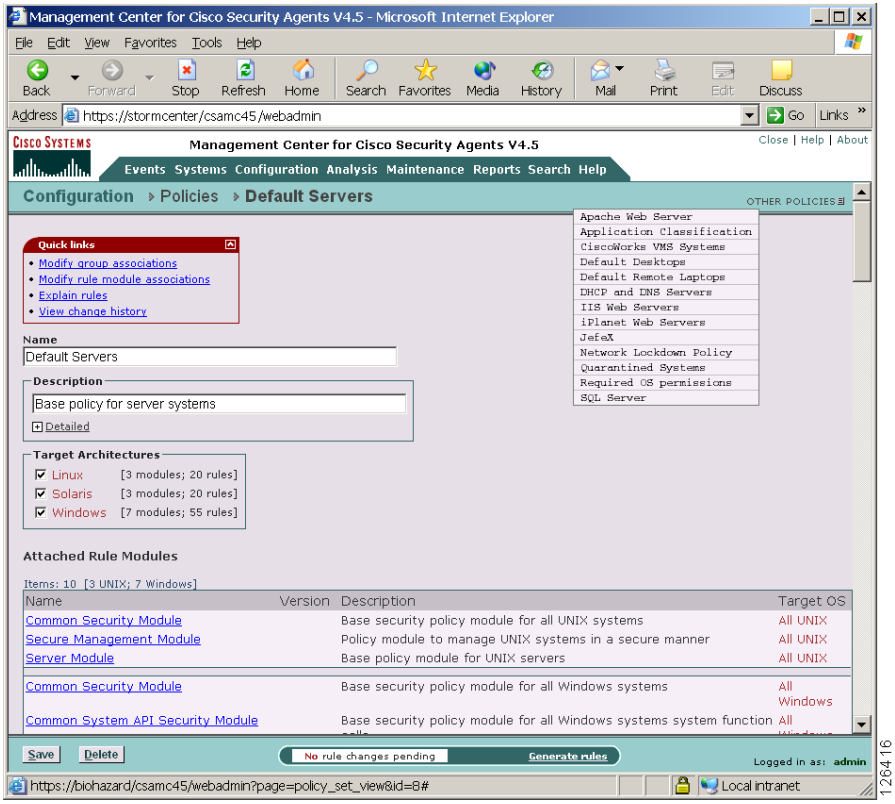



## Shortcuts and Hints

**Other <configuration item>**—In configuration views, an Other [Policies, Applications, Files Sets, etc] link appears on the right side of the user interface below the menu bar. Click this link to view a drop-down list containing the names of other configurations within the category you are currently working (see Figure 2-7). Click one of these names to view the configuration page for that item.

**Note** If you jump to another configuration page without saving the page you are working in, the information on the current page is lost.

*Figure 2-7 Other Policies Link*




## Summary Pages

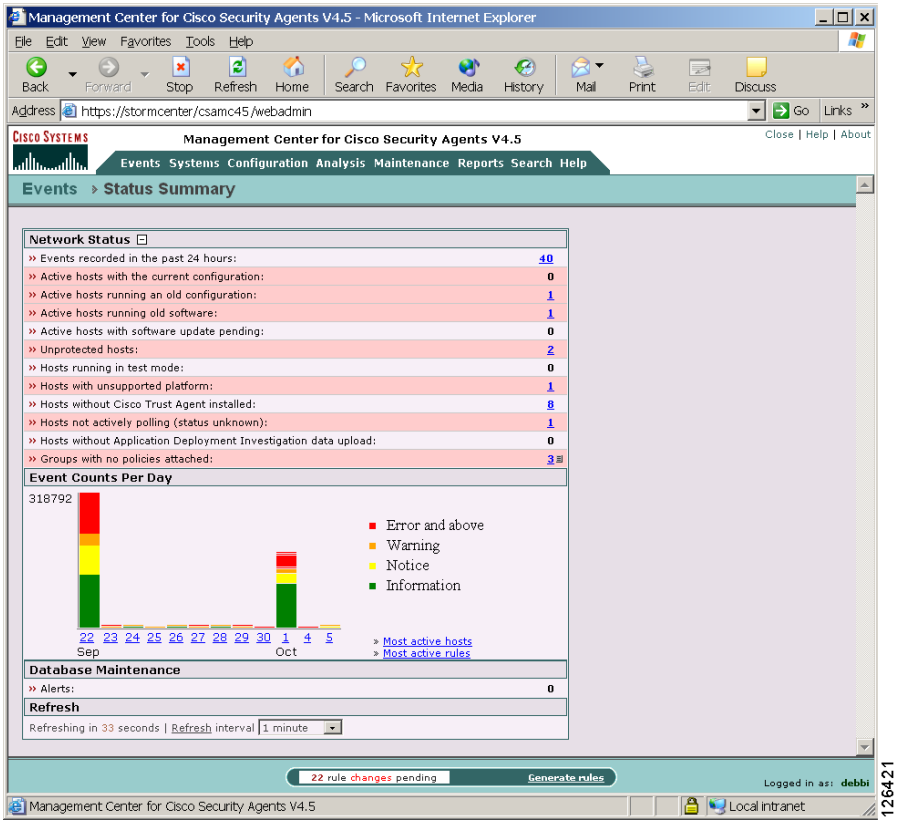
**Status Summary**—When you first login, the **Status Summary** view appears (see Figure 2-8). This page supplies overall system summary information including recorded events and agent rule versions. You can access this page at any time by selecting it from the Events category in the menu bar. A colored graph displays the event log according to severity level. Click on a color in the graph to view logged events of that severity level.

By default, items in the **Network Status** category do not appear in the list if their number is 0. Expand the Network Status view to see all items. Refer to Chapter 8, "Event Logging and Alerts" for detailed information on the Status Summary view and event logging features.

Use the **Most active rules** and **Most active hosts** links to open a new window which displays the rules that have triggered the most (logged the most events to the MC) and the hosts that have been most active. You can sort these lists by event or by hosts triggering events. This is useful to help you tune your policies for rules that are being tripped too often. This can also alert you to common unwanted occurrences that may be triggering across your enterprise. Additionally, you can purge the events that appear in these lists.

**Note** If there is an alert present in the **Database Maintenance** category, we recommend that you access the Database Maintenance page from **Maintenance** in the menu bar and shrink the database. See Database Maintenance (Free Up Disk Space on CSA MC ), page 10-8 for details.

*Figure 2-8 Status Summary View*




## CSA MC Views and Navigation

**List View**—Each CSA MC configuration category has a top level list view. This list view displays a list of links, each of which represent a configured item for that category. It is from this list view that you create configurations and delete existing configurations. Buttons for New, Clone and Delete actions are present on list view pages. From the list view, you click an item link to access the configuration page for that item.

**Configuration View**—Access the configuration view for an item by clicking on that item in the list view. Configuration views may contain edit fields, radio buttons, checkboxes, and/or listboxes depending on the configuration

requirements. Enter the necessary information and click **Save** to store data in the CSA MC database. Configuration views contain Save and Delete buttons. See Creating, Saving, and Deleting Data, page 2-26 for further details.

**Navigation Tools**—The heading link (below the menu bar, see Figure 2-9) contains hierarchal links for the item you're configuring. Use these header links to switch between top level list views and subcategory configuration views. For example, in Figure 2-9, the header bar contains links to the top level Policies list view and the MS IIS Server policy. Note that leaving a configuration view without clicking the Save button causes any newly entered data to be lost.

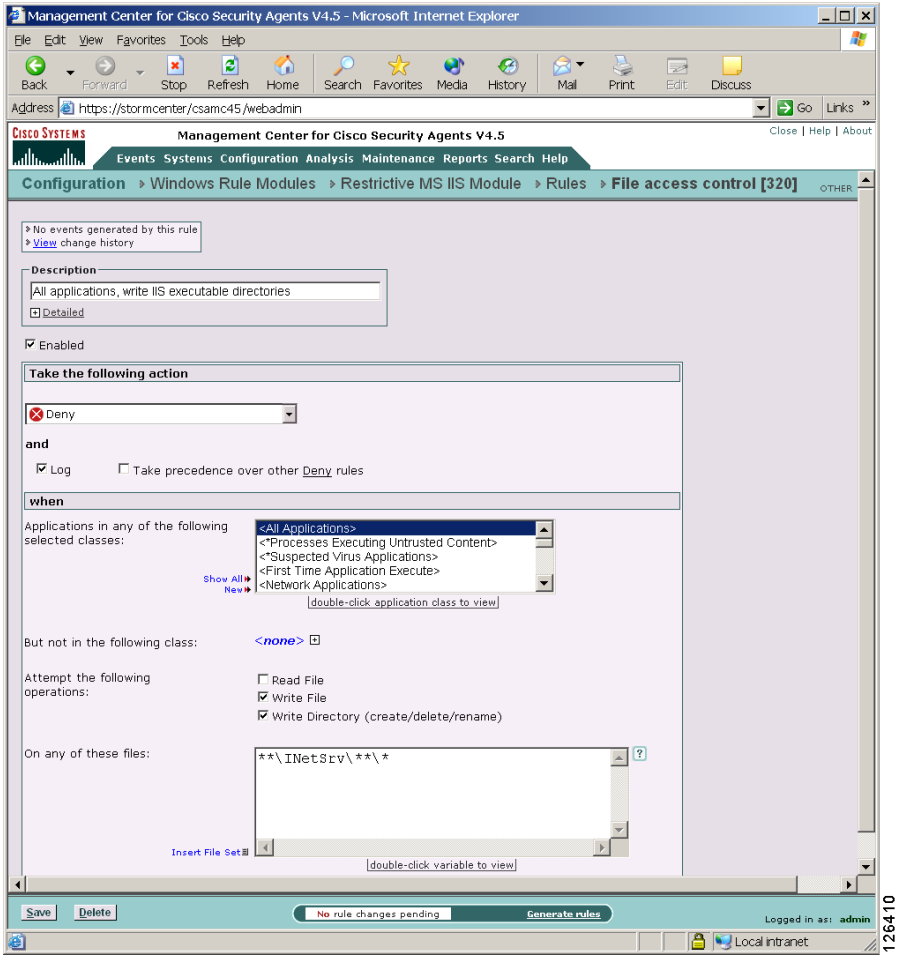
**Show reference list**—Configuration items that are used in other configurations have a "Show reference list" link on their pages. Clicking this link displays all the configurations where the current item is used. This display also links to the items that are shown.

**Note** You can click the gray arrow on the right side of the Policy list page to go directly to the rules contained in the policy.

**Configuration Shortcuts**—Rule pages allow you to insert pre-configured variables such as file sets and COM components into your rules. If there is no pre-configured variable that you wish to use and you want to create a new one, you can do it without leaving the rule page. When you click the Insert link beside any edit box in the rule page, there is a New item in the list that appears first. Selecting the "New" item pops up a configuration page for that variable type. You can then configure a new variable and use it in the rule without having to leave the rule page to access the variable page. You can double-click on an existing item to view its configuration page.

Application classes also have a shortcut you can use to create a new item. Clicking the New link beside the list of application classes in each rule configuration page lets you create a new application for your rule.

*Figure 2-9 Configuration View*



# Creating, Saving, and Deleting Data

## CSA MC Button Frame

All CSA MC action items appear in a frame at the bottom of CSA MC. The buttons in this frame change in accordance with the actions available for the page you're viewing. Available CSA MC buttons and links are as follows.

**Generate rules (pending changes)**—When you are ready to deploy your configuration (policies, rules, variables, etc.) to Cisco Security Agent systems, you must click this link in the bottom frame to view all pending database changes and then to generate them. (See Chapter 4, "Building Policies".)

**New**—Use the New button to create a new configuration item within the list view you have selected. Click the New button and a new item appears in the list view. Click the new item link to access the configuration view for that item.

**Clone**—Use the Clone button in conjunction with the checkboxes beside each list view item. To clone a particular configuration, select its checkbox and click the Clone button. You can clone one item at a time. New links to the cloned configurations appear in the list view.

**Note** In most list view pages in CSA MC, there are New, Clone, and Delete buttons (Clone is not present in all list views as you can only clone certain configurations)

**Note** When you clone an item, such as a policy, that contains variable items like file sets or network services, the cloned rule uses the same variables used in the original rule. The variables themselves are not cloned.

**Delete**—Use the Delete button in conjunction with the checkboxes beside each list view item. To delete a configuration, select its checkbox (you can select several at once) and click the Delete button. All checked items are deleted. To quickly select all checkboxes, click the very top checkbox in the list view heading bar. Clicking the Delete button then deletes all items.

**Save**—When you enter configuration information, whether you are entering new data or editing existing data, you must click the Save button once you are finished to save your configuration in the CSA MC database. If you do not click Save before moving to another page in CSA MC, your data is lost.

**Note** Although your information is stored in the database when you click Save, it is not distributed to the agents across your network until you generate rules. See Generating Rule Programs, page 4-118 for further information.

**Compare**—Groups, Policies, Rule Modules, Variables, and Application Classes provide a Compare button in their item list views. When you select the checkbox next to 2 items (you cannot compare more than 2 configurations at a time) and click the Compare button, CSA MC displays the configurations side by side and highlights the differences in red. Once you've examined how the configurations compare, you can select to merge them.

**Note** The purpose of this compare tool is to assist you after you've imported configurations or upgraded CSA MC. These processes can cause you to have duplicate or very similar configuration items. Comparing and merging configurations can help you to more easily consolidate duplicate items. See Chapter 4, "Building Policies" for details on using Compare to merge configurations.

**Note** Right-clicking your mouse on a CSA MC page displays a shortcut menu for performing the tasks provided by buttons on that page and for additional configuration tasks not as easily accessible from the current page you're viewing.

# Using the Correct Syntax

CSA MC contains text fields that require you to enter information using a specific syntax. Most of the text fields in these pages are similar and require similar syntax. The text fields are categorized and listed below with the required syntax.

When using configuration variables in rules, application classes, and alerts you must enter the variable name preceded by a dollar sign. The insert links beside each text field automatically insert variables using the correct syntax.

For example, if you have a file set variable named Web Browsers, clicking the Insert File Set link lets you select Web Browsers. It then places $Web Browsers in the corresponding field using the correct syntax. The dollar sign tells CSA MC that this is a variable value.

When entering a Name for any item you configure, use the following syntax:

Names of items must be unique per operating system. Items may only have the same name if they have different operating system designations. (Host names, however, do not have to be unique.) All names are case insensitive, must start with an alphabetic character, can be up to 64 characters long and can include alphanumeric characters, spaces, hyphens - and underscores _ . (Note one exception, agent kits do not accept spaces in names.)

### File entry text boxes require:

In a list of items, each item must appear on a single line. Do not specify multiple items on a single line.

Leading and trailing spaces are removed from each line. Other spaces, such as the one located in "Program Files" are recognized. To indicate leading or trailing spaces you must use special characters. The following special characters are recognized. (Note that the need to use the characters listed below should occur very rarely.)

`'b` Leading/Trailing Space

`'t` Tab

`'n` Line feed

`'r` Carriage return

**Note** If you want to use a single quote(') in a file name, you must enter two single quotes ('') for CSA MC to recognize the syntax correctly. Two single quotes are seen as one quote.

Local system files are entered using full path and disk drive.

Windows:

```
c:\Program Files\Outlook\msimn.exe
c:\winnt\regedit.exe
```

You can also use **@fixed** to indicate all local system drives without having to indicate the drive letters.

For example, `@fixed:\Program Files\Outlook\msimn.exe`

UNIX:

```
/etc/passwd
```

Local system files are entered using full path and disk drive (Windows) with optional wildcard notations.

Windows

```
c:\Program Files\Outlook\*.exe
```

UNIX

```
/usr/bin/*
```

**Note** Windows peripherals, such as floppy and CD drives, can be referenced by their drive letter.

Use the wildcard notation (* or ?) to indicate files within directories and whether directories and subdirectories are recursive.

***Table 2-2 Wildcard Operators***

| Example | Translation |
|---|---|
| * | One wildcard entry indicates a single directory level or all files in a specified directory. |
| ** | Two wildcards entered in this manner indicate a recursive directory path (including all directories, passing down as many levels as exist in the path). |
| ? | Use the question mark wildcard to represent a single character. For example, ???.doc. This indicates a file name containing only three characters with a .doc extension. |

For example:

The following entry indicates all files one directory level down in the winnt directory. It does not include files in the winnt directory itself.

`c:\winnt\*\*`
The following entry indicates all files in the winnt directory and all subfolders recursively (digging down as deep as necessary) and files.

`c:\winnt\**\*`
The following entry indicates all files in the winnt directory and all subfolders recursively (digging down as deep as necessary) and files that contain exactly two characters in their name and have any extension.

`c:\winnt\**\??.*`
If you do not specify a drive path in a file text field, CSA MC always prepends the string `**\` to the named file. For example, if you enter foo.doc into a text field, it is saved as `**\foo.doc`.

**Note** You can use the same wildcard notations for indicating UNIX files and directories.

## File and Directory Protection

File access control rules provide three checkboxes which offer you the option of protecting files and/or directories. You should understand that file protection encompasses read/write access. Directory protection encompasses directory deletes, renames, and new directory creation.

**Caution** Directory protection ignores the file portion of the specified path and only matches the directory portion of the path. If the directory portion is not well specified, the protection will be overly broad. For example, if you select to protect a directory in a deny rule and enter the directory path as follows: `**\Program Files\**Outlook.exe`, then no directories can be modified under Program Files. That is an overly broad protection to specify and would likely result in system instability. If you choose to protect directories, be sure to get very specific in your path string and understand the resulting behavior.

When protecting against directory creation, in particular, you should note that directory creation applies to an exact directory path match, but directory write and rename protection applies to all directories explicitly named in a path. If a directory name is completely wildcarded **\, no protections exist for that particular component of the directory.

The following Windows example displays what protections exist for a literally entered resource in a Deny, File access control rule where the following checkboxes are selected: Read File, Write File, and Create, Delete, Rename Directory.

Example:

```
**\Program Files\**\*SQL*\bin\*.exe
```

In the example above, the following protections exist:

- Directory protection: `**\Program Files` cannot be renamed or deleted, but it can be created.
- Directory protection: `**\Program Files\**\*SQL*` cannot be renamed or deleted, but it can be created.
- Directory protection: `**\Program Files\**\*SQL*\bin` cannot be renamed, deleted, or created.
- Directory protection: A new directory cannot be created which matches `**\Program Files\**\*SQL*\bin`

- File protection: Executable files located in the specified directory path cannot be read or written to.

In the following UNIX example, `/usr/adm/sg/` is the directory and `x`, `y`, and `z` are files in the sg directory.

The following entry protects files x, y, and z in the sg directory and it protects the directory structure (if all checkboxes are selected in the File access control rule).

```
/usr/adm/sg/*
```

This example works just like the previous Windows example. Therefore, directory creates are only prevented if the directory attempted to be created

exactly matches the entire path of `/usr/adm/sg/*`. Directory deletes and renames are prevented for each directory named in the path. Note that the only file protection provided here is within the `sg` directory because the last entry in a path is always assumed to be the file. If you only wanted to provide directory protection and not file protection, you would still have to enter the literal in the same manner. You must provide /* at the end of the path or the last entry would be seen as a file rather than a directory. In this case, you would only select the Write Directory checkbox and even though all files in the `sg` directory are specified, they are not protected.

To protect files in the `usr` directory, you would have to make that another entry, e.g. /usr/* would have to be entered on another line below the original UNIX example. (Note that Windows works the same way.)

For UNIX directory entries, because there is no drive letter to specify (as in Windows) the wildcarded path (/**/) is not automatically placed in front of a UNIX path that begins with "/". If you begin the path with a forward slash, the directory path is taken literally. If you do not place a slash in front of the path, a wild card path is inserted before the entry when you save the rule.

**Caution** You must make some file specification when you are entering literal paths. A wildcard is acceptable to specify all files in a named directory. CSA MC always assumes the last entry in a literal path (not a variable) is a file.

**Caution** Symbolic Links—For UNIX, if you create a File access control rule to protect a symbolic link, ONLY that symbolic link is protected. The underlying resource, unless also specified, is NOT protected. For example, a File access control rule

written for /etc/hosts does not protect /etc/inet/hosts. Similarly, a File access control rule written for /etc/inet/hosts does not protect /etc/hosts. If you want to protect a symbolic link and its underlying resource, both must be specified in the rule. See Resource Access Control, page 4-102 for further symbolic link protection information.

You can use the following "short hand" entries in File Sets, File access control rules, File monitor rules, and Application classes to indicate common system directories. The @symbol must appear at the start of the short hand name. These entries resolve to the Windows directory on each agent system.

*Table 2-3 Sample Short Hand File Tokens (Windows only)*

| Example | Translation |
|---|---|
| @windows | Use `@windows` to indicate the directory pointed to by the `%SystemRoot%` environment variable<br>When using @windows, for example, in the File access control rule Files field, it is interpreted as `@windows\*` to indicate the files within the directory. |
| @system | Use `@system` to indicate `%SystemRoot%system32` |
| @(regpath Registry key/value pair default=default directory) | Use `@(regpath Registry key/value pair default=default directory)` to localize the directory structure of an application or other resource. This is useful to indicate software regardless of the directory to which it has been installed. Note that the default= field is optional but recommended, For example:<br>`@(regpath HKLM\CCS\foo\instdir default=**\Program Files\foo\bin)` |
| @dynamic | Use `@dynamic` in the File set text field to indicate all files that have been quarantined by CSA MC as a result of correlated suspected virus application events, correlated virus scanner log messages, or files that were added manually by the administrator. This list updates automatically (dynamically) as logged quarantined files are received.<br>To view the files that are added to the dynamically quarantined files list and to manually add files to be quarantined, click the Manage **dynamically quarantined files** link on the Global Event Correlation page. See Manage Dynamically Quarantined Files and IP Addresses, page 5-23 for more information. |

You can use the following "short hand" entries in File Sets and in File access control and File monitor rules to indicate removable media. The @ symbol must appear at the start of the name. These entries resolve as follows:

*Table 2-4 Removable Media Token Syntax (Windows only)*

| Example | Translation |
|---|---|
| @removable | This indicates all removable media. That includes, floppies, CDs, zip drives, etc. Note that if you want to indicate all removable media except floppies, for example, you'd have to configure a file set that explicitly excludes floppies from all removable media. |
| @floppy | This indicates all floppy drives. You can specify particular file paths on floppy media using the following syntax: `@floppy:\<specify wildcards or paths>`. Note that `@floppy:\` means only the top level files on the floppy media. `@floppy` or `@floppy:\**` means all files on the floppy media. |
| @CD | This indicates all CD-ROM drives( including DVD). You can specify particular file paths on CD media using the following syntax: `@CD:\<specify wildcards or paths>`. Note that `@CD:\` means only the top level files on the floppy media. `@CD` or `@CD:\**` means all files on the floppy media. |

**Note** USB connected drives are removable media.

You can also use **@fixed** to indicate all local system drives without having to indicate the drive letters. For example, @fixed:\Program Files\Outlook\msimn.exe

For correct directory path specifications on internationalized Windows versions, you can use the following universal tokens in File Sets, File access control rules, File monitor rules, and Application classes to indicate common system directories for the localized version of the OS. These entries resolve to the appropriate Windows directory on each localized agent system.

***Table 2-5 Universal Tokens for Localized Directory Paths***

| Token | Translation |
|---|---|
| @startup | The file system directory that corresponds to the user's startup program group. The programs in the startup group start automatically when the user logs in. |
| @startmenu | The file system directory that contains the programs and folders that appear on the start menu for all users. |
| @program_files | This represents program files and program files\common. This folder is for installed programs and for components that are shared across applications. |
| @mydocuments | This represents documents and my documents. This folder contains documents that are common to all users. |
| @desktop or @desktop directory | The file system directory that contains files and folders that appear on the desktop for all users. |

**Note** When you specify one of the tokens in the table above, the next component is automatically wildcarded. This is necessary to correctly resolve the specified directory path.

**Tip** Use the diagnostics tool on the Host page to view what a token translates to for an individual host.

### Network system paths (Windows only) entered using the following syntax:

```
\\<machine name>\<share>\<path>\<filename>
\\Backup_Server\finance\records\database.db
```

You can also use **@network** (on Windows and UNIX) to indicate all network shares. For example, `@network:\finance\records\database.db`

**Caution** Do NOT enter a drive letter for network share paths.

### Network address text boxes require addresses entered in any of the following formats:

When entering addresses, type each entry on its own line. The ranges are inclusive of the first and last IP address in the range.

*Table 2-6 Network Address Syntax*

| Example | Translation |
|---|---|
| 128.66.24.130 | Indicates a single address |
| 128.67.2.10-20 | Indicates a range of addresses 128.67.2.**10** - 128.67.2.**20** |
| 128.67.3.0-4.255 | Indicates a range of addresses 128.67.**3.0** - 128.67.**4.255** |
| 128.67.0.0/16 | Indicates a range of addresses 128.67.**0.0** - 128.67.**255.255** |

You can use the following "short hand" entry in Network Address Sets and in Network Access Control rules to indicate all local addresses on the agent system in question. The @ symbol must appear at the start of the short hand name.

Use **@local** to indicate all local addresses on the agent system.

Use **@remote** to indicate all addresses that are not on the local agent system.

Use **@subnet** to indicate the local subnet addresses of the agent system. This is useful for allowing communications on your internal network but not to the outside world. This gives you more granularity for specifying internal communications without having to know all subnet addresses.

Use **@recent** to track addresses with which agent systems have recently communicated. This is useful for restricting callback connections to addresses with which you've recently initiated communications. You can also use this to restrict server connections to only those hosts that have initiated the control channel.

Use **@dynamic** in the Network address set text field to indicate all IP addresses that have been quarantined by CSA MC as a result of correlated communications with untrusted hosts events or IP addresses that were added manually by the administrator. This list updates automatically (dynamically) as logged quarantined IP addresses are received.

To view the IP addresses that are added to the dynamically quarantined IP addresses list and to manually add IP addresses to be quarantined, click the Manage dynamically **quarantined IP addresses** link on the Global Event Correlation page. See Manage Dynamically Quarantined Files and IP Addresses, page 5-23 for more information.

Use **@smb-null-session** in Network access control rules (as the network service). A null session is an unauthenticated session to one of the NetBIOS or CIFS ports on a system. These ports are typically used for file and print sharing, but they can also be used as an attack vector (e.g. SMB die). Use the @smb-null-session token to control connections to the system via an unauthenticated null-session.

**Caution** On UNIX platforms, IPV6 addresses are not officially supported; however, an IPV6 connection will work as the applied rules dictate if the address in question is covered by the "all" addresses range (0.0.0.0-255.255.255.255 includes IPV6 addresses) or by @local. Local addresses on the agent system (indicated by @local) also include IPV6 addresses.

See Network Access Control, page 4-69 for more information.

### Network service text boxes require protocols and port ranges entered in the following formats:

Format all entries as:

```
protocol/port or port range
TCP/80
UDP/53
TCP/1024-65535
```

The protocol here is either "TCP" or "UDP".

Port ranges are designated in the range 0-65535.

Designating ephemeral ports—In some cases, an application may want to offer a temporary service port for callback data connections. An ephemeral port is a temporary system-assigned port for this purpose.
For example, an ephemeral port would be the likely data connection for active FTP. If you do not specify an ephemeral port range for accepting an active FTP connection, you would have to allow clients to listen on a wide range of ports to accept this connection type. This would unnecessarily open a wide range of data channels and possibly create a vulnerability that could be exploited by a Trojan.

You can specify an ephemeral port range for a Network service as follows:

```
TCP/ephemeral
UDP/ephemeral
```

**Note** It only makes sense to use ephemeral ports on systems accepting connections. Also note that Deny log messages triggered by a rule using an ephemeral port range appear in the event log containing the real port number.

**Caution** Ports that are ephemerally allocated are only matched against an explicit ephemeral class. Ephemeral ports are treated as "port 0" for rule comparisons. For example, ephemeral port 2000 matches port 0, not port 2000.


# Configuring Groups and Managing Hosts

## Overview

The system hosts across your network, including mobile systems in the field, must download Cisco Security Agent software and register with Management Center for Cisco Security Agents to receive the security policies configured for them. When you are ready to apply policies to the hosts running agents, having those hosts placed into common groups streamlines the process of assigning policies to several hosts at once. To place hosts into groups, you must first analyze the security needs of each host system and map out a security plan. Hosts with similar requirements can then be grouped together.

Management Center for Cisco Security Agents ships with several pre-configured groups you can use. If the included groups do not suit your needs, use the instructions in this chapter to configure new groups or to edit existing ones.

This section contains the following topics.


- Grouping Hosts Together, page 3-2
- Mandatory Group Enrollment, page 3-3
- Configuring Groups, page 3-3
- Managing Agent Kits, page 3-7
- Creating Agent Kits, page 3-8
- Agent Registration, page 3-17
- Scripted Agent Installs and Uninstalls, page 3-18

- Registration Control, page 3-18
- Modifying Agent Kits, page 3-19
- Managing Hosts Using CSA MC, page 3-21
- Viewing General Host Statuses with CSA MC, page 3-21
- Viewing All Hosts Managed by CSA MC, page 3-21
- Viewing Host Details, page 3-22
- Searching for Hosts, page 3-28
- Deleting Hosts, page 3-30
- Changing Host Memberships in Groups, page 3-31
- Distributing Software Updates, page 3-39
- Configuring Scheduled Software Updates, page 3-41
- Software Updates in a Distributed Configuration, page 3-45


# Grouping Hosts Together

Host groups reduce the administrative burden of managing a large number of agents. All hosts across your network, including mobile systems in the field, must exist as registered host entries in the Management Center for Cisco Security Agents for policy configurations to be assigned to them.

Grouping individual host systems together provides the following advantages:

- It lets you consistently apply the same set of policies across multiple host systems.
- It lets you apply Alert mechanisms and Event Set parameters based on group configurations.
- It lets you use Test Mode to try out policies on groups of hosts before you actively enforce those policies.

You can group hosts together based on any criteria that best fits your enterprise. For example:

- Group hosts according to system function, such as web servers. Then you would create a policy that corresponds specifically to the needs of your web servers and distribute it to that group.

- Group hosts according to business groups, such as finance, operations, and marketing. Distribute policies based on each business group's individual needs.
- Group hosts according to geographical or topological location. For example, group hosts based on their subnet designation for reporting purposes.
- Group hosts according to their importance to your organization. Place mission-critical systems into a common group to apply critical alert level configurations to them.

**Note** Hosts may belong to multiple groups and automatically receive policies that are attached to every group to which they belong. You can add or remove hosts from a group at any time. However, the policy configuration of a host that is moved to another group will not take effect until you generate your rule programs and distribute them.

# Mandatory Group Enrollment

CSA MC provides three auto-enrollment architectural groups <All Windows>, <All Solaris>, <All Linux> that are mandatory for all hosts of a given OS architecture. For example, all Windows hosts are automatically enrolled in the <All Windows> (in addition to any other groups you have specified) when they register with CSA MC. Hosts cannot be removed from these mandatory groups.

By providing group auto-enrollment for hosts, any policies you attach to these groups also become mandatory by association. You might want to use these mandatory groups to apply policies that prevent some critical service from being inadvertently banned. For example, you could attach policies to prevent DNS or DHCP from being disabled by an overly restrictive rule.

# Configuring Groups

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 agent kits.

You do not configure hosts with CSA MC as you do other CSA MC elements. When hosts across your network download and install agent kits, they automatically and transparently register with CSA MC. Hosts inherit membership to the groups that were associated with the agent kit they installed. Successfully registered hosts appear in a linked list when you select Hosts from the Systems category in the menu bar. At registration time, hosts are also automatically put into their assigned group. You can change host groupings at any time.

**Note** Management Center for Cisco Security Agents ships with preconfigured groups (in addition to the mandatory 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 and select **Groups** from the drop-down list that appears. The list of existing Groups is displayed. Management Center for Cisco Security Agents ships with several pre-configured groups.

**Step 2** Click the **New** button to create a new group entry. (This group is empty until hosts install agents and register.)

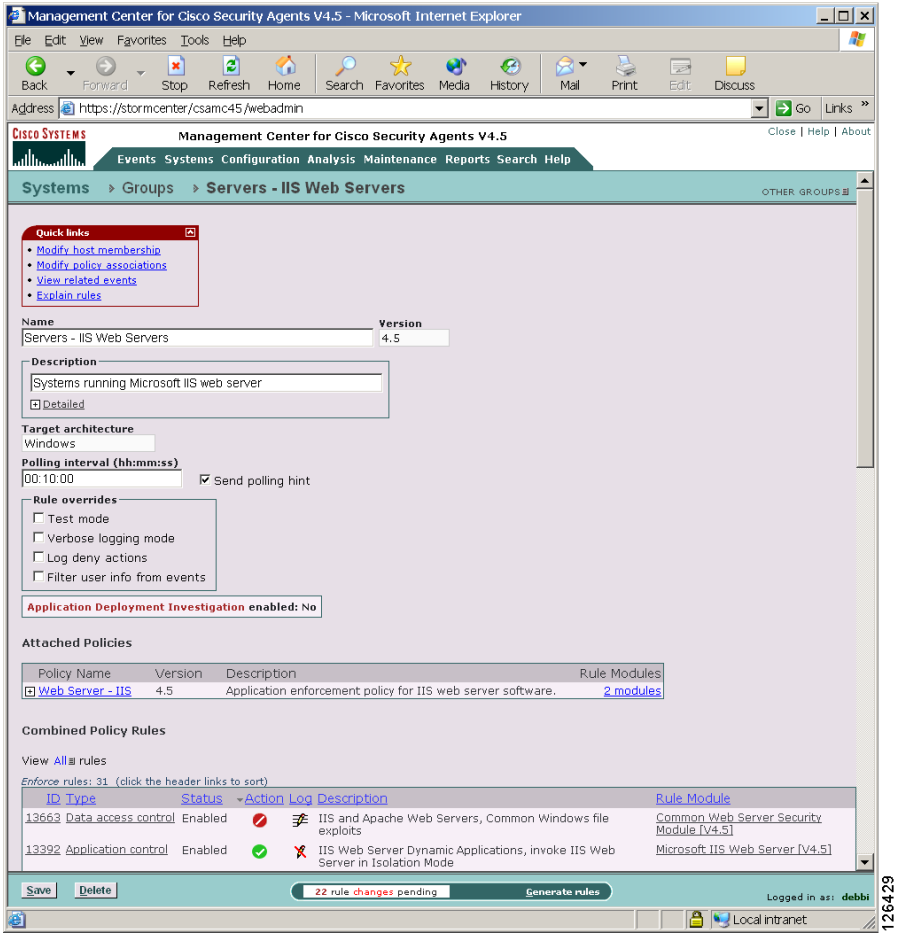
**Note** If you have "All" designated as the operating system type for your administrator session, you are prompted to select whether this is a Windows, Solaris, or Linux group. See Administrator Preferences, page 2-6 for details. (You cannot combine hosts of differing OS architectures in the same group.)

**Step 3** In the available group 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, hyphens, and underscores. You should adopt a naming convention that lets you quickly recognize groups in the CSA MC group list view.
- **Description**—This description appears in the list view to help you identify this particular group. Expand the **+Detailed** field to enter a longer description.

**Tip** You can use the Tab key to navigate between edit fields.

***Figure 3-1 Group Configuration Page***




**Step 4** You can change the default **Polling interval** to any value between 10 seconds and 24 hours (formatted as hh:mm.ss). This controls how often agents in this group poll into CSA MC for policy updates. Shortening the polling time can be useful when you are trying out new policies. Otherwise, the default value is

recommended. (If you have the same hosts in multiple groups, the group containing the shortest polling interval setting takes precedence for the hosts in question.)

**Note** If you change a group's polling interval, that new interval time will not take effect until the host polls in again for new rules. Therefore, it may take as long as the previous polling interval setting before hosts begin polling in using the new setting.

**Step 5** Optionally, enable the **Send polling hint** capability. Normally, if you make changes to a policy, schedule a software update, or make any other change to a host's configuration, the host does not receive that change until it next polls into the MC. But if you have the Send polling hint checkbox selected, certain changes that occur on the MC will cause a "non-reliable" signed UDP message to be sent to the appropriate hosts. This message tells hosts to poll into the MC earlier than their next scheduled polling interval. The UDP message would be sent if a policy change occurs, if a global correlation event causes a file to be added to the global quarantine list, and if you select to retrieve status information from a particular host. (This feature only works if no NAT or PAT exists between CSA MC and the agent.)

**Step 6** Optionally, enable one or more **Rule overrides** for the group. You can select the **Test Mode** checkbox for this group.

**Caution** In Test Mode, the Cisco Security 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 (if logging is selected for the rule). This helps you to understand the impact of deploying a policy on a host before enforcing it. For further information, see Using Test Mode, page 4-114.

**Step 7** Optionally, enable **Verbose Logging Mode** to change the event log timer to log all reoccurring events rather than suppressing duplicates. See Chapter 8, "Event Logging and Alerts" for more information on the event log.

**Step 8** Optionally, enable **Log all deny actions** to turn on logging for all deny rules running on hosts within the group regardless of the individual rule settings for the policy attached to the group. You may wish to use this feature to turn on all deny logging for diagnostic purposes.

**Step 9** Optionally, you can select the **Filter user info from events** checkbox for this group. Due to privacy issues, you may not want this username information displayed in events or in the additional information screen available from the event Details link.

**Step 10** Optionally, for Windows groups, you can select to enable Application Deployment and Analysis. This analysis functionality works with CSA MC and the agent, serving as a data collection tool for administrators deploying policies across systems and networks. See Chapter 11, "Using Cisco Security Agent Analysis" for detailed information. If this feature is enabled, you can access analysis reports from a link on this page.

**Step 11** When all required information is entered, click the **Save** button to enter and save your group in the CSA MC database.

Once you attach (associate) policies to specific groups, the configuration view for the group displays a table listing all the rules, in order of precedence, that are applied to that group. From this table, you can navigate to those rules and policies.

**Tip** To remotely reset *all* hosts in a group to the system default settings, click the **Reset Cisco Security Agent** button in the footer frame of the Group page. This functionality is also available from the individual Host page, letting you reset one host at a time. See The Agent User Interface, page A-10 for more information on the agent reset option (also available locally on the agent system).

# Managing Agent Kits

The Management Center for Cisco Security Agent allows for the creation and maintenance of custom agent installation kits that greatly reduce the administrative burden of deploying the agent on new systems.

Agent kits must have a group association for deployment. Groups are a collection of policies and are associated with a number of Hosts. When hosts downloads agent kits, the kits place the host in the corresponding groups and enforce the associated policies of each group.

CSA MC also ships with preconfigured agent kits you can use if they meet your initial needs. There are kits for generic desktops, generic servers, and CSA MCs (CiscoWorks VMS).

# Creating Agent Kits

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

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

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

**Note** If you intend to distribute Cisco Trust Agent (CTA) in an agent kit, make sure that you have installed the correct CTA installer files before you begin this procedure. See *Installing the Management Center for Cisco Security Agent* manual for the procedure to install CTA installer files.

To create agent kits, do the following.

**Step 1** Move the mouse over **Systems** in the menu bar and select **Agent Kits** from the drop-down menu that appears. Existing agent kits are displayed.

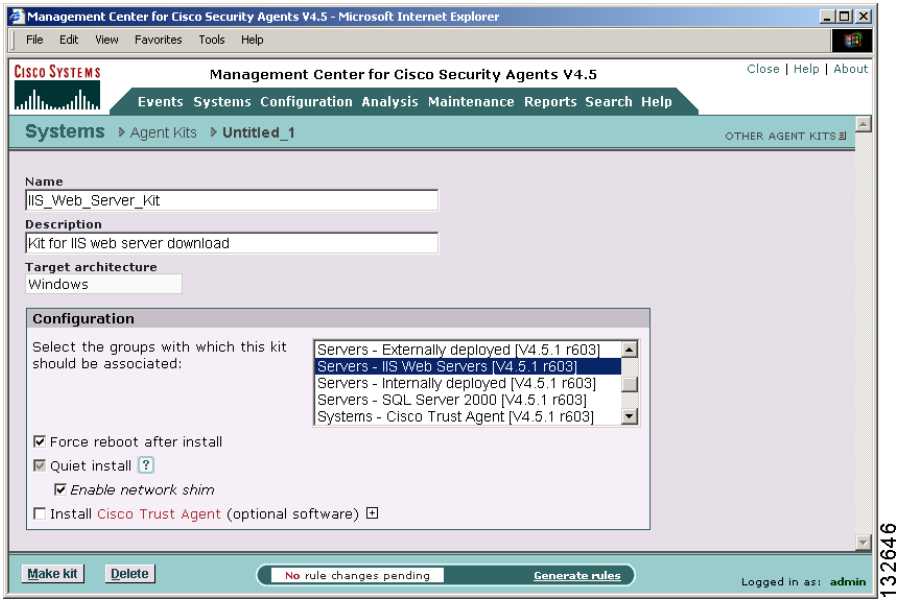
**Step 2** Click the **New** button to create a new agent kit.

**Note** If you have "All" designated as the operating system type for your administrator session, you are prompted to select whether this is a Windows, Linux, or Solaris kit. See Administrator Preferences, page 2-6 for details. (You cannot select a Solaris group for an agent kit that you have configured for Windows systems.)

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

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

***Figure 3-2 Create Agent Kit***




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

**Step 6** You have the option of forcing systems to reboot after the agent installation completes (Windows and Linux only). If you select the Force reboot after install checkbox, when the install finishes, a message appears to the end user warning that the system will automatically reboot in 5 minutes. This reboot cannot be stopped by the end user. Keep in mind, if you are selecting to force a reboot, the installation must also be "Quiet". See the next step for more details.

**Note** Solaris agent kit installations do not have the option to reboot automatically when complete. If you wish to reboot a Solaris system after installing an agent, you must do so manually.

**Note** NOTE: In some cases, you may not want a system to reboot after the installation completes. If a reboot does not occur after the agent installation, partial security is enforced immediately. Full security is enforced after the first reboot. (Note that Windows NT4 systems must be rebooted after an agent installation.)

Refer to Agent Reboot vs. No Reboot, page 3-15 for information on what security is not enforced if a system is not rebooted after an agent installation.

**Step 7** Select whether or not to have agents install "quietly" on end-user systems (Windows and Linux only). A **Quiet install** requires users to download the self-extracting executable as does the "noisy" install. The difference is, no prompts appear and the user is not required to enter any information or select any options. A noisy install prompts the user for installation options, such as enabling the network shim, in addition to the reboot prompt.

These possible checkbox options would be combined for the following effects once the Windows or Linux agent installation has completed:

| | |
|---|---|
| Force reboot checkbox=enabled<br>Quiet install checkbox=enabled | The install ends by displaying a prompt indicating that a reboot will occur within 5 minutes. |
| Force reboot checkbox=disabled<br>Quiet install checkbox=enabled | The install proceeds and ends quietly with no prompts. Full functionality occurs the next time the user happens to reboot. |
| Force reboot checkbox=disabled<br>Quiet install checkbox=disabled | The install prompts the user to enable the network shim and ends by displaying a prompt indicating that an update has occurred and the end user can reboot the system at their convenience for full functionality. |

**Step 8** For Windows kits, if you select Quiet install, you can also select whether the **Network shim** is enabled or not during the installation.

**Caution** 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 not be needed. To allow users to enable network shims, you would create kits as "noisy" installations. (Do not select the Quiet install checkbox.) This way, users are prompted to enable the network shim during the agent installation. For more information, see Network Shim Optional, page A-7.

**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 (configured in the Network Shield rule page) mentioned in the previous paragraph are not enabled.

**Step 9** (Optional) Install the Cisco Trust Agent by selecting the checkbox next to **Install Cisco Trust Agent**. The area below the checkbox expands to show several fields.

These fields allow you to also specify the following settings:

- CTA Installer. From the drop-down menu specifiy which Cisco Trust Agent installer to use.
- Initialization data. The text you enter In the Cisco Trust Agent initialization data field is used to create the ctad.ini file for CTA.
- Certificate file. Specify a Cisco Secure ACS server certificate to be installed along with CTA.
- Install scripting interface. The CTA Scripting Interface is only available for NAC Phase 2 networks. If you use select a CTA 1.x installer, you will not be able to install the CTA Scripting interface.
- Check the last box if you want CTA to remain installed even if CSA is uninstalled.

**Note** The choices you make in this step are important. Refer to Cisco Trust Agent Administrator Guide for a complete description of how these settings impact your CTA installation. For NAC and CTA plugin details, see Cisco Security Agent Posture Plug-in for CTA, page 10-20. For details on NAC, go to the following link on Cisco.com: http://www.cisco.com/en/US/netsol/ns466/networking_solutions_sub_solution_home.html

**Step 10** Click the **Make Kit** button. A new page opens with the message, "The kit was successfully created."

**Step 11** Click the **rule generation** link to advance to the Generate Rule Program page. The rules that require generation are listed at the bottom of the page.

**Step 12** Click **Generate** to generate these rules and make your kit available for deployment. Once the generation rules operation completes, you receive the message, "Rule program generation successful."

**Step 13** Move the mouse over **Systems** in the menu bar and select **Agent Kits** from the drop-down menu that appears. The agent kit you just created has been added to the list of available kits.

**Step 14** Click the name of your new kit to see its agent kit page. The page 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:

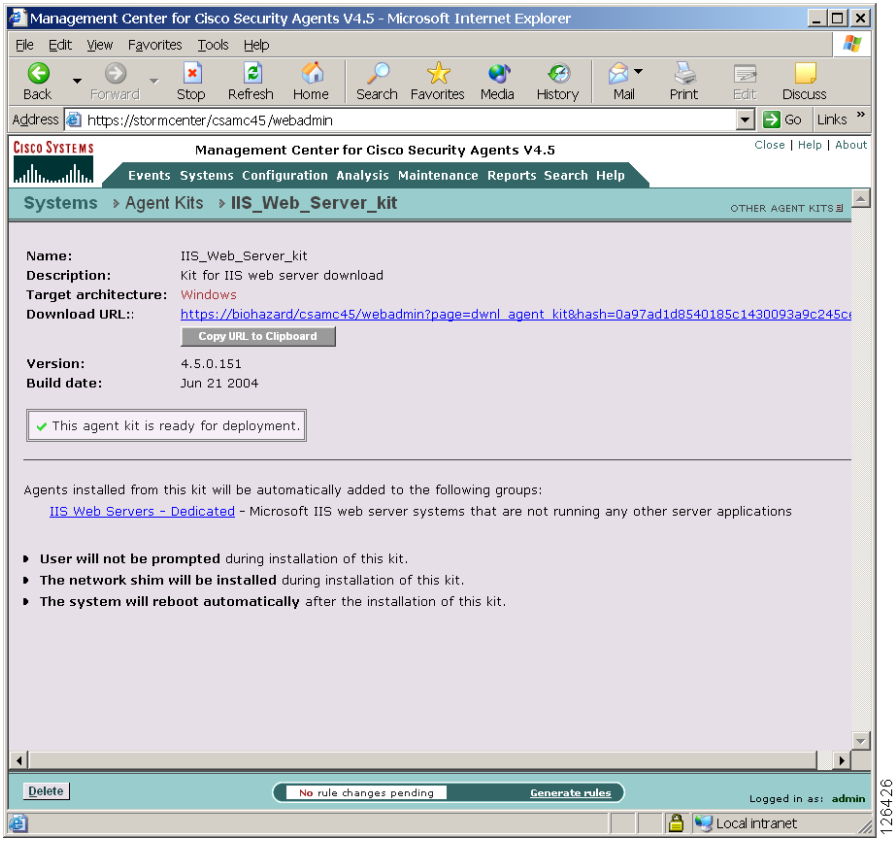
```
https://<ciscoworks system name>/csamc45/kits
```

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

**Note** Note that the Registration Control feature also applies to the <ciscoworks system name>/csamc45/kits URL. If the Registration Control feature (see Registration Control, page 3-18 for details on the feature) prevents your IP address from registering, it also prevents you from viewing this "kits" URL.

**Note** The page for your agent kit also displays the status of the kit. See Agent Kit Status, page 3-14 for details on when a kit is ready for download.

***Figure 3-3 Agent Kit Download URL***




**Note** If you installed Management Center for Cisco Security Agents to the default directory, all agent kits are placed in the `%Program Files%\CSCOpx\CSAMC45\bin\webserver\htdocs\deploy_kits` directory.

## Agent Kit Status

When you create an agent kit, it is given one of these four status levels based on how far into the configuration you've progressed. Those status levels are as follows:

- Ready: This means the agent kit is ready for download to host systems.
- Needs rule generation: This means that all agent kit configuration parameters are complete, but you must generate rules before the kit can be downloaded.
- Incomplete: This means that you have not configured all the necessary parameters for this agent kit. You must complete the configuration and then generate rules before the kit can be downloaded.
- Undeployable: This status will only occur if you have ungenerated kits on CSA MC and then you upgrade CSA MC to a new version. Agent kits that were created but never generated and have an old version number can never be deployed and should be deleted.

*Figure 3-4 Agent Install Complete Prompt for Optional Not-Automatic Reboot*

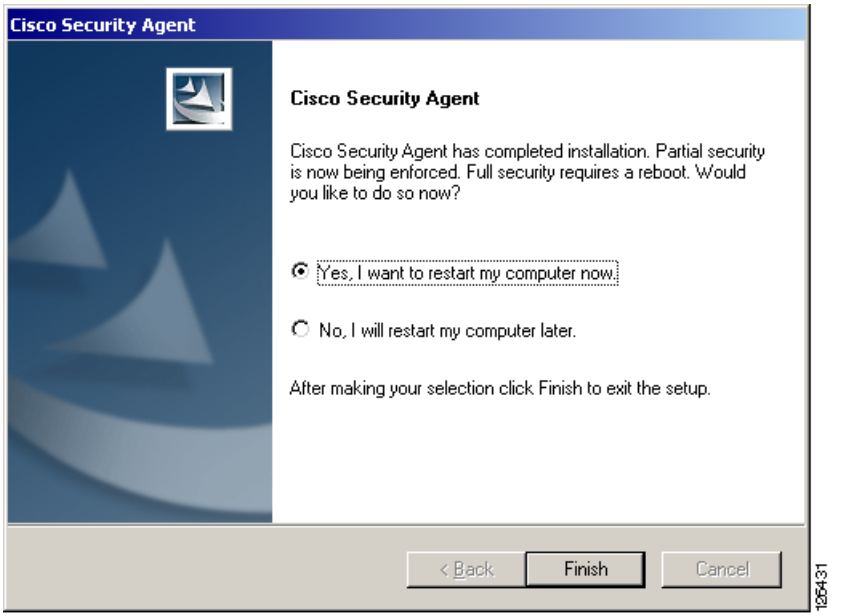
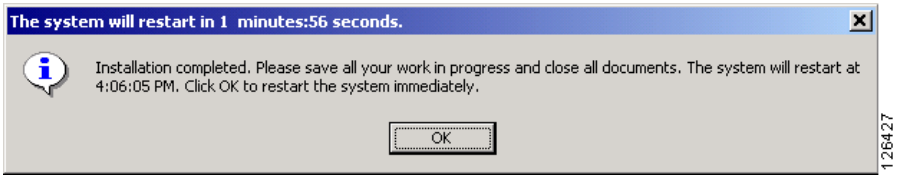



*Figure 3-5 Agent Install Complete Prompt for Automatic Reboot*




## Agent Reboot vs. No Reboot

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

Windows agents

- Network Shield rules are not applied until the system is rebooted.

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

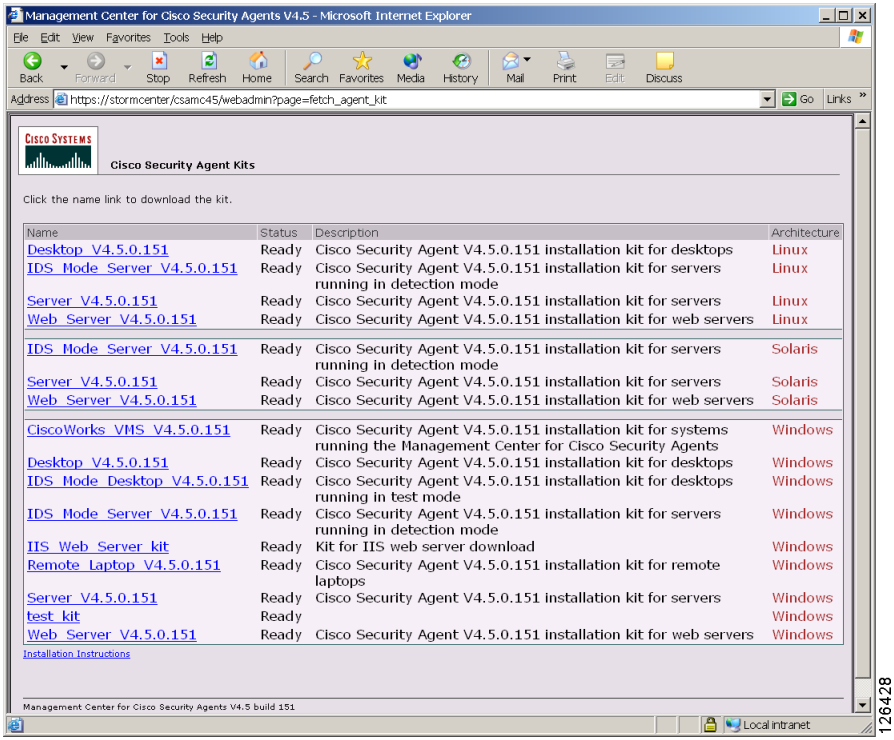
Solaris and Linux agents, when no reboot occurs after install, the following caveats exist:

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

**Caution** Windows NT systems must be rebooted after the agent installation completes. Windows NT systems will not receive a reboot optional prompt at the end of an agent installation (even if that option is part of the agent kit installation).

**Note** The reboot information here only applies to new agent installations. It does not apply to software updates. Please refer to Table 3-1 on page 3-43 for software update reboot details.

*Figure 3-6 Download Agent Kits*




# Agent Registration

When an agent kit is ready for distribution, you can notify end users to download and install the kit from the URL produced by CSA MC when the kit is made. Once the kit installation is complete, each individual host's agent automatically and transparently registers with CSA MC.

**Note** Each kit is created for particular groups based on the policies that will be attached to those groups. Policies are described in Chapter 4, "Building Policies".

# Scripted Agent Installs and Uninstalls

You can use scripts to silently install and uninstall Windows Cisco Security Agents on end user systems. (Scripted agent installs and uninstalls are not supported on Linux and Solaris systems.)

- Scripted install: The agent kit is a self-extracting executable placed in the following directory on the server: `%Program Files%\CSCOpx\CSAMC45\bin\webserver\htdocs\deploy_kits`. (Retrieve the kit from this directory or download it from the server.) You can then use a script to copy and silently install agent kits on systems. Note that you must select the **Quiet install** checkbox when you build the kit if you are planning to install it via a script.
- Scripted uninstall: The agent installation places a bat file in the system32 directory. Administrators may use a script to remotely and silently uninstall the agent by invoking the CSA_uninstall.bat file in the system32 directory. You must also pass a parameter to the file for the agent to uninstall silently regardless of whether the original agent kit was a Quiet install. Enter the following: `CSA_uninstall.bat 3`

**Note** Before silently uninstalling the agent via a script, you must disable any agent service control rules that deny or query administrators before stopping the agent service.

Whether or not an end user system is going to have a visible agent UI or a hidden one (see Agent UI Control, page 4-48), the end user (or administrator) must download and install the agent kit on the system. The initial installation of an agent kit cannot be done automatically (unless you have written your own script to do so, see Scripted Agent Installs and Uninstalls, page 3-18).

# Registration Control

This feature is accessible from the Systems item in the menu bar. Access the Registration Control page to enter a range of addresses which restricts agent hosts attempting to successfully register with CSA MC to those with addresses listed here.

This feature prevents unauthorized hosts from downloading agent kits and receiving rules. (Note that any user who is logged in to CSA MC, can download a kit.)

The default entry here is <all> (0.0.0.0-255.255.255.255) which applies no address registration restrictions. An example entry of restricted registration addresses is as follows. (Only those addresses within the range listed can register. This range is inclusive):

```
192.168.10.0-192.168.10.255
172.16.20.0-172.16.20.255
```

# Modifying Agent Kits

After an agent kit is made and deployed, new groups can be associated with the kit and existing groups can be removed from the kit.

One use for this feature is to prolong the life of installation images by requiring fewer changes to agent kits. For example, agent kits would most likely be deployed in test mode until all the rules, rule-modules, and policies are fine-tuned to meet the needs of your enterprise. An image installed on new desktops during the testing period would include an agent kit, which includes the Test Mode Systems group, which makes all other groups run in test mode.

Once the period of testing is over, the image deployed for new desktops would still include the Test Mode System group but it may no longer be needed because the rules and policies have been finalized and it is time to "go live" for some or all of your enterprise. This feature would allow you to remove the Test Mode System group from the agent kit that is currently included in the installation image for all desktops. When the agent on a new desktop registers with CSA MC for the first time, the Test Mode System group will be removed from the agent kit and the new desktop will not run in test mode.

To modify group associations with agent kits, follow this procedure:

**Step 1** Move the mouse over **Systems** in the menu bar and select **Agent Kits** from the drop-down menu that appears.

**Step 2** Click the name of the kit you want to modify.

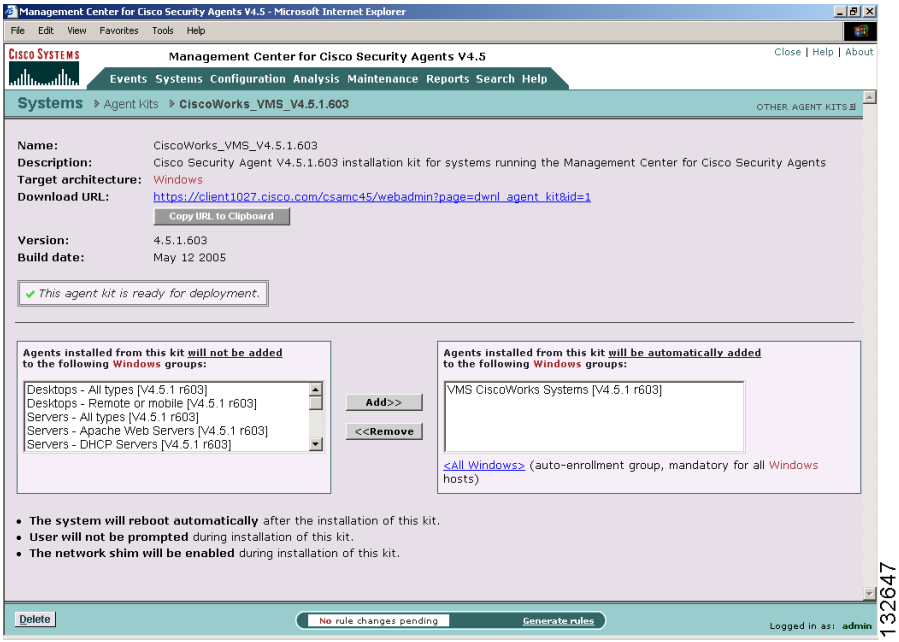
**Step 3** Now, add or remove groups from an agent kit (See Figure 3-7):

- To add a group to an agent kit, click the group name in the **Agents installed from this kit will not be automatically added to the following groups** swap box and click **Add**.
- To remove a group from an agent kit, click the group name in the **Agents installed from this kit will be automatically added to the following groups** swap box and click **Remove**.

**Step 4** Click the **rule generation** link to advance to the Generate Rule Program page. The rules that require generation are listed at the bottom of the page.

**Step 5** Click **Generate** to generate these rules and make your kit available for deployment. Once the generation rules operation completes, you receive the message, "Rule program generation successful."

***Figure 3-7 Agent Kit Page***




This procedure would not work for desktops after they have initially registered with their CSA MC. Considering our example, when desktops poll in to CSA MC on regular intervals they are still included in the Test Mode System group. To

move them out of the Test Mode System group, they can be moved in bulk out of the group using the Bulk Transferring Hosts From One Group to Another procedure described in Changing Host Memberships in Groups, page 3-31.

# Managing Hosts Using CSA MC

A host is any system that has installed an agent kit from CSA MC and has registered with CSA MC. The host may be a desktop or server and may be of any supported operating system type.

Once the host has registered with CSA MC, it can receive policy updates, it can be added to or removed from groups, and its status can be monitored by CSA MC.

## Viewing General Host Statuses with CSA MC

Follow this procedure to view the general status of all hosts managed by CSA MC:

**Step 1** Move your mouse over **Events** in the menu bar and click **Status Summary** in the drop-down list.

**Step 2** If it is not already expanded, click the plus box next to **Network Status.**

**Step 3** There are several Network Status categories listed in the status summary page. Next to each category is a number indicating how many hosts have been placed in each of the status categories. Click the link for the number of hosts in the category to see the host list view for that category.

## Viewing All Hosts Managed by CSA MC

To view all the hosts that are managed by CSA MC, follow this procedure:

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

**Step 2** (Optional) Sort the host list by operating system.

**Step 3** From the Architecture drop-down list box, select one of the following host statuses:

- **Active**: A host is active if it polls into the management server at regular intervals and has not missed three polling intervals. When you select this viewing option, a “Yes” for Active or a “No” for Not Active appears in the column.

  Note that a "Not active host" is a host that has missed three polling intervals or has not polled into the server for at least one hour.
- **Protected**: When you select this viewing option, a "Yes" for Protected or a "No" for Not Protected appears in the column. A system is not protected if it does not belong to a group or if it belongs to a group that has no policies attached.
- **Latest software**: When you select this viewing option, a "Yes" for Latest Software or a "No" for Not Latest Software appears in the column. If an agent is not running the latest software, you will want to deploy a software update.
- **Test Mode**: When you select this viewing option, a "Yes" for running in Test Mode or a "No" for Not Running in Test Mode appears in the column.
- **Last Poll**: When you select this viewing option, the time and date of the most recent poll for the host is displayed.

# Viewing Host Details

To view detailed information about one host, follow this procedure:

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

**Step 2** (Optional) Sort the host list by operating system.

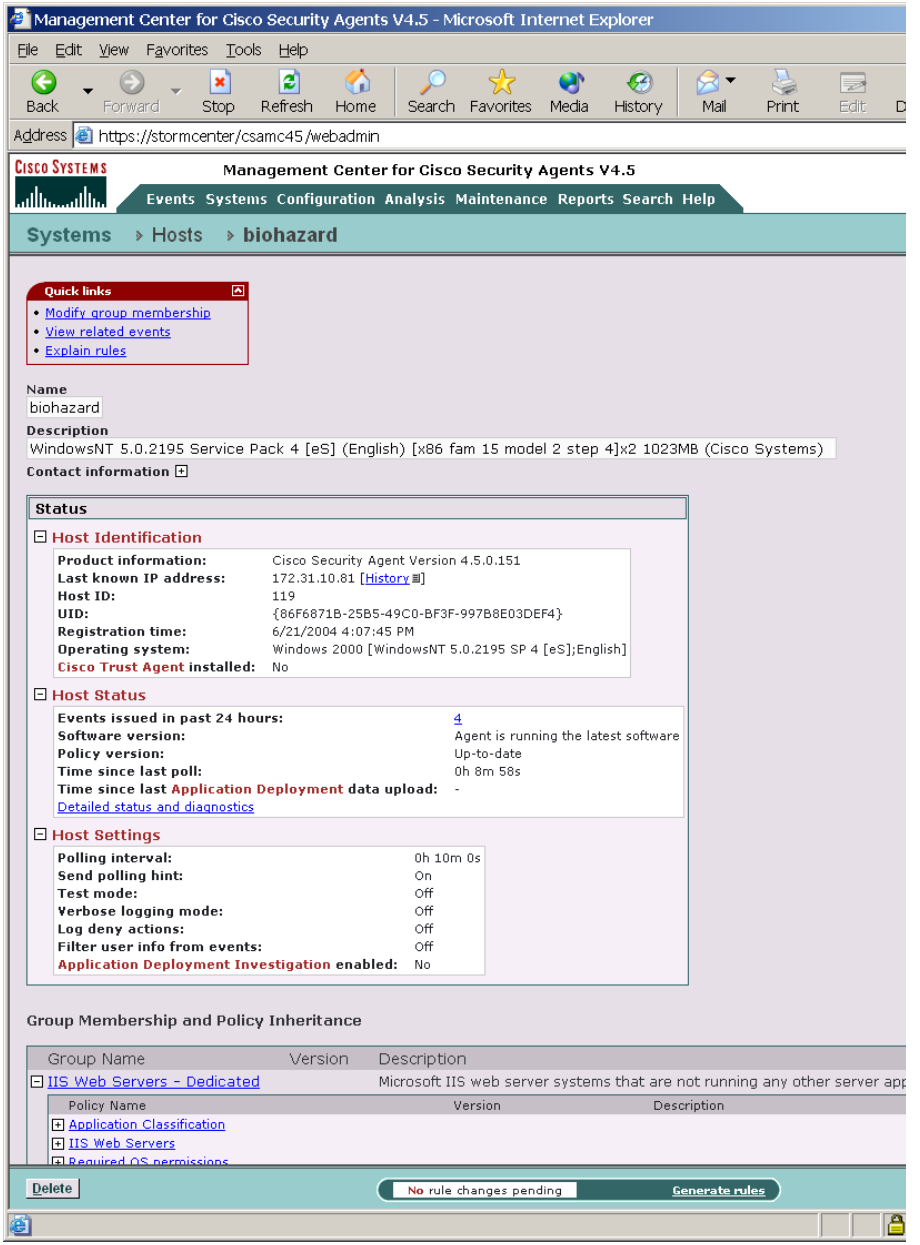
**Step 3** Click the link to a host to view detailed information about that host on the Host Detail page (see Figure 3-8).

From the Host Detail Page you have access to these tasks and information:

- Quick Links Tasks
- Host Name and Description
- Host Identification

- Host Status
- Host Settings
- Group Membership and Policy Inheritance Table
- Combined Policy Rules Table

*Figure 3-8 Host Detail View*



## Quick Links Tasks

- Click the **Modify group membership** link in the Quick Links box on the host detail page (see Figure 3-8) to add or remove this host from a group. See the procedure, Modifying the Group Membership of a Single Host, page 3-32, for the complete procedure.
- Click **View Related Events** to view an event log showing only the events for the host you are looking at.
- CSA MC provides an explanation, in paragraph form, of the policies attached to each host. Clicking the **Explain rules** link takes you to this paragraph explanation.

## Host Name and Description

- Name and Description: These fields are populated with information received from the agent system when it registers. This is the name that identifies this host system on the network. This name does *not* have to be unique. CSA MC assigns each registering host a unique ID number by which the database identifies it.
- Contact Information: Click this link to view any contact information provided to the agent by the user. The available fields for the user are: first name, last name, email, telephone, and location. This user is not required to provide this information, however, if an agent is generating alerts, having this contact information readily available could expedite troubleshooting measures.

## Host Identification

- Product Information—This is the Cisco Security Agent version for this particular machine.
- Last known IP address—This is the IP address of the host. If DHCP addressing is used, this is the last known address of the host.
- Host ID—CSA MC assigns each registering host a unique ID number by which the database identifies it.
- UID—This is a globally unique ID for your agent. It is obtained from the agent kit. Different kits present different IDs. Every host that installs a particular kit will have the same registration ID. Once registered, however, each host receives a unique global ID.

- Registration time—This is the time that the agent registered with CSA MC.
- Operating System—This is the operating system installed on this particular machine. If the operating system is unsupported, this information appears here in red text.
- Cisco Trust Agent installed—This displays whether optional CTA software is installed on the system. If CTA software is installed, this field also displays the current CTA posture status.

## Host Status

- Events issued in the past 24 hours—This is the number of events (rule triggers) that have occurred on the host system in the given time frame.
- Software Version—This is the version of Cisco Security Agent software the system is running. If there is a software update available for this host, this field provides that information. If an update for a host is scheduled but not yet installed, this field provides that information as well.
- Policy version—This field reads “Up-to-date” or “Not up-to-date”, indicating whether the agent has the latest policy configuration from CSA MC.
- Time since last poll—This is the interval since the host system's last polling request.
- Time since last Application Deployment data upload—If application deployment data collection is enabled on the end user system, this indicates the time of the most recent upload of analysis logging data.
- Detailed status and diagnostics—Click this link to view status information for the host in question. The window that is opened by this link uploads information from the agent. NOTE that you may have to click the **Diagnose** button to retrieve the most recent host information. This causes the agent to poll in with status data. You can use this information to diagnose agent issues, to view the current states and policies running on the agent system, and to reset the system default settings (Reset Cisco Security Agent). See The Agent User Interface, page A-10 for more information on the factory default reset option.

**Note** The same Reset Cisco Security Agent functionality is also available from a button located in the footer frame of the Host page. To remotely reset *all* hosts in a group to the system default settings, click the **Reset Cisco Security Agent** button in the footer frame of the Group page. (Note that this reset option is also available locally on the agent system.)

## Host Settings

- Polling interval (seconds)—The value shown here indicates the time interval in which this system polls in to the management server. This feature is configurable through the Groups page.
- Send polling hint—This field indicates if the polling hint capability is turned on for the group in which this host is a member. See Configuring Groups, page 3-3 for details on this setting. This field will display "On (unavailable)" if NAT or PAT exists between CSA MC and the agent - preventing the hint message from being received.
- Test Mode—If this host is part of a group operating in "test mode," that information is displayed here. See Test Mode for further information.
- Verbose logging mode—This field can read as either OFF or ON, indicating whether this feature is enabled for this host. This feature is configurable through the Groups page.
- Log deny actions—This field indicates if the Log <all> deny actions capability is turned on for the group in which this host is a member. See Configuring Groups, page 3-3 for details on this setting.
- Filter user info from events—This field indicates if the Filter user from events capability is turned on for the group in which this host is a member. See Configuring Groups, page 3-3 for details on this setting.
- Application Deployment investigation enabled—This appears if application deployment data collection capability, available from the Analysis menu bar item, is enabled on the end user system. If this feature is enabled, you can access analysis reports from a link on this page. If this feature is not enabled, you can enable it from a link here. (You may have to create a new group in order to enable this feature. You can also do that task from a link that appears here.) See Chapter 11, "Using Cisco Security Agent Analysis" for detailed information on this feature.

## Group Membership and Policy Inheritance Table

The group membership and policy inheritance table provides you with a list of hyperlinks to all the groups the host is a member of, the policies attached to those groups, and the rule modules attached to those policies. From these links you can jump to any of the listed security components to learn more about them.

## Combined Policy Rules Table

This table provides you with a list of all the rules that affect the host. These combined lists are often quite long for any host. You can filter and sort the rules to get a better understanding of how the rules work

# Searching for Hosts

**Step 1** Move the mouse over **Search** in the menu bar and select **Hosts** from the drop-down menu that appears.

**Step 2** In the search field, enter a string to search for. The search will find hostnames containing this string.

**Step 3** Refine your search by selecting one additional radio button from the Host Search Criteria Box. The buttons are explained below:

- **Active hosts with the "the latest" or "an old" configuration**. The search finds hosts that poll into the management server at regular intervals and have not missed three polling intervals. The search will find a host with either the "the latest" policy updates or "an old" policy.
- A**ctive hosts with "software update pending" or "old software."** This search finds hosts that poll into the management server at regular intervals and have not missed three polling intervals. It will find hosts with Cisco Security Agent software updates pending or hosts with old software.
- **Hosts not actively polling (status unknown).** This search finds hosts that have not polled into the management server in at least one hour or that have missed three polling intervals in a row.
- **Hosts that have not polled for** (a specified number) **of days**.

- **Unprotected hosts.** This search finds hosts that do not belong to any group or hosts that belong to groups which have no policies attached.
- **Hosts with unsupported platforms.** An unsupported platform is an operating system not listed in the System Requirements section of the "Installing Management Center for Cisco Security Agents." It is also an operating system running with a service pack not qualified for use with the agent.
- **Hosts with or without Cisco Trust Agent installed.** This search finds hosts on which optional Cisco Trust Agent software is or is not installed.
- **Hosts attached to group.** This search finds hosts attached to the one group you pick from the drop down box.
- **Hosts running in test mode.** Agents on hosts running in test mode do not deny any action or operation even if an associated policy says it should be denied. Instead, the agent allows the action and logs an event if a deny or query rule is triggered. (Read Using Test Mode, page 4-114 for more information about test mode.)
- **Hosts currently using or that have used a particular IP address**.
- **Hosts without Application Deployment Investigation data upload**. This search finds hosts where the Application Deployment Data collection capability is disabled on the end user system.
- **All**. This is the default setting. All the hosts, containing the string searched for, will be found.

**Step 4** Use the **Display Hosts** drop-down list box to display only the hosts of a particular operating system or of all operating systems, if you make no other selection.

**Step 5** In the **Preferences** box, select any of the following check-boxes:

- **Show references box**. This box is checked by default. When you include this in your search criteria, you will be able to look up the group memberships of the hosts you found with the search.
- **Search on description**. If you check the box for this preference, hostnames and description fields are both searched for the string you entered in the search field.
- **Search all other fields**. Select this checkbox to search all database fields (including the description field) for the string value.

**Step 6** Specify how many search results will be displayed on a page in the **Results per page** field.

**Step 7** Click **Find**. If the search finds matches, the hosts are displayed in a list and the search criteria box is collapsed. If the search finds no matches, the message "No Results Found" is displayed under the search criteria.

# Deleting Hosts

Once an agent installs on a host system and registers with CSA MC, that host is not immediately and automatically removed from the CSA MC hosts list if that agent is uninstalled from the system. The host remains in the host list until you manually delete it or until it becomes inactive (has not polled in) for approximately 30 days. Once that 30 days of inactivity time frame has been reached, the Global Event Manager automatically purges the host in question from the hosts list.

## Deleting Hosts Using the Host List Page

Use this procedure to manually delete a host.

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

**Step 2** (Optional) Sort the host list by operating system to find the correct host to delete.

**Step 3** (Optional) Sort the hosts using the hosts statuses in the Architecture drop-down list box to find the correct host to delete.

**Step 4** From the host list page there are two ways to delete hosts.

- Select the checkbox next to the hostname(s) you want to delete and then click **Delete**. When prompted, make sure you are deleting the correct host(s) and click **OK** to delete the host(s).
- From the host list page, click the link to a host. Review the host details (see Figure 3-8) to make sure you are deleting the correct host and then click **Delete**. When prompted, make sure you are deleting the correct host and click **OK** to delete the host.

## Deleting Hosts that Meet a Search Criteria

Use this method to find all the hosts that match a certain criteria and delete them.

**Step 1** Use the procedure "Searching for Hosts" on page 3-28 to find the hosts you want to delete.

**Step 2** Click the checkboxes next to specific hosts to act on those hosts alone, or leave all the boxes unchecked to act on all the hosts found by the search.

**Step 3** Click the **Operations** button at the bottom of the search results list page. (See Figure 3-11 on page 3-38.) The Host Operations Box opens. (See Figure 3-12 on page 3-39)

**Step 4** In the **Available Operations** drop-down list box, select **Delete**.

**Step 5** In the Delete drop-down list box, select either **All hosts matching the current search criteria** or **Selected Hosts**.

**Step 6** Click **Execute**. This function deletes hosts from the local database.

When prompted, click **OK** to perform the operation or **Cancel** not to perform the operation. You receive a message confirming the success or failure of the operation.

# Changing Host Memberships in Groups

When a host registers with CSA MC, it is automatically placed into the group(s) you designate for it. There is no need to add a host to a group initially. You only need to add hosts to groups when you are changing their group designation after they have registered.

Hosts may belong to multiple groups and receive policies that are attached to every group to which they belong. Removing hosts from a group removes the protection the hosts received from the various policies associated with that group.

**Caution** You can add or remove hosts from a group at any time. If you do change host group assignments, the policy configuration of a host that has been moved to another group will not take affect until you generate your rule programs and distribute them. This process is detailed in Generating Rule Programs, page 4-118.

**Note** See Viewing Host Details, page 3-22 for details on hosts.

There are several ways to change the host memberships in a group:

- Modifying the Group Membership of a Single Host
- Modifying the Host Membership in a Single Group
- Bulk Transferring Hosts From One Group to Another
- Modify Groups With Hosts That Meet a Search Criteria

## Modifying the Group Membership of a Single Host

Use this procedure to add a host to, or remove a host from, various groups.

**Step 1** Move the mouse over **Systems** in the menu bar and select **Hosts** from the drop-down menu. This shows you the host list view; it is a list of all the hosts managed by CSA MC.

**Step 2** Click the link for the host whose group membership you want to modify.

**Step 3** Click **Modify group memberships** in the Quick Links box. This takes you to a swap box page containing a list of groups of which the host is **not** a member on the left and a list of groups of which the host **is** a member on the right.

**Step 4** Add or remove your host to groups:

- To add your host to a group, select a group in the left swap box and click the **Add** button. The group now appears in the right swap box with the other groups to which the host belongs.
- To remove your host from a group, select a group in the right box and click the **Remove** button. The group now appears in the left swap box with the other groups to which the host does not belong.

**Step 5** Click the **Generate Rules** link at the bottom of the page. CSA MC updates the group memberships. When a host polls in to CSA MC, it will receive the group membership changes along with updates to any rules it now follows.

**Note** Note: You may want to wait until all your maintenance tasks are performed on CSA MC and then generate rules for all your changes at once.

## Modifying the Host Membership in a Single Group

Use this procedure to add or remove hosts from a single group.

**Step 1** Move the mouse over **Systems** in the menu bar and select **Groups** from the drop-down menu that appears. This shows you the group list view; it is a list of all the groups managed by CSA MC.

**Step 2** From the group list view, click the link for the group to which you want to add or remove hosts. This brings you to that group's edit view.

**Step 3** From the edit view, click the **Modify host membership** link in the Quick Links box. This takes you to a swap box page containing a list of host systems that **are not** members of the group on the left and a list of hosts that **are** members of the group on the right.

**Step 4** Add or remove hosts to this group (see Figure 3-9):

- To add a host to this group, select the host in the left box and click the **Add** button. The host now appears in the right box with the list of all hosts attached to this group. The host is now a members of the group.
- To remove hosts from this group, select the host in the right box and click the **Remove** button. The host now appears in the left box with the list of all hosts unattached to this group. The host is now not a member of this group.

In either case, to select multiple nonsuccessive items in a swap box, hold down the **Ctrl** key as you select each item. To unselect a single item, hold down the Ctrl key while you click on the item in question. Click the **Select all** link beneath the swap box to select all items in the swap box. When you click the Add or Remove button, all selected items are added or removed.

**Step 5** Click the **Generate Rules** link at the bottom of the page. CSA MC updates the group memberships. When a host polls in to CSA MC, it receives the group membership changes along with updates to any rules it now follows.

**Note** Note: You may want to wait until all your maintenance tasks are performed on CSA MC and then generate rules for all your changes at once.

## Bulk Transferring Hosts From One Group to Another

Use the bulk transfer feature to easily move or copy all hosts from one group into the Group you are currently viewing.

**Step 1** Move the mouse over **Systems** in the menu bar and select **Groups** from the drop-down menu that appears. This shows you the group list view; it is a list of all the groups managed by CSA MC.

**Step 2** From the group list view, click the link for the group to which you want to add or remove hosts. This brings you to that group's edit view.

**Step 3** From the edit view, click the **Modify host membership** link in the Quick Links box. This takes you to a swap box page containing a list of host systems that **are not** members of the group on the left, and a list of hosts that **are** members of the group on the right.

The bulk transfer operations are at the bottom of this page. (See Figure 3-9.)

**Step 4** In the Bulk Transfer box, select **Move** or **Copy** in the first drop-down list box to move hosts or copy hosts, from the group you specify to the group whose membership your are modifying.

**Step 5** In the second drop-down list box, select the group whose members will be moved out of or copied to the group whose membership you are modifying.

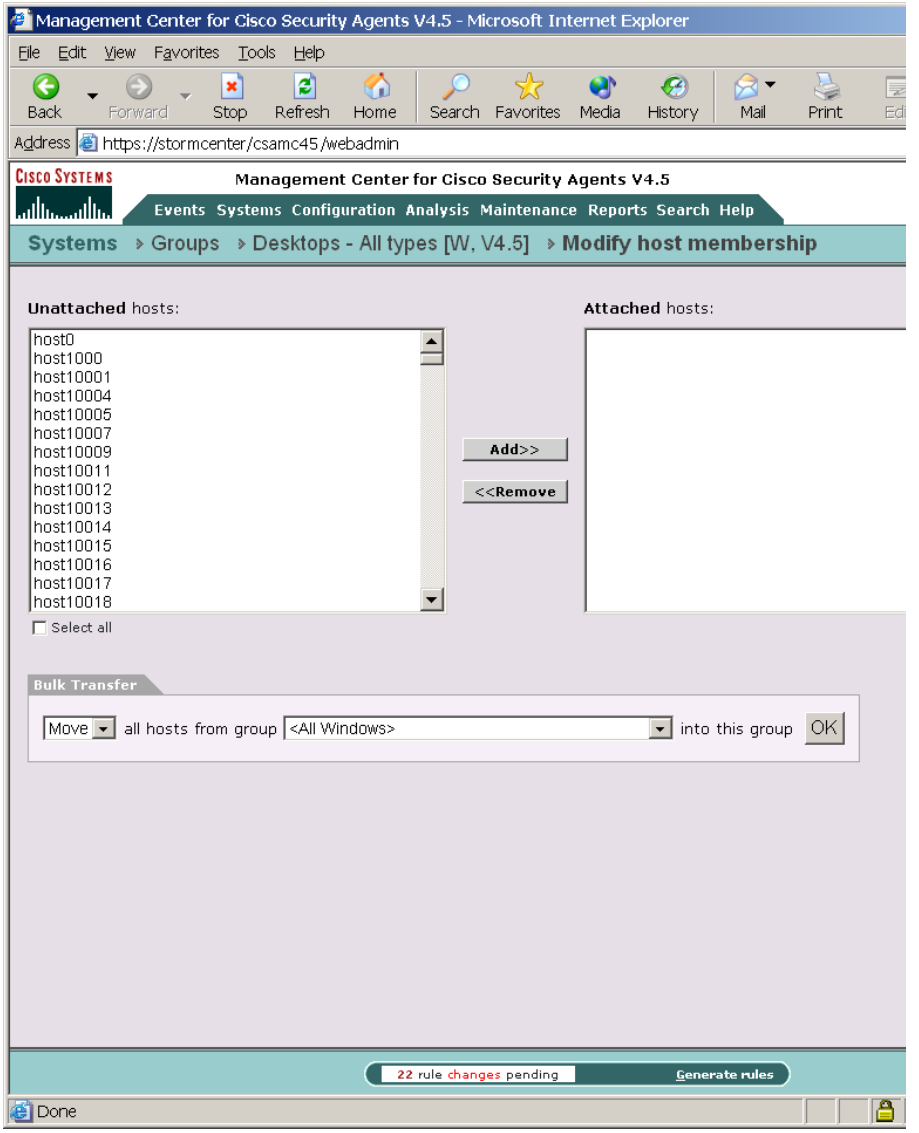
**Step 6** Click **OK**. The hosts you moved or copied now appear in the right swab box with the list of hosts attached to this group. The hosts you moved or copied are now members of the group.

**Step 7** Click the **Generate Rules** link at the bottom of the page. CSA MC updates the group memberships and when a host polls in to CSA MC, it receives the group membership changes along with updates to any rules it now follows.

**Note** Note: You may want to wait until all your maintenance tasks are performed on CSA MC and then generate rules for all your changes at once.

When you next click the **Generate** button, policies associated with this group will no longer be applied to the removed hosts. (The host is not deleted from the database, it is just no longer part of the group.)

*Figure 3-9 Add Hosts to Group*



## Modify Groups With Hosts That Meet a Search Criteria

Use this method to find all the hosts that match a certain criteria and move them in and out of groups.

**Step 1** Use the procedure "Searching for Hosts" on page 3-28 to find the hosts whose group memberships you want to change.

**Step 2** Click the checkboxes next to specific hosts to act on those hosts alone, or leave all the boxes unchecked to act on all the hosts found by the search.

**Step 3** Click the **Operations** button at the bottom of the search results list page. (See Figure 3-11 on page 3-38.) The Host Operations Box opens. (See Figure 3-12 on page 3-39)

**Step 4** In the Available Operations drop-down list box, select one of the following options:

- **Delete**. This function deletes hosts from the local database. In the Delete drop-down list box, select either **All hosts matching the current search criteria** or **Selected Hosts**.
- **Attach to group**. This function copies hosts from one group to another.
  - In the Attach (if applicable) drop-down list box, select either **All hosts matching the current search criteria** or **Selected Hosts**.
  - In the **to the following group** drop-down list box, select the group to which you want to add the hosts.
- **Detach from group**. This function removes hosts from a group.
  - In the Detach (if applicable) drop-down list box, select either **All hosts matching the current search criteria** or **Selected Hosts**.
  - In the **from the following group** drop down list-box, select the group from which you want to remove the hosts.

**Step 5** Click **Execute**.

**Step 6** When prompted, click **OK** to perform the operation or **Cancel** not to perform the operation. You receive a message confirming the success or failure of the operation.

*Figure 3-10 Host Search Page*

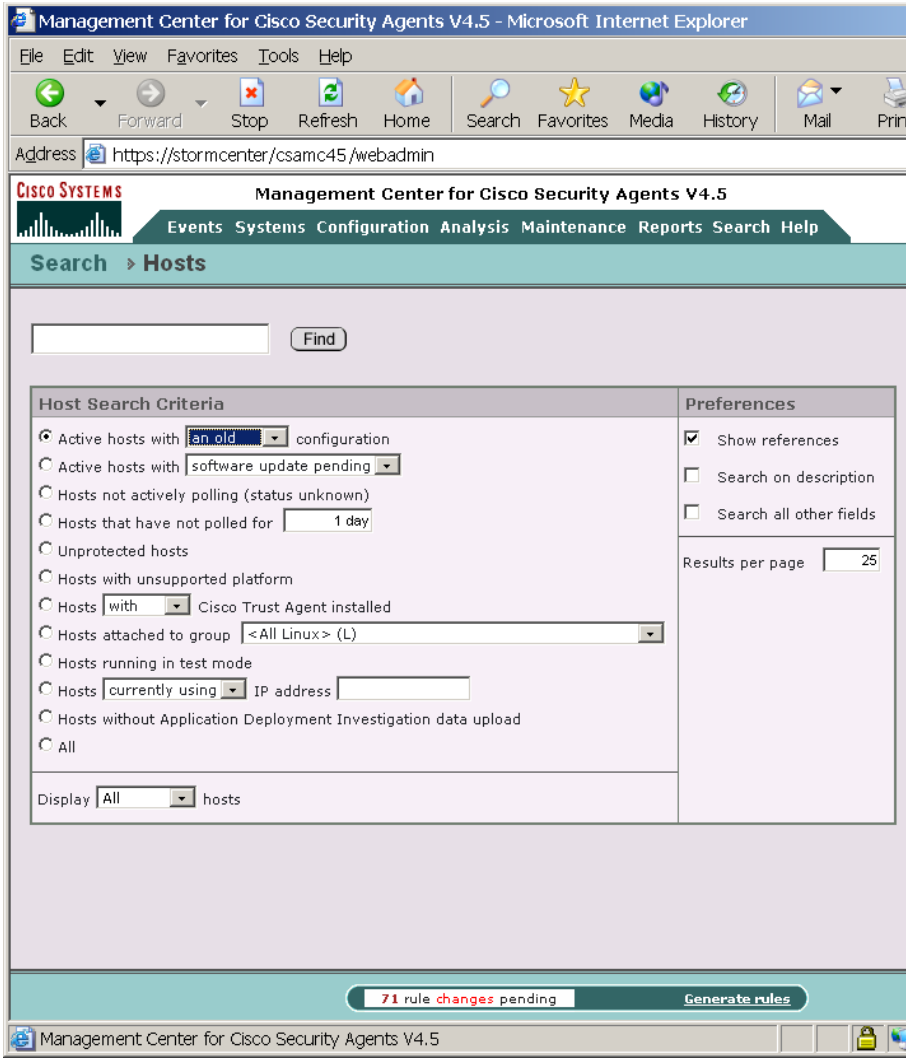


*Figure 3-11 Hosts List Page*

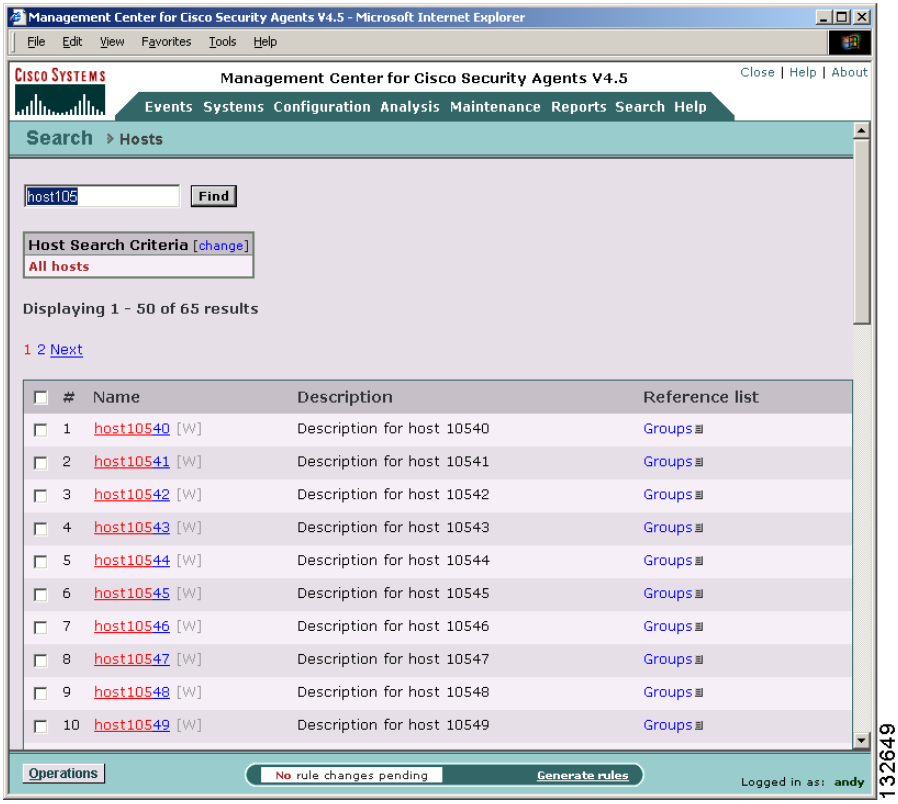
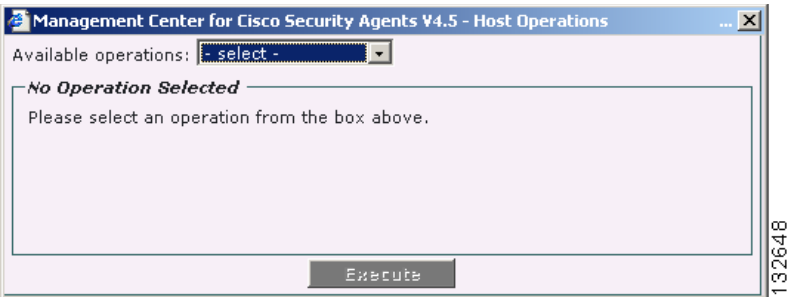


*Figure 3-12 Host Operations Box*




# Distributing Software Updates

Cisco provides software updates via its web site (www.cisco.com) for both CSA MC and the agent. You can download these updates, install them on CSA MC, and then distribute them to agent systems across your network as easily as you deploy new rule programs. When you download a self-extracting executable update and install it on the server system, the agent software update files get placed under **Available Software Updates** in CSA MC (accessible from **Systems>Software Updates** in the menu bar).

From the list of available updates that is created in the Available Software Updates page, you can make the appropriate updates available to agents through the Scheduled Software Updates page. Creating Scheduled Software Updates allows you to distribute updates to designated groups of agent systems. See Configuring Scheduled Software Updates, page 3-41 for details.

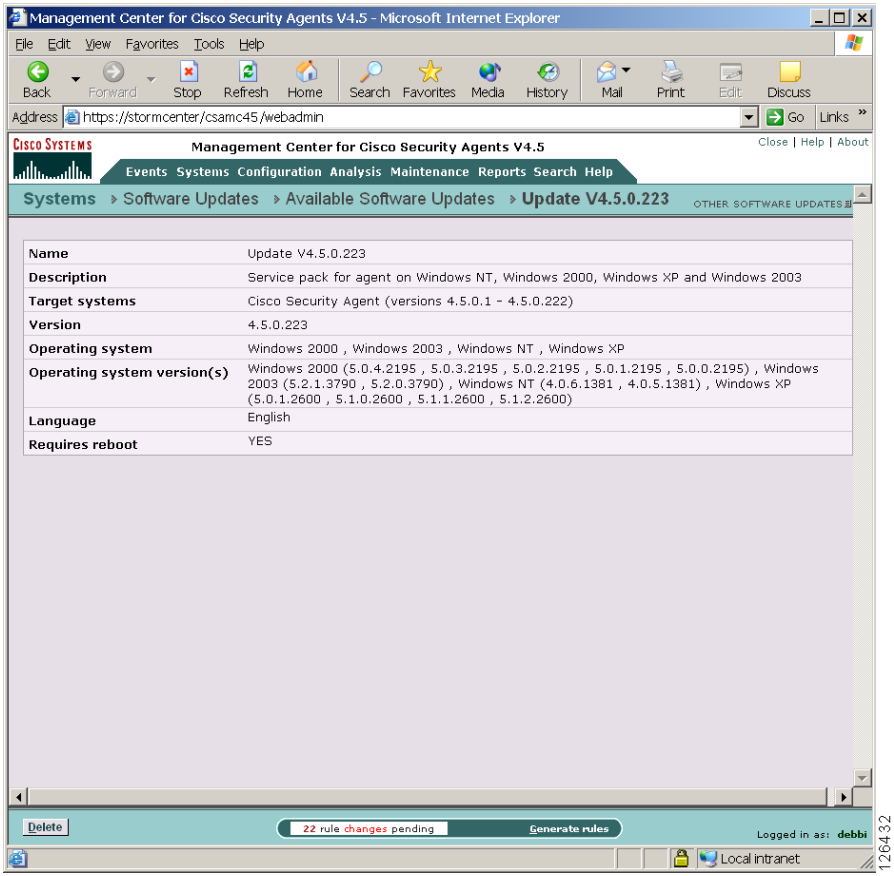
**Note** All "Quiet" Windows and Linux updates begin installing automatically during the designated installation window with no action occurring on the part of the end user.

From the Available Software Updates page, you can click on a particular update and view the following information (see Figure 3-13):

- Name of the software update, for example SP 4.5.0.58
- Description of the software update, for example Service Pack for agent on NT and Win2K

- File, a link to the software update file itself on the server system
- Target system, a description of the system type for which the update is issued (agent and/or server)
- Version, this is the version of the software update
- Operating system, the operating system for which the update is issued
- Operating system version(s), the exact OS version numbers for which the update is issued

***Figure 3-13 Available Software Updates Page***



# Configuring Scheduled Software Updates

Create Scheduled Software Updates to distribute an update or updates you have available in Available Software Updates to a selected group or groups.

To create Scheduled Software Update for distribution to agent systems, do the following.

**Step 1** From the menu bar **Systems** drop-down list, move the mouse over **Software Updates**. A cascading menu with further selections appears. Select **Scheduled Software Updates** (see Figure 3-14).

**Step 2** Click the **New** button to create a new entry. This takes you to the update configuration page.

**Step 3** Enter a **Name** for the update that makes it easily identifiable.

**Step 4** Enter a **Description**. This is a useful line of text that is displayed in the list view and helps you to identify this particular configuration.

**Step 5** Select the **Target operating system** for the update you're distributing (Solaris, Linux, or Windows). When you select an OS, the available updates and selectable groups change accordingly.

**Step 6** From the **Software update** pulldown list, select the Solaris, Linux, or Windows update you want to distribute. Generally, it's called something like Update V4.5.0.52.

**Step 7** **Enable update for hosts in selected groups** From the available list of groups, select one or more to distribute this update to.

**Step 8** To select multiple items in a list box, hold down the Ctrl key as you select each item. To unselect a single item, hold down the Ctrl key when you click on the item in question. Press the Shift key to select multiple successive items.

**Step 9** **Update time** Enter a time frame during which agent systems can receive and install updates. By default, the time frame is set to "any time" or for 24 hours. This way, users will update at any time you choose. If you put a time limit on the update, for example enter 10:00 to 11:00 (this would be AM), then after 11:00, if the user is not logged in during this hour window, the update would not be available again until the same time the next day.

**Step 10** “Quiet install” updates begin installing automatically with no action occurring on the part of the end user. A reboot on the agent system is not required after a software update. Security continues to be enforced after an update, but if the

system is not rebooted, configuration changes and other changes are not applied. They are only applied on the next reboot. You can control what the end user sees during an update and whether a reboot is required after an update by using the following checkboxes.

- **Force reboot after install** (available for Windows and Linux): If you select this checkbox, when the update completes, a message appears to the end user warning that the system will automatically reboot in 5 minutes. This reboot cannot be stopped by the end user. Keep in mind, if you are selecting to force a reboot, the update must also be "Quiet". Therefore, regardless if the end user is present or not, if the machine is running and a quiet update with a forced reboot is received, both the install and the automatic reboot take place within the time frame specified in the update. (Generally, you will only want to use a quiet install with a forced reboot for an unattended server so that the update is installed and the system is rebooted without a user having to be present at the server.)
- **Quiet install** (available for Windows and Linux): If you select this checkbox, when the update completes, no prompt is displayed to the user. Therefore, since the update begins without prompting the user, this quiet install update occurs as a completely transparent process. The user does not know that a software update has occurred. Configuration changes provided in the update will take effect when the system is next rebooted.
- Noisy install (implied by no checkbox selection): If you do not select the Quiet install checkbox, and the end user has an agent UI, the end user is prompted that an update is available. The user can start the update at that time or postpone it.

**Note** Software update functionality and prompt options occur regardless of Agent UI configurations on the end user system. Therefore, if you have deployed agents with no UI, you can deploy "noisy" software updates that prompt the end user. These functions are independent of each other. So, if you want all agent functions to be invisible to the end user, you should configure your update accordingly. (Note that there is one exception to this statement. If the end user does not have an agent UI and you deploy a "noisy" update, the option to postpone the update will not appear. The update will behave as though it were "quiet.")

These possible checkbox options would be combined for the following effects once the software update has completed:

*Table 3-1 Software Update Reboot/Install Options*

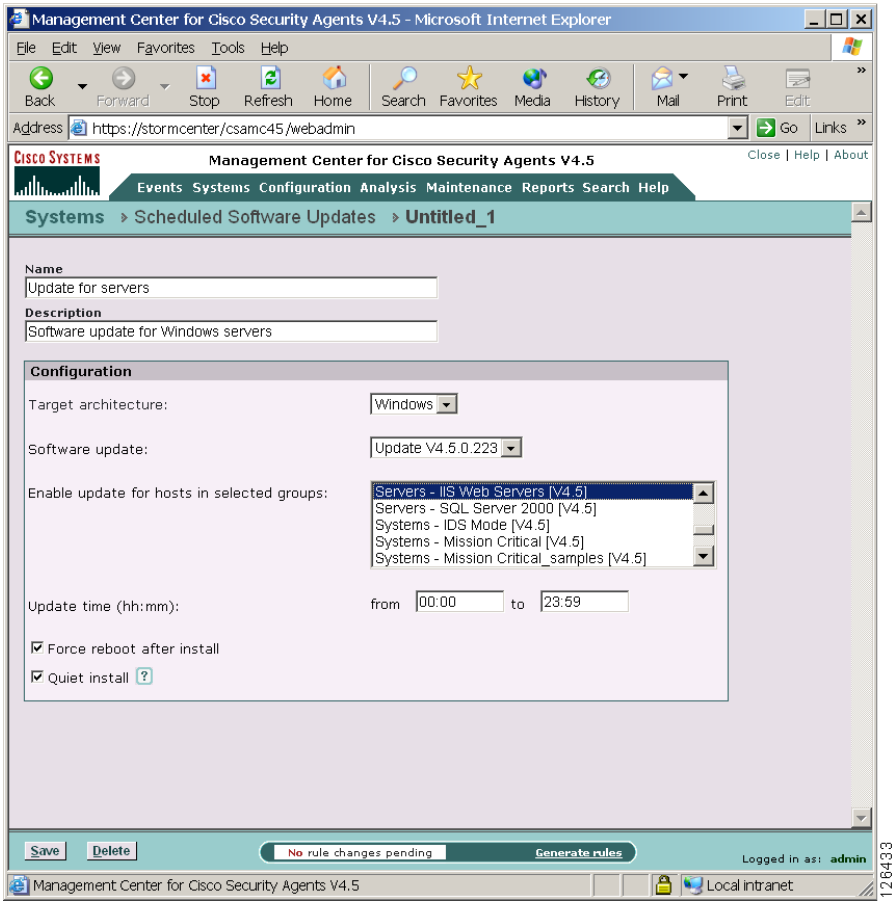
| | |
|---|---|
| Force reboot checkbox=enabled<br>Quiet install checkbox=enabled | The install ends by displaying a prompt indicating that a reboot will occur within 5 minutes. (This combination is recommended for unattended servers.) |
| Force reboot checkbox=disabled<br>Quiet install checkbox=enabled | The install ends quietly with no prompts. Therefore, the update is completely transparent to the end user. The update takes effect the next time the user happens to reboot. |
| Force reboot checkbox=disabled<br>Quiet install checkbox=disabled | The install prompts the user that an update is available. The user can update at that time or postpone the update. When the update occurs, the install ends by displaying a prompt indicating that an update has occurred and the end user can reboot the system at his/her convenience to apply the changes. |

**Step 11** Click the **Save** button.

You must Generate rules to deploy software updates to agents.

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

*Figure 3-14 Scheduled Software Updates Page*




The next time agents poll in to CSA MC, they receive a prompt informing them that a software updated is available.

On Solaris agent systems, use the `csactl` utility to check for software updates and to install them. See Appendix A, "Cisco Security Agent Overview" for details.

# Software Updates in a Distributed Configuration

There are two procedural items to note when installing a software update in a distributed installation environment with multiple MC's.

- In a distributed environment, you *must* install the software update on *all* MC's in your distributed configuration.
- In a distributed environment, when installing, upgrading, or uninstalling any MC in the distributed configuration, the service must be stopped on the other MCs. For example, in a configuration with 2 MCs, you *must* first *stop* the CiscoWorks Daemon Manager (`net stop crmdmgtd`) on one MC before you install the software update on the other MC.

CHAPTER 4

# Building Policies

## Overview

The policies you create on the Management Center for Cisco Security Agents should reflect a well-planned, enterprise-wide security policy. If your corporate enterprise already has security guidelines in place, the rules that form your policies should reflect those guidelines.

It is important that you spend time charting out your security needs in advance rather than attempting to backfill holes as they are discovered. Because both networks and network security are dynamic entities, it is expected that you will need to adjust policies to meet the changing and growing needs of your enterprise. A well thought-out security plan is certain to save you time in the end.

This section contains the following topics.


- Developing a Security Policy, page 4-3
- About Rules, page 4-6
- Combining Policies, page 4-7
- Policy Components, page 4-9
- Rules: Action Options and Precedence, page 4-9
- Rules: Action Definitions, page 4-10
- Rules: Manipulating Precedence, page 4-13
- Monitoring Access, page 4-14
- Querying the User, page 4-15
- Caching Responses, page 4-18

- Building Policies and Rule Modules, page 4-19
- Configure a Policy, page 4-19
- Configuring Rule Modules, page 4-22
- Setting State Conditions, page 4-24
- System State Sets, page 4-25
- User State Sets, page 4-30
- Adding Rules to a Rule Module, page 4-32
- Filtering the Rules Display, page 4-36
- Copying Rules between Modules, page 4-36
- Comparing Configurations, page 4-39
- Merging or Copying Rule Modules, page 4-41
- View Change History, page 4-41
- Explanation of Rules, page 4-42
- Rules Common to Windows and UNIX, page 4-44
- Agent Service Control, page 4-44
- Agent UI Control, page 4-48
- Application Control, page 4-52
- Connection Rate Limit, page 4-56
- Data Access Control, page 4-60
- File Access Control, page 4-64
- Network Access Control, page 4-69
- Windows Only Rules, page 4-74
- Clipboard Access Control, page 4-74
- COM Component Access Control, page 4-76
- File Version Control, page 4-79
- Kernel Protection, page 4-84
- NT Event Log, page 4-87
- Registry Access Control, page 4-90
- Service Restart, page 4-93

- Sniffer and Protocol Detection, page 4-96
- UNIX Only Rules, page 4-99
- Network Interface Control, page 4-99
- Resource Access Control, page 4-102
- Rootkit / kernel Protection, page 4-104
- Syslog Control, page 4-107
- Attaching Rule Modules to Policies, page 4-111
- Attaching Policies to Groups, page 4-112
- Using Test Mode, page 4-114
- Generating Rule Programs, page 4-118


# Developing a Security Policy

If you are crafting your own policies, please refer to Chapter 12, "Policy Definition Guidelines," for information.

**Caution** To maintain the integrity of the preconfigured policies shipped with CSA MC, it is recommended that you do not change them. If you are using preconfigured policies but want to edit them slightly due to your own site's needs, you should instead clone the policy in question or create a new policy and add it to the group. Note that each pre-configured rule, rule module, policy, and group page has data in the expandable **+Detailed** description field explaining the item in question. Read the information in these fields to learn about the items described and to determine if the item in question meets your needs for usage.

A corporate security policy should temper business concerns with security concerns. It should allow the user community to access required resources, while protecting that community from the dangers those resources can introduce. To achieve this goal, it is crucial to have a carefully planned network security policy in place to safeguard valuable organizational resources and information.

Before configuring your policies, it is important to understand exactly what network resources and services you want to protect and what threats you are most concerned about. The first step in planning a security policy is identifying the

resources your user community requires to do business. That could include specific applications, protocols, network servers and web servers. Collect this information and use it to design the main features of your policy.

## Providing Safe Access to Required Resources

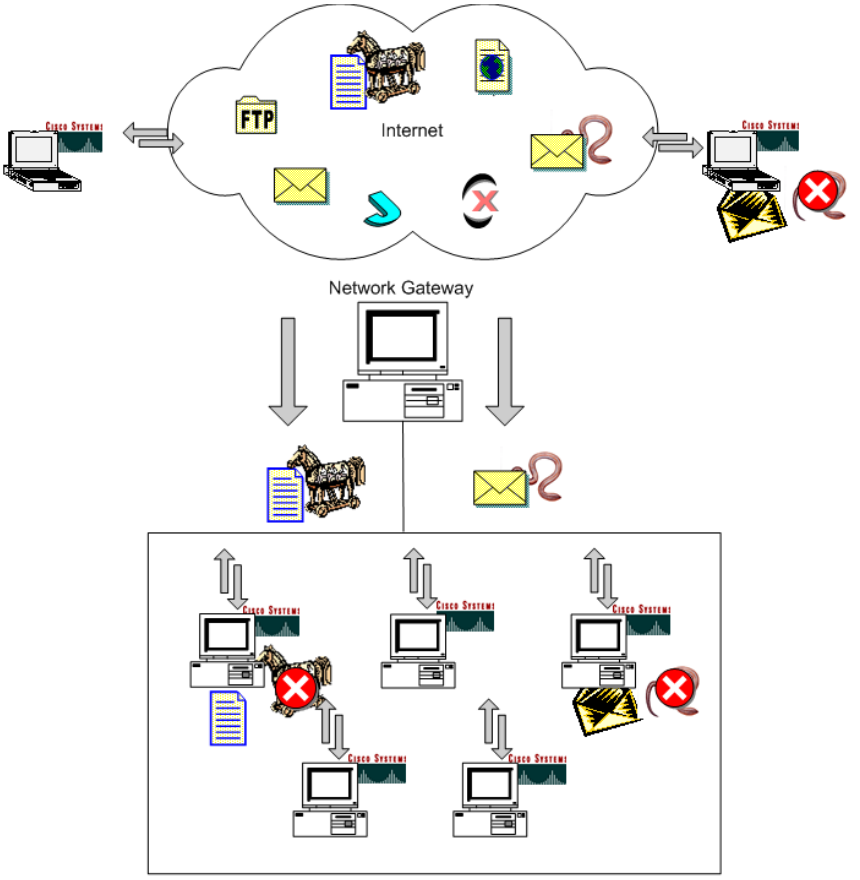
As you determine the network resources that are required by your user community, you can identify some of the threats posed against those resources. For example, while putting together a security plan, you might find it beneficial to limit access to some resources based on various parameters such as traffic direction and allowed file types.

Upon examining past breaches of security, you could determine that email attachments and Internet file downloads pose the greatest threat to your network. In this case, you would want to develop policies to diminish the danger of accessing these particular resources. Your security plan should then incorporate policies for commonly used services such as Web, email, and instant messengers.

You could take a couple of approaches to enforcing your security plan depending upon the immediacy of any perceived threats and your basic corporate philosophy toward security. Both approaches are equally valid. On the one hand, you might choose to allow most activities and selectively add targeted restrictions. This would be a more permissive security model. This approach facilitates uptime, but may be less secure. Conversely, you could decide to shut everything down and then slowly add targeted permissions. This approach is far more restrictive and some legitimate requests could be rejected, but this may be suitable for highly secured environments. You could use both approaches for different groups.

As your security plan evolves, you can refine your policies, making them more or less granular to keep pace with your user community's needs. Your network system security depends on your implementing security policies carefully, and checking to see that they work as intended.

*Figure 4-1 Protecting Information*




Formulate a policy to protect systems from common email worms and Trojans. Once these attacks infiltrate your network and propagate to the user community, a well-defined policy can identify errant system actions and stop an attack before it can damage mission-critical information.

126461

# About Rules

Rules are the foundation of your security policies. CSA MC lets you create several rule types. Each rule type requires you to enter varying combinations of information using a specific syntax. Most Policies and Rule Modules use a combination of *Enforce* and *Detect* rules. Enforce rules are primarily access control rules that allow, deny, or terminate a process. Detect rules are monitoring, and tagging rules. In rule display lists, enforce rules are shown at the top of the list and detect rules are shown at the bottom. These rule types work together to monitor actions, build application classes, and protect systems.

For example, the following basic *enforcement* rules require information as follows:

Use file access control rules to allow or deny what operations(read, write) selected applications can perform on files and directories according to:

- the action you are allowing or denying
- the application attempting to access the resource
- the operation (read, write) attempting to act on the file or directory

Use network access control rules to control access to specified network services according to:

- the action you are allowing or denying
- the application attempting to access the service or address
- the direction (client, server, listener) of the communication
- the service a system is attempting to use
- the address a system is attempting to communicate with

Use registry access control rules (Windows only) to allow or deny selected applications from writing to specified registry keys according to:

- the action you are allowing or denying
- the application attempting to write to the registry keys and values
- the modification of Key/Value pairs

Use COM component access control rules (Windows only) to allow or deny selected applications from accessing specified COM components according to:

- the action you are allowing or denying

- the application accessing the COM component

Other types of enforcement rules shipped with CSA MC provide event correlation and heuristic features which can be enabled on a per group basis, like portscan detection, SYN flood protection, the prevention of predictable TCP sequence numbers, and the blocking of malformed IP packets. (These features are located on the Network shield rule page.) This is especially useful for network servers. (See Chapter 5, "Using System Correlation Rules" for more information.)

The following basic *detection rules* work as follows:

Use various tagging rule types with "Add process to application class" or "Remove process from application class" selected to build application classes based on process behavior rather than executable name. Once applications are built or "tagged" they are used in other enforcement rules.

Use rules such as NT Event log and Sniffer and protocol detection to log designated event types when they occur.

By tying together the controlling and monitoring of various system functions and by operating under the direction of assigned policy rules, agents provide overall system protection,

# Combining Policies

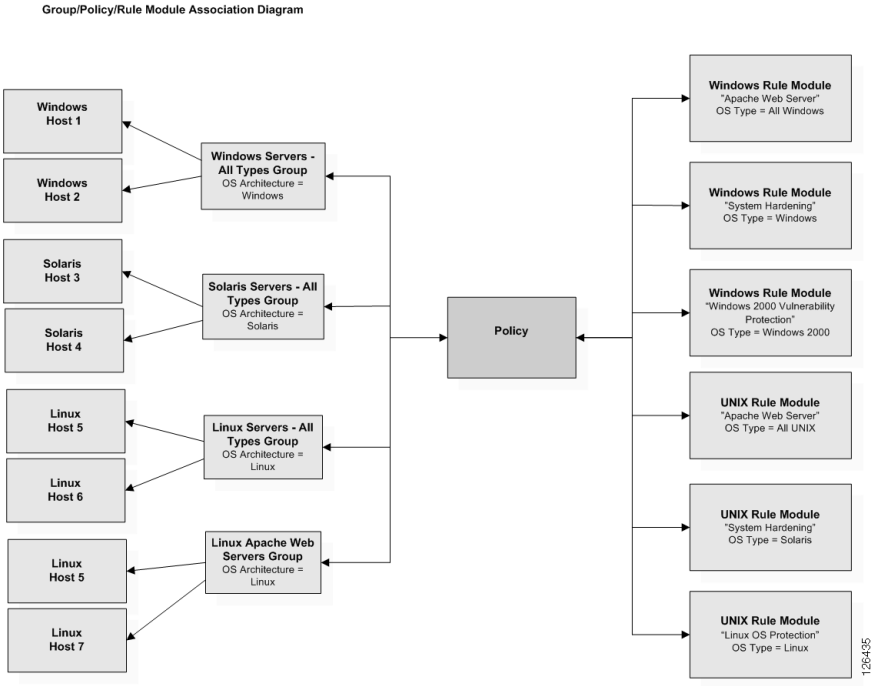
You can attach multiple rule modules to single policies and you can attach multiple policies to a single group. Moreover, a host can belong to multiple groups and inherit policies from all of them. For example, a desktop can belong to the Desktop-All types group and inherit the Systems-Test Mode policy. It can also belong to the All group through which it receives the Remote Systems Policy.

When more than one policy is associated with a host, the rules modules in the individual policies are merged as though they were all defined within a single policy. In particular, the rules in the policy are ordered in the same sequence as they would be within a single module. See the section on Rules: Action Options and Precedence, page 4-9 for priority order information.

Figure 4-2 displays the relationship between host, group, policy, and rule module configuration items. In the diagram, you can see that the policy level is the common ground by which host groups acquire the rules that make up their security policy.

**Note** You can view merged policy rules at both the group and host levels.

*Figure 4-2 Host, Group, Policy, Rule Module Associations*



# Policy Components

The following sections describe the various components you must configure as part of rules modules that will form your policies.

## Rules: Action Options and Precedence

When you configure certain rule types, you select an action for that rule (allow, deny, etc.). When you add your rule modules to policies, CSA MC orders individual rules from multiple modules according to action, in the following manner within each policy.

| | |
|---|---|
| Priority 1 | High Priority Terminate Process |
| Priority 2 | High Priority Deny |
| Priority 3 | Allow |
| Priority 4 | Query User (Default Terminate) |
| Priority 5 | Query User (Default Deny) |
| Priority 6 | Query User (Default Allow) |
| Priority 7 | Terminate Process |
| Priority 8 | Deny |
| Priority 9 | Default Action (Allow) |
| Priority 10 | Add process to application class |
| Priority 11 | Remove process from application class |
| Priority 12 | Monitor |

The priority listings beside each item indicate the manner in which CSA processes rules. All priority 1 enforcement rules (High Priority Terminate Process) are checked first and priority 8 enforcement rules (Deny) are checked last and that is only if no other higher priority rules have already been triggered by a system action. Detection rules, such as priority 12 Monitor rules, are always checked, even in the presence of a higher priority enforcement rule which governs the same resources triggering first.

**Note** The default action of the agent is to allow an operation (priority 9 in the previous table) in the absence of any applicable rule. An exception to this occurs when attempts are made to modify the Cisco Security Agent resources. Due to agent self-protection, these requests are denied by default.

# Rules: Action Definitions

When you configure your access control rules, you must select an action for that rule. The following is a description of all possible action types. You should note that not all action types are available for all rules.

*Enforcement Actions*

- **High Priority Terminate Process**—Select this action type to create a terminate rule that takes precedence over all other allow, terminate, deny, and query rules. This action denies the application access to the resource in question and also attempts to terminate the application process. Under the same circumstances, if the terminate is not high priority and a conflicting allow rule exists in the same policy, the allow takes precedence. Note that all processes cannot be safely terminated (e.g. winlogon). If it is not safe to terminate the process, the action will be denied but not terminated.
- **High Priority Deny**—Select this action type to create a deny rule that takes precedence over all other allow, deny, and query rules. For example, if you configure an allow rule that conflicts with this high priority deny, the high priority deny always takes precedence. Under the same circumstances, if the deny is not high priority and a conflicting allow rule exists in the same policy, the allow takes precedence.
- **Allow**—Select this action type to create a rule that allows the action you specify to take place. Because the default action of all rules is "allow", generally, you'll only want to configure allow rules as exceptions to existing deny rules within policies.
- **Query User (Default Terminate)**—Select this action type to prompt the user when the action you indicate occurs. The user then has 5 minutes to answer Yes, No, or Terminate. By default, it will be denied and the process will be terminated unless the user decides otherwise. See Query User for more details. (Query User options are not available for Solaris rules.)

- **Query User (Default Deny)**—Select this action type to prompt the user when the action you indicate occurs. The user then has 5 minutes to answer Yes, No, or Terminate. By default, it will be denied unless the user decides otherwise. See Query User for more details. (Query User options are not available for Solaris rules.)
- **Query User (Default Allow)**—Select this action type to prompt the user when the action you indicate occurs. The user then has 5 minutes to answer Yes, No, or Terminate. By default, it will be allowed unless the user decides otherwise. See Query User for more details. (Query User options are not available for Solaris rules.)

  **Text used to query user**—If you are configuring a Query User rule, you must also configure query settings. The text you type into the query settings field is the same text that will appear in the Query User pop-up box to explain what is occurring on the system to the user.
- **Terminate Process**—This action denies the application access to the resource in question and also attempts to terminate the application process. Note that all processes cannot be safely terminated (e.g. winlogon). If it is not safe to terminate the process, the action will be denied but the process will not be terminated.
- **Deny**—Select this action type to create a rule that stops the action you specify from occurring on systems. (When you select Deny for this rule, if the user attempts to run the application in question, he/she is notified with a pop-up box explaining that the application is forbidden to run.)

*Detection Actions*

Note that Detection rules, such as priority 12 Monitor rules, are always checked, even in the presence of a higher priority enforcement rule which governs the same resources triggering first.

- **Add process to application class**—Use this for defining dynamic application classes. A dynamic application class is built based on an application's behavior rather than by a specific application executable name. A process will be added to a dynamic class when the parameters of the rule (allow, deny, terminate) that dictate access to a resource are met. See Chapter 6, "Using Application Classes" for details.
- **Remove process from application class**—Use this action type to remove a dynamic application tag from a process. A process will be removed from a dynamic class when the parameters of the rule (allow, deny, terminate) that dictate access to a resource are met.

**Note** Dynamic classifications are part of an application class when they are running on the system. When the process stops running, the CSA MC application classification for that process also ends. Should the process begin again, it may or may not fall into the same application class depending on the process's behavior and on the definition of the application class. Therefore, all dynamic application classifications are ephemeral and are constantly being re-evaluated and classified on the system.

**Note** All rules are evaluated before any dynamic application classifications are applied to processes. This ensures that application class memberships are consistently applied for all rules being evaluated for a given request.

- **Monitor**—Most rule types provide a "Monitor" action. You may want to write monitor rules to produce events for certain resource accesses without having to write an explicit allow or deny rule about that resource. You can also write monitor rules in the presence of other similar rules dictating the availability (allow, deny, etc.) of a resource. For example, you can write a monitor rule for a resource and if the monitor rule is triggered, any subsequent rules about the resource in question will trigger as well. This allows you to configure general alerts about resources regardless if the resource access action is an allow or a deny.

For every rule module you configure, the default action of that rule is Allow. All rule modules allow all system actions until you write a rule denying a specific action. Following that logic, it is unlikely that you would write allow rules unless they are to make exceptions to deny rules you are writing within a module or for monitoring purposes (see Monitoring Access, page 4-14). If you do write a stand-alone allow rule, because the default action is allow, the allow rule itself is then essentially irrelevant.

A good model for configuring rules within modules would be to take the priority levels into account and work from the bottom up, lowest priority to highest priority. Before you even add a single parameter to a rule, by default, it allows all system actions. First, write a deny rule and then if you want to make any exceptions to that particular deny, write an allow rule. Next consider using query rules for access controls that allowing the user to decide if an action should be allowed or denied. Lastly write any high priority rules you might need.

# Rules: Manipulating Precedence

In addition to using the selected "action" type to order rules within a policy, CSA MC uses the selected logging type as a way to suborder similar rules within a policy. Logging automatically takes precedence over disabled logging if the action type is the same for multiple rules in a policy. Therefore, for rules of a given priority, e.g. Allow, a Log rule will be evaluated before a No Log rule.

For most policies, this automatic ordering and subordering of rules provides the desired effect when policies are combined and deployed. However, there are cases when the CSA MC ordering scheme causes policies to behave in an undesired manner. For this reason, most rule types provide a checkbox that allows you to manipulate how similar rule types are subordered within a policy. This checkbox, called **Take precedence over other <similar action> rules**, is located in the rule configuration page. A rule with this precedence checkbox selected is evaluated before similar rules that do not have this checkbox selected.

Here is an example of two rules within the same policy which do not behave as expected due to automatic rule ordering. There are two Network access control rules in the same policy as follows:

- Log, Deny, All applications, acting as a server, for TCP/1-65000
- No Log, Deny, All applications, acting as a server, for TCP/1900

The rule that involves connections on TCP/1900 would be denied and logged despite the fact that logging is not selected for that rule. This is because the rule involving connections on TCP/1-65000 would be evaluated within the policy first and connections made on TCP/1900 would go to the event log even though the rule did not have logging selected.

In this example, using the **Take precedence over other <action> rules** checkbox in the TCP/1900 rule would allow you to designate its precedence as higher than other deny rules in the policy, giving you the ability to suppress log messages for actions you want to be denied but for which you do not want to be continually notified due to another rule within the policy.

**Caution** The **Take precedence over other <action> rules** checkbox is a rule ordering tool you should rarely need. In most cases, the CSA MC automatic ordering of rules is sufficient. But if you are using this checkbox to manipulate rule ordering, you

should understand the following rule order scheme. Within a given policy, rules are sorted using this criteria:
* Action type
* Precedence checkbox On/Off
* Log checkbox On/Off

**Note** For a given policy, if you have multiple rules of the same action type, the same logging type, and the same "take precedence" type, the ordering of these rules is inconsequential within the policy because there is no differential criteria by which to order them.

# Monitoring Access

Most rule types provide a “Monitor” action. You may want to write monitor rules to produce events for certain resource accesses without having to write an explicit allow or deny rule about that resource. You can also write monitor rules in the presence of other similar rules dictating the availability (allow, deny, etc.) of a resource. For example, you can write a monitor rule for a resource and if the monitor rule is triggered, any subsequent rules about the resource in question will trigger as well. This allows you to configure general alerts about resources regardless whether the resource access action is an allow or a deny.

## Making a Policy Mandatory

CSA MC provides three auto-enrollment architectural groups (Windows, Solaris, Linux) that are mandatory for all hosts of a given OS architecture. By providing group auto-enrollment for hosts, any policies you attach to these groups also become mandatory by association. You might want to use these mandatory groups to apply policies which prevent some critical service from being inadvertently banned. For example, you could attach policies to prevent DNS or DHCP from being disabled by an overly restrictive rule.

# Querying the User

When you create access control rules, beyond simply allowing or denying a specific action, you can select to query the user when an action triggers the rule in question. The user can then decide to allow the action, deny it, or terminate the process at that time. When you select to query the user, you are also crafting explanation text to display to the user and whether to allow, deny, or terminate the action by default if the query is not answered within 5 minutes. If the user is not logged in to the system, the default action is taken immediately.

Query configurations are a Variable setting which allows you to decide which radio button options are displayed in the pop-up query box, which action is the default, whether the answer given by the user is to be remembered, and what the query text to be displayed will be.

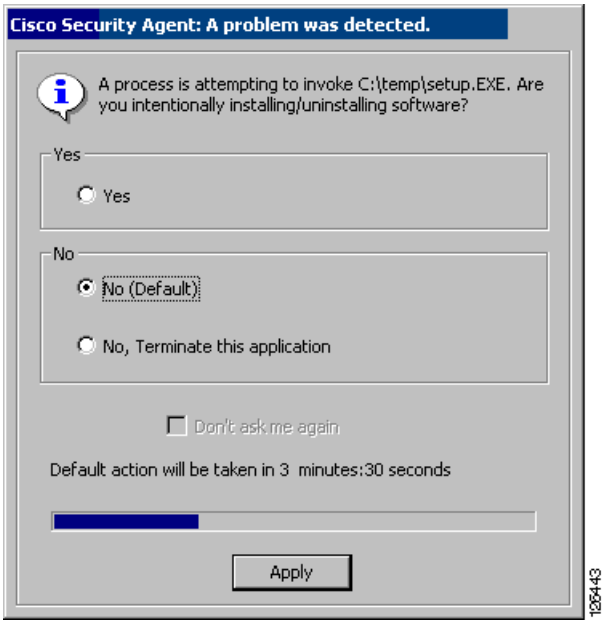
For a Query setting, the response to the query is relevant to the question, not the resource. For example, if a File access control rule queries the user for a response and that identical query is also configured for a Network access control rule, the user is not queried again when the Network access control rule triggers. The query response from the previous File access control rule is automatically taken.

See Query Settings, page 7-25 for configuration details.

**Caution** For Solaris rules, Query user options are not available. Instead, the default action is immediately taken.
For Windows and Linux agents, agent settings (including user queries) are configurable by the administrator. If the agent UI is hidden for the group, there are no query user pop-up boxes displayed. The default is immediately taken on all query user rules and heuristics that are present in the assigned polices.

When an action is attempted on a system where a query user rule is triggered, a pop-up box appears on the system where the resource is located.

*Figure 4-3 Query User Pop-up Box*




From the Query Settings page, accessible from the **Configuration>Variables** menu, you configure the query text and the query radio buttons that appear in the pop-up box the end user will see. In the Query pop-up box, the user reads the information given on the attempted action and selects one of the following possible choices and clicks Apply:

- **Yes**—Allows the application access to the resource in question.
- **No**—Denies the application access to the resource in question.
- **No, Terminate this application**—Denies the application access to the resource in question and also attempts to terminate the application process. The name of the application in question is displayed with the terminate option. (Some processes cannot be safely terminated, such as winlogon.)

  **Default Action**—You chose one of the radio buttons displayed in the query pop-up to be the Default action. If the query is not answered by the user within 5 minutes or if the user is not logged in to the system, the default action is taken immediately.

**Don't ask me again**—In addition to the button s that will appear on the query box, you can decide to also display a **Don't ask me again** checkbox so that the user's query response is remembered. If the user selects that checkbox when he/she responds to the query, and the same query is triggered, the remembered response is automatically taken and the user is not queried again.

**Query challenge**—For added security, you can issue a query challenge on the query pop-up box. If the default answer is not selected by the user and the selected answer is weaker than the default, a challenge will appear. This ensures that the user sitting in front of the system is answering the query rather than a malicious remote user or program attempting to respond. To pass the challenge, the user enters the information displayed in a graphic on the pop-up box itself. (See Query Settings, page 7-25.)


When you configure your query settings for the rule, the text you type into the Query Setting page's **Text used to query user** field is the same text that will appear in the Query User pop-up box to explain what is occurring on the system to the user. Therefore, making this information descriptive of the system action that triggered the pop-up is important.

**Caution** With file access control rules, the query user pop-up box appears on the system where the file or files in question are located. If a user is attempting to remotely access restricted files, the pop-up box appears on the remote machine where the files are located, not on the user's machine. That being the case, you would likely not want to place "query user" file access restrictions on files that are kept on an unattended system.

# Caching Responses

When users are queried, the agent can remember the response permanently or temporarily. This way, if the same rule is triggered again, the action is allowed, denied, or terminated based on what answer was given previously with no pop-up query box appearing again either permanently or for some period of time.

For example, if a user is queried as to whether an application can talk on the network and the user responds by selecting the **Yes** radio button and clicking a **Don't ask again** checkbox, the Yes response is remembered permanently and that response appears in the edit field in the agent UI query response window. But if the user is queried as whether setup.exe can install software on the system and the user responds by selecting the **Yes** radio button, but there is no **Don't ask again checkbox** or it is there but the user does not select it, this response is remembered temporarily and it does not appear in the agent UI query response window.

If the user response is only cached temporarily (for approximately an hour) the user can click the **Clear** button in this window to delete all temporarily cached responses. To clear permanent responses listed in the edit field, the user must select the response in the edit field and press the Delete key.

**Note** Permanent responses are remembered across reboots. Temporarily cached responses are not remembered across reboots. Also note, a query response is tied to the user who responded. On multi-user machines, multiple users may be asked the same question.

## Query Rule Priority Information

You should note how CSA MC manages rule priority if there are multiple similar query rules which need to be evaluated.

Base Priority: Action=Allow, Deny Terminate/no challenge/no don’t ask again/no logging.

Relative priorities for query options that are turned on are as follows (top to bottom):

- Challenge/Don’t ask again/Logging
- Challenge/Don’t ask again
- Challenge/Log

- Don’t ask again/Log
- Don’t ask again
- Log

# Building Policies and Rule Modules

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

The policy level is the common ground by which host groups acquire the rules that make up their security policy. If you are configuring your own policies, you should begin by understanding the purpose of your policy and how you must build your rule modules to meet your needs. It’s recommended that you build your policies from the top down. In other words, configure items in the following manner:

a. Decide what purpose the policy serves.

b. Understand what tasks the rule modules that comprise your policy must accomplish.

c. Decide what rule types you must configure to accomplish the tasks you’ve isolated.

## Configure a Policy

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

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

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

To configure a policy, do the following.

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

**Step 2** Click the **New** button to create a new policy entry. This takes you to the policy configuration page.

**Step 3** In the available policy configuration fields, enter the following information:

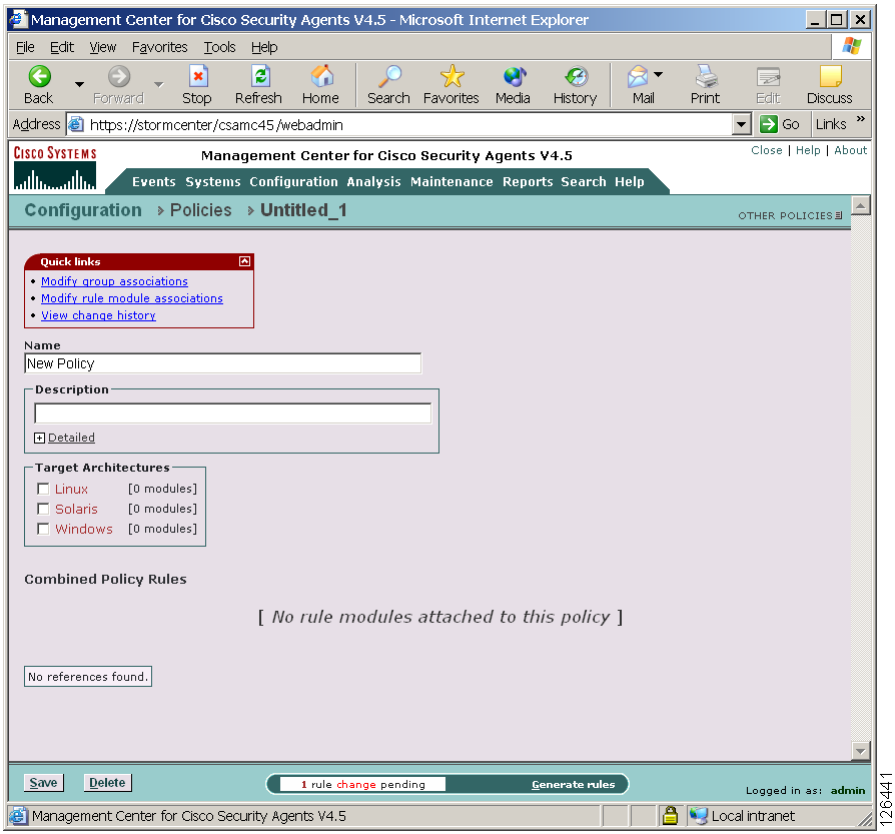
- **Name**—This is a unique name for this policy grouping of rule modules. Names are case insensitive, must start with an alphabetic character, can be up to 64 characters long and can include alphanumeric characters, spaces, and underscores.
- **Description**—This is an optional line of text that is displayed in the list view and helps you to identify this particular policy.

**Step 4** Select one or more **Target architecture** types for the policy. You can have one policy, for example - an Apache Web Server policy, and have all three architecture checkboxes selected. This way, each architecture specific rule module for Apache can be attached and deployed through one single Apache policy.

**Step 5** Click the **Save** button.

This policy is empty until you attach configured rule modules to it.

*Figure 4-4 New Policy*



# Configuring Rule Modules

Rule modules are the building blocks for your policies. Modules are made of several different types of rules. See Chapter 5, "Using System Correlation Rules" for information on event correlation and heuristic rules such as System API control.

**Note** Carefully read the section on writing allow and deny rules (page 4-9) so that you will understand how rule precedence works once policies are deployed. You should also refer to the chapter on configuration Variables (Chapter 7, "Configuring Variables") to help you understand the information required by the rule text fields.

**Caution** To maintain the integrity of the preconfigured policies and rule module shipped with CSA MC, it is recommended that you do not change them. If you are using preconfigured policies but want to edit them slightly due to your own site's needs, you should instead create a new policy (you can do this by cloning an existing policy) and add that policy to the group.

To configure a rule module, do the following.

**Step 1** Move the mouse over **Configuration>Rule Modules** in the menu bar. If you have not set OS admin preferences, you must select whether this is a Windows or a UNIX rule module from the cascading menu that appears. When you make a selection, the list of existing rule modules is displayed. CSA MC ships with several pre-configured modules.

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

**Tip** You can click the <#>rules link on the rule module list page to go directly to the rules contained in the module.

**Step 3** In the rule module configuration view, enter a unique **Name** for your module. Names are case insensitive, must start with an alphabetic character, can be up to 64 characters long and can include hyphens and underscores _ . Spaces are also allowed in names. Use a descriptive name that you can easily recognize in the policy listbox when you are attaching modules to policies.

**Step 4** Enter a **Description** of your module. This description is visible in the rule module list view. Optionally, expand the **+Detailed** field to enter a longer description.

**Step 5** In the **Operating System** box, optionally, you can select to target this module for a specific operating system within your Windows or UNIX classification.

**Step 6** Optionally, you can put this rule module into **Test Mode**. This way, you can have the rules within the test mode module operating in test mode while rules from other modules assigned to the same host are operating in a live mode. This is useful for testing new rule modules or changes to existing modules without having to turn off all protections for the hosts in question. You can also apply test mode on the group level. See Using Test Mode, page 4-114 for details.

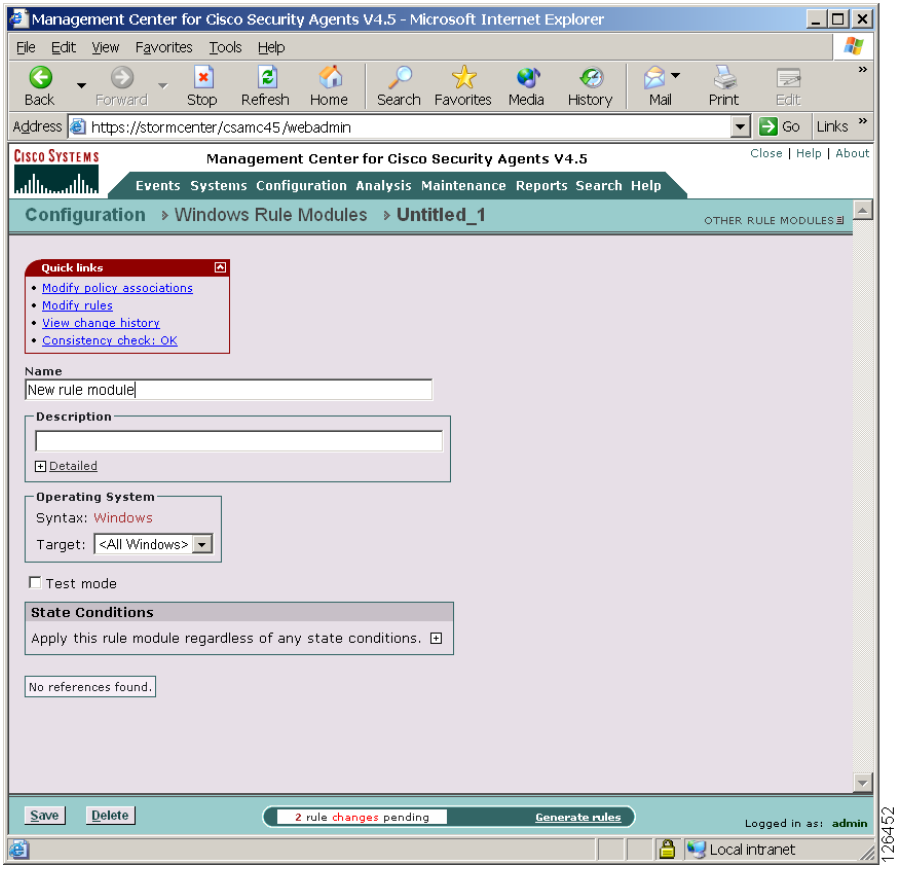
**Step 7** Click the **Save** button.

**Step 8** Now you add rules to your module. Click the **Modify rules** link at the top of the page.

Refer to the following sections for details on adding, copying, and configuring rules.

**Step 9** Optionally, you can impose configured **State Conditions** on rule modules. You can configuration System State conditions or User State conditions.

*Figure 4-5 New Rule Module*




# Setting State Conditions

System State and User State conditions let you write *conditional* rules based on the state of a system or the user of the system. Therefore, rules are only applied if the configured conditional settings are met.

# System State Sets

System state parameters let you dictate conditions based on detected machine settings. When a machine is operating an agent with a configured system state, the rules associated with that state apply only when the state parameters are met. They are conditional rules. For example, if you apply a system state to a rule module, you can dynamically "activate" and "deactivate" rules modules based on the changing state of a system. For example, you can apply special boot time rules that apply only at boot time. After booting is complete, normal operation rule modules are applied. Also, for example, you can apply a looser set of rules if an installation is occurring on a system. Once the installation is complete, a more stringent, normal operating set of rule modules are applied.

**Note** You do not have to specify a setting for every field in the System State page. If you do specify multiple settings, note that within single fields, multiple selections are "or-ed". If settings are specified for multiple fields, they are "and-ed".

For a more detailed description of system state setting options, read the configuration instructions here.

Configure a System State Set by doing the following:

**Step 1** Move the mouse over **Configuration>Rule Modules** in the menu bar. Select **System State Sets** from the cascading menu that appears.

**Step 2** Click the **New** button to create a new system state. See Figure 4-6.

**Step 3** Enter a unique **Name** for your system state. You will select this name in the Rule Module page. Names are case insensitive, must start with an alphabetic character, can be up to 64 characters long and can include hyphens, underscores, and spaces.

**Step 4** Enter a **Description**.

**Step 5** In the Network Admission Control section, you can select one or more (Hold the Shift key down while you click the mouse to choose multiple, concurrent options. Hold the Ctrl key down to select non-concurrent options.) **Cisco Trust Agent posture** state conditions for a system to ensure that corporate security requirements are met on that system. This feature works in conjunction with the capabilities of Cisco's Network Admission Control (NAC) functionality. See Creating Agent Kits, page 3-8 and Cisco Security Agent Posture Plug-in for CTA, page 10-20 for more information.

**Note** Currently, the Cisco Trust Agent (an optionally installed product available from Cisco Systems) is only supported on Windows platforms.

The Cisco Trust Agent checks the status of a system and reports this status back to the Cisco Secure Access Control Server (ACS). Based on this status check, ACS returns a "posture state" that the Cisco Security Agent can act upon.

For example, if a machine is running anti-virus software that is not up-to-date or is disabled, the Cisco Trust Agent can report this status to ACS which can then return an "Unknown" or a "Quarantine" state. The Cisco Security Agent will then take action based on that posture state and enforce a stricter policy to protect that system or even quarantine the system from the network. Refer to your ACS documentation for information on posture states and what they mean. Possible posture states are:

- <Don't care>—This state is not provided by ACS. All received posture states can match or not match this selection and the policy state is not affected. For UNIX states, this is currently the only valid posture state.
- Healthy—Host credentials are up-to-date and the risk to the network from this host is low.
- Checkup—Host credentials are not quite up-to-date, but the risk to the network is low. The host should update credentials as soon as possible.
- Quarantine—Host credentials are out-of-date. The host is vulnerable to compromise and should be updated immediately. The risk to the network from this host is high.
- Transition— The Host is in the process of having its posture checked and is given interim access pending a result from a full posture validation. A transition result may be applicable when a host is booting and requires restricted access to the network to complete the booting process , but not all posture information is available, for example, Windows machines need access to domain controller before user has logged in and before all posture applications may be running.
- Infected—Host has been compromised. The risk to the network from this host is very high. The host should be cleaned immediately.
- Unknown—The posture of host cannot be determined due to an error.

- Other—This state is not provided by ACS. If there is an incompatibility with posture state information received from ACS, it is seen as "Other" by the Cisco Security Agent. You can use this posture state as a criteria for enforcing a set of rules in the same manner you use other criteria.

**Step 6** In the System Security section, you can select one or more (Hold the Shift key down while you click the mouse to choose multiple, concurrent options. Hold the Ctrl key down to select non-concurrent options.) **Security level** conditions. If the end user has an agent UI, you can have a Security level condition apply which allows the user to set the security slidebar on their UI to a specific level. This provides some degree of user control to manage false positives or to control security when operating remotely or on the local network. This allows the user to decide, again to some degree, how much security they require.

**Step 7** In the System Location section, you can use the **Network address ranges** field to enter one or more addresses or address ranges to create a state condition based on system address. By default, no restrictions are set here. If you enter address conditions here, the condition applies if at least one interface matches what is specified. If you enter multiple ranges here, only one address has to match for the system state to apply.

**Step 8** In the System Location section, you can use the **DNS suffix matching** field to set a condition based on DNS server domain. It is the suffix of the DNS server used to resolve names that this field refers to. If any DNS server suffix (e.g. cisco.com) matches an item specified here, the condition is applied. You can use the **but not** field to make specific exclusions to DNS suffix matching parameters you configure.

**Step 9** In the Additional State Conditions section, you click the **Add State** link to add one or more of the following additional states to this page. (Use the pulldown menus that appear to select an option. Then use the pulldown to the right of your selected option to choose one of the following settings: <Don't care>, Yes, No.)

- Select the **Management Center reachable** option to set a state condition based on whether the Cisco Security Agent can communicate with the Management Center. Based on this condition, rules are applied or not applied. When the agent service first starts, it assumes that the management center is unreachable. When it attempts to communicate with the management center to receive rule changes or to upload events, if it can communicate with the management center at that time, it is then considered reachable.

- Select the **Installation process detected** option to set a state condition to apply if an installation is in progress on a system. For example, perhaps you want to apply a less restrictive set of rules to allow an installation when it is detected on a system. See Installation Applications Policy, page 5-19 for more information.
- Select the **Rootkit detected** option to set a state condition if a driver is seen attempting to dynamically load. Based on this condition, rules are applied or not applied. This state condition could be met if you are using the "Unauthorized rootkit" built-in dynamic application class in a rule module. When a process is added to the dynamic Unauthorized rootkit class, this system state condition is triggered. See page 6-8 for details on this application class.
- Select the **System booting** option to set a state condition to apply for the time frame in which the system is booting. Based on this condition, a set of designated rules apply only during boot time.
- Select the **Virus detected** option to set a state condition to apply if a virus is detected on a system. Based on that virus detection, a state condition setting can enforce a designated set of rules. This state condition could be met if you are using the "Suspected Virus Applications" built-in dynamic application class in a rule module. When a process is added to the dynamic Suspected virus applications class, this system state condition is triggered. See page 6-8 for details on this application class.

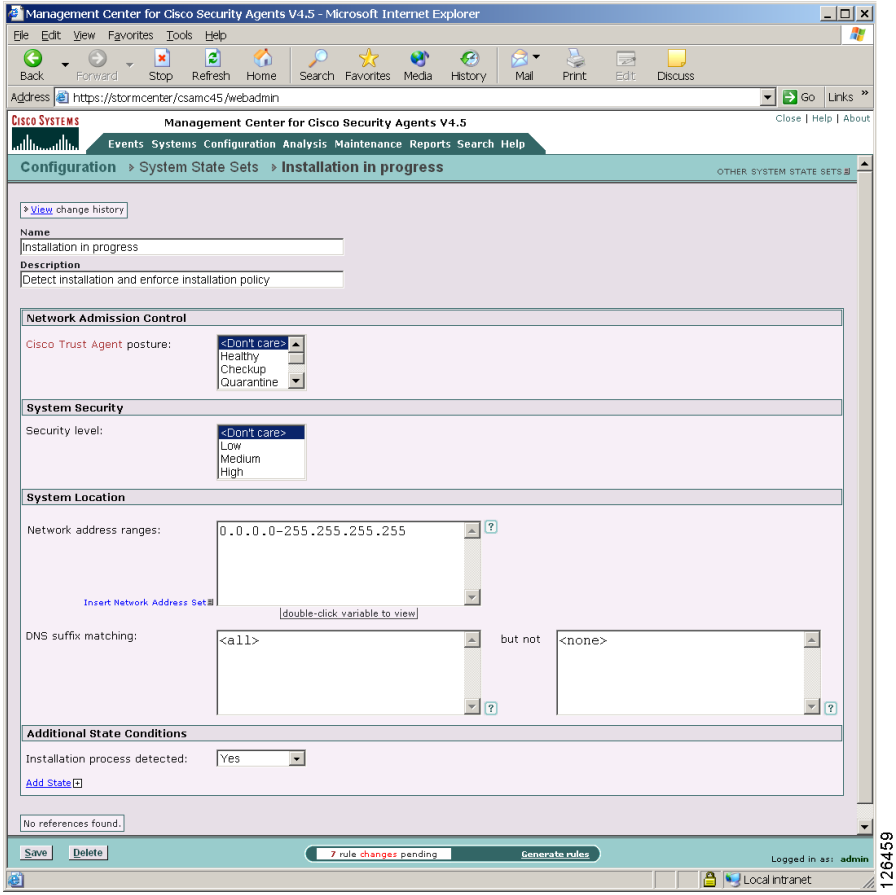
**Step 10** Click the **Save** button.

**Note** The system states you configure are additive. All specified state conditions are used as part of the requirement(s) to be met for the state to trigger.

**Caution** Remote VPN Clients - System Location and Management Center Reachable system states are checked by the agent whenever the network configuration changes on the system. Some VPN clients may make network configuration changes on a system that cause a system state to trigger. Such VPN clients can make use of System Location and Management Center Reachable settings to change the policy depending upon whether a tunnel is up or not. Other VPN clients, such as the Cisco VPN client V3.6, do not change network configurations

on a system. Therefore, you cannot use System Location and Management Center Reachable states to detect tunnels with these types of VPN clients. You should understand how your VPN client operates if you want to use these system states.

***Figure 4-6 System State Conditions***



# User State Sets

User state parameters let you dictate conditions based on detected user and/or group settings. When a machine is operating an agent with a configured user state, the rules associated with that state apply only when the state parameters are met. They are conditional rules. Keep this in mind when assigning a user set to a rule module.

You should also keep in mind that the process of checking user states is an expensive one for the system. You should use these settings judiciously.

An example of when you might want to employ a user state is as a restriction dictating who can alter web server pages. The web server application itself should only serve pages, not edit them. You could use a setting here to ensure that only authenticated administrators using a specific application (e.g. FrontPage) are allowed to alter web server content.

Another example of appropriate user state setting usage is a situation where groups of users are restricted from performing certain tasks that you only want to allow administrators to perform, such as suspending agent security.

Configure a User State Set by doing the following:

**Step 1** Move the mouse over **Configuration>Rule Modules** in the menu bar. Select **User State Sets** from the cascading menu that appears.

**Step 2** Click the **New** button to create a new user state. See Figure 4-7.

**Step 3** Enter a unique **Name** for your user state. You will select this name in the Rule Module page. Names are case insensitive, must start with an alphabetic character, can be up to 64 characters long and can include hyphens and underscores _ . Spaces are also allowed in names.

**Step 4** Enter a **Description**.

**Step 5** In the **Users matching** field, if you choose to set a condition based on user information, enter the user string data using machine name or domain name\user account. For example, entries in this field might appear as follows:

- `Domain_Accounting\Administrator` This represents the administrator in the Windows domain "Domain_Accounting."
- `W2K-jefe\Administrator` This represents user "Administrator" defined locally on the computer "W2K-jefe."
- `*\Administrator` This represents any user administrator.

- `Domain_Accounting\*` This represents all users in the domain "Domain_Accounting".

You can use wildcards in the Users matching/but not fields.

**Step 6** You can use the **but not** field to make specific exclusions to user matching parameters you configure.

**Step 7** In the **Groups matching** field, if you choose to set a condition based on group information, an entry in this field might appear as follows:

- `NT AUTHORITY\SYSTEM`
- `Domain_Accounting\Administrators`

For Windows, you can also enter SID (Security Identifier) numerical classifications into the Group matching field. Using a SID rather than a group name is useful when writing states that will apply across international versions of operating systems. Group names may be different across languages, but a SID classification is always the same.

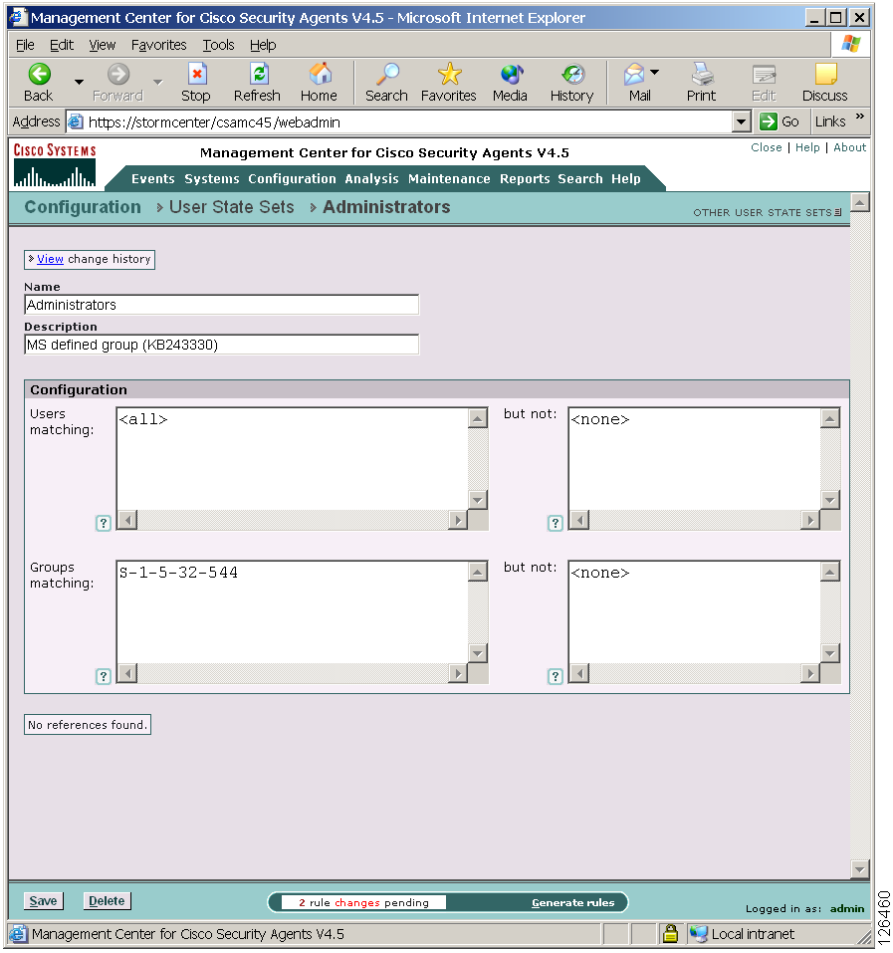
You cannot use wildcards in the Groups matching/but not fields. If users belong to multiple groups, they only need to match one named group to meet the criteria of the user state.

**Note** It is recommended that you use Group permissions rather than User permissions because Group designations are more widely applicable.

**Step 8** You can use the **but not** field to make specific exclusions to group matching parameters you configure.

**Step 9** Click the **Save** button.

*Figure 4-7 User State Conditions*

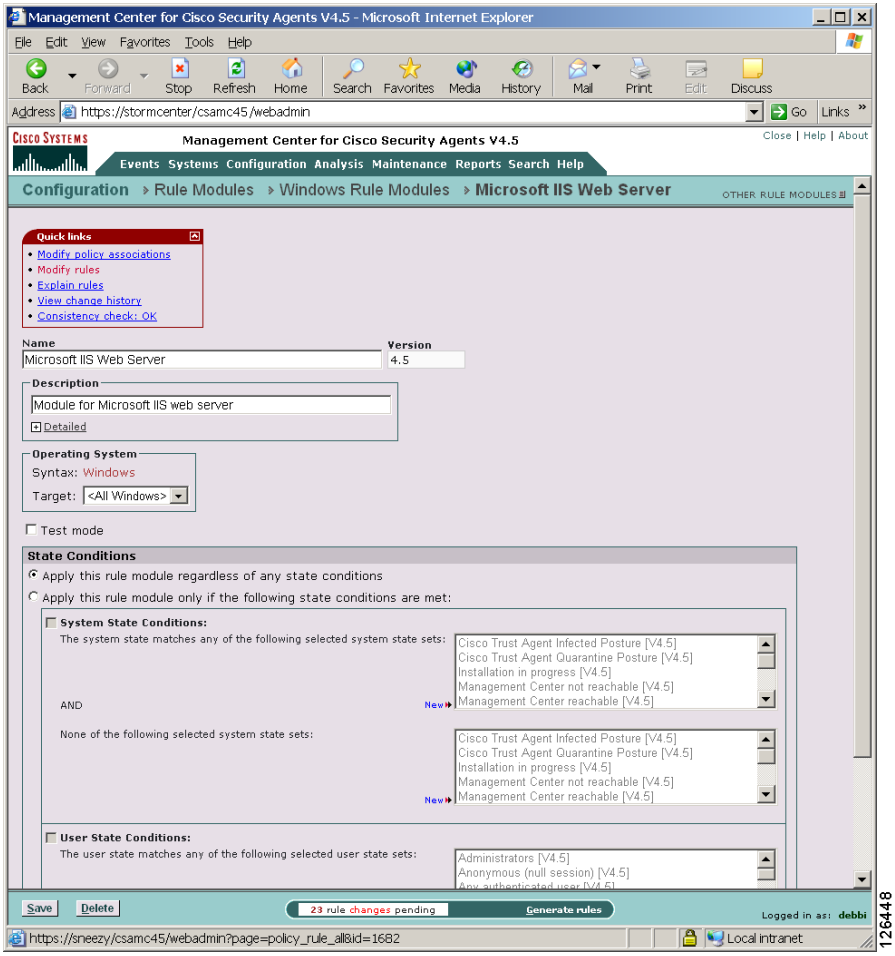



# Adding Rules to a Rule Module

First, click the **Modify rules** link at the top of the Rule Module page to go to the Rules page. See Figure 4-8.

To add rules to this policy, click the **Add rule** link in the Rules page. A menu list of the available rule types appears. Click on one to select it. This takes you to the configuration view for this rule type. Note that this rule contains no parameters until you create them.

***Figure 4-8 Rule Module, Modify Rules***



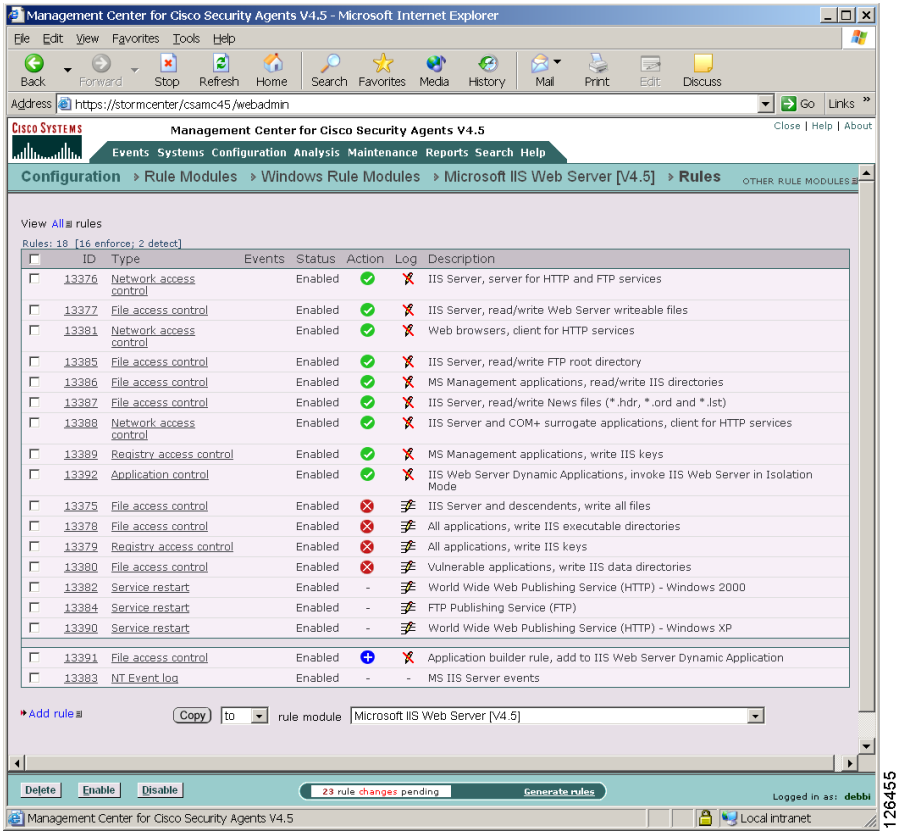

**Note** Refer to the following sections for details on configuring particular types of rules.

Use the **Enable** and **Disable** buttons in the rule module configuration view to enable or disable rules within a module without having to navigate to the configuration view for that particular rule. Select the checkbox for the rule you want to enable or disable and click the corresponding button. See Figure 4-9.

The **ID** column in the Rules section is the rule ID number assigned to the particular rule in question. This number increments each time a new rule is created. It is only used as an identifier for the rule. This ID is referenced in Event Log messages and can help you refer back to a particular rule.

The **Events** column in the Rules section (see Figure 4-10) displays the number of events generated by the rule in the last 24 hours. Clicking this number link takes you to a list of the events themselves.

*Figure 4-9 Rules List*



# Filtering the Rules Display

The Groups configuration page, Policy configuration page, and the Rules configuration page each display a table listing either the rules attached to the group or the rules included in the module (see Figure 4-10). On all of these pages, there is a **View All rules** item above the table. Clicking the **All** link here lets you filter your view of this rule list by selected rule type. When you click All, a pop-up appears listing the rule types present in the module or modules. Select a rule type from the pop-up, and that is now the only rule type displayed in the table. You can also select to view only enabled rules by selecting the **show enabled rules only** checkbox and then select the rule type you wish to view.

**Note** When you filter the rules display, other rules are NOT removed from the module. It is only your view of the module that changes. You can revert back to the entire summary view by selecting All from the same pop-up menu.

This filtering feature is useful when lists of rules grow extensive and you want to pare down your view to specific rule types.

If you have user or system states applied to rule modules, you can also filter the display based on those settings. This is useful to view which rules are applied when particular states are active.

# Copying Rules between Modules

Use the **Copy** button in conjunction with the pulldown lists at the bottom of the Rule Module page to copy selected rules to another rule module that you designate. Copying rules across modules works similar to the way cloning configurations works. (You can also clone rules within policies using the Copy button that will be described in this section.)

To copy selected rules from one module to another module, do the following:

**Step 1** From the Rule Module page (see Figure 4-10), select the checkbox for the rule or rules you want to copy to another module.

**Step 2** Beside the Copy button, **to** is the default selection in the pulldown menu. (Do not change this for copying individual rules between modules.) From the **rule module** pulldown list, select the name of the module to which you want to copy the selected rule or rules.

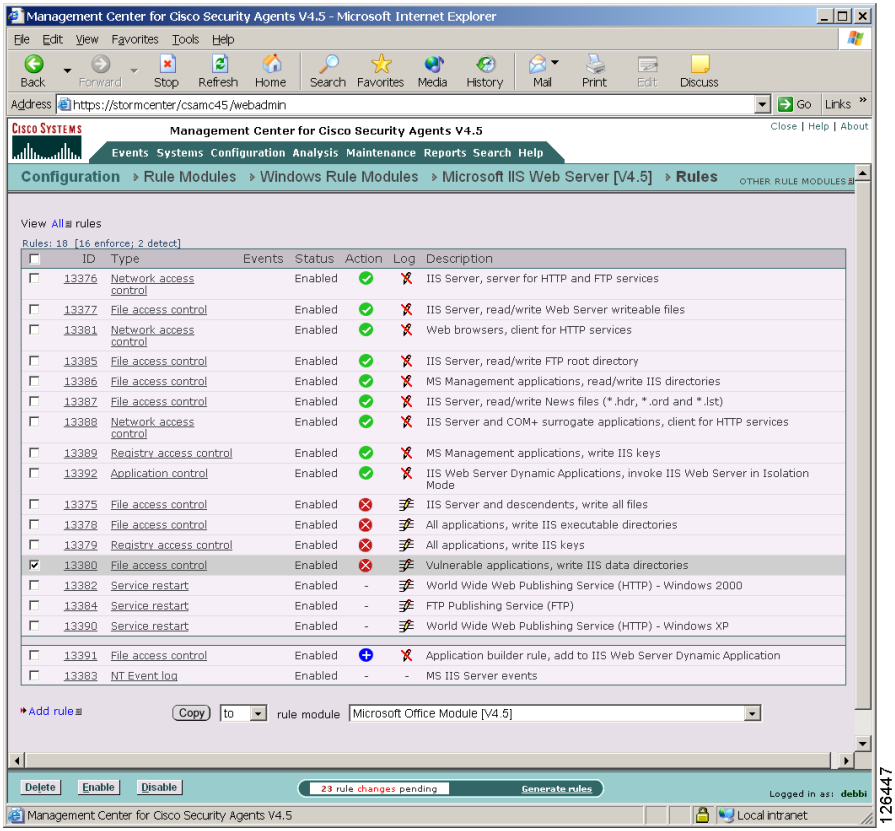
**Step 3** Click the **Copy** button.

All checked rules are copied to the selected module.

To clone rules within a module, repeat step 1 above. Then, rather than selecting another module in the rule module pulldown list, select the current module you are in from that same pulldown. Selected rules are cloned within the same module when you click the Copy button.

Select **from** in the pulldown menu beside the **Copy** button to copy ALL the rules from the selected module (in the rule module pulldown list) to the current module.

*Figure 4-10 Copy Rules between Modules*



# Comparing Configurations

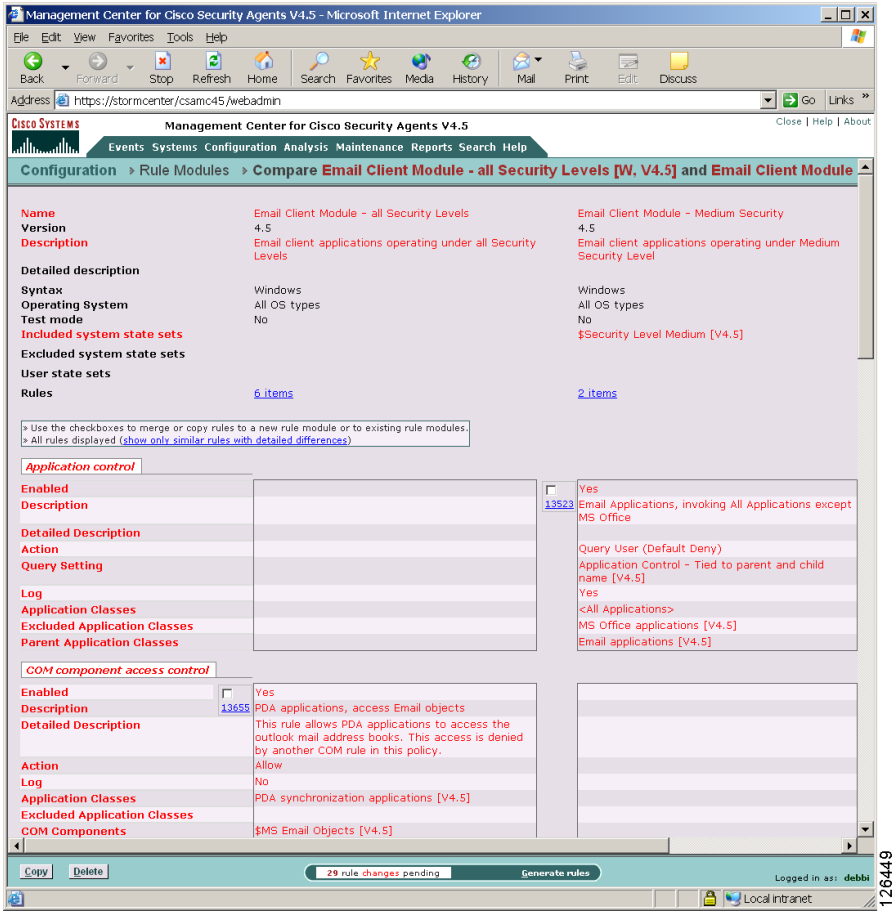
When you select the checkbox next to 2 items (you cannot compare more than 2 configurations at a time) and click the **Compare** button, CSA MC displays the configurations side by side and highlights the differences in red (see Figure 4-11). Once you've examined how the configurations compare, you can select to merge specific rules, to copy rules to another module, or to copy rules to a new module. Additionally, you can attach and detach groups and policies. (You can compare application classes and variables, but you can only copy and merge rules from the compare page.)

The purpose of this compare tool is to assist you after you've imported configurations or upgraded CSA MC. These processes can cause you to have duplicate or very similar configuration items. Comparing and merging configurations can help you to more easily consolidate duplicate items. This Compare utility is also available for Groups, Policies, Application Classes, and Variables.

Feature notes:

- When you compare rule modules, the similar rules within those modules are displayed side by side with the differences highlighted in red. If there are no differences, rule description text appears in black.
- If there is a rule in one modules and no corresponding similar rule in the second modules, there is nothing displayed beside that rule in the comparison.
- If you have rules in your modules comparison that have the same description, application class and other configuration items, they will not appear side by side if they have different logging options selected or different Allow/Deny actions. Logging and allow/deny actions change the priority of the rule within the policy. If the priority is not the same for each rule, they are not displayed side by side.

*Figure 4-11 Compare Rule Modules*

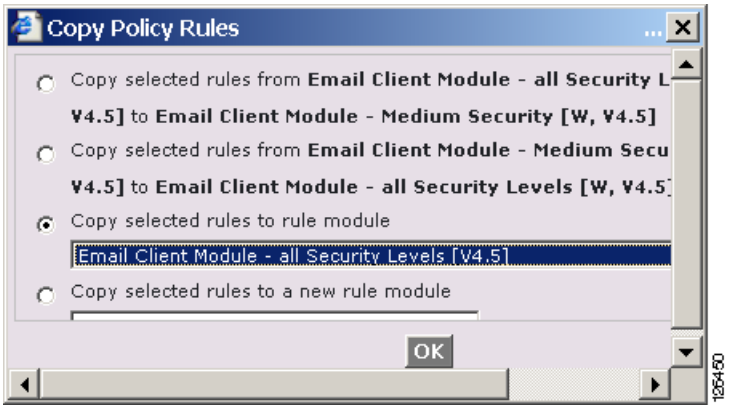


# Merging or Copying Rule Modules

Merge or copy rules by selecting the available checkbox above the rule or rules in question. When you click the Copy button in the bottom frame, a pop-up window appears. From this window, you select to do one of the following:

- Copy the selected rules from one rule module in the comparison to the other rule module in the comparison
- Copy the selected rules to another rule module you select (not part of the current comparison)
- Copy the selected rules to a new rule module which you create at this time by entering its name in the available field

***Figure 4-12 Copy Rule Module Pop-up Box***



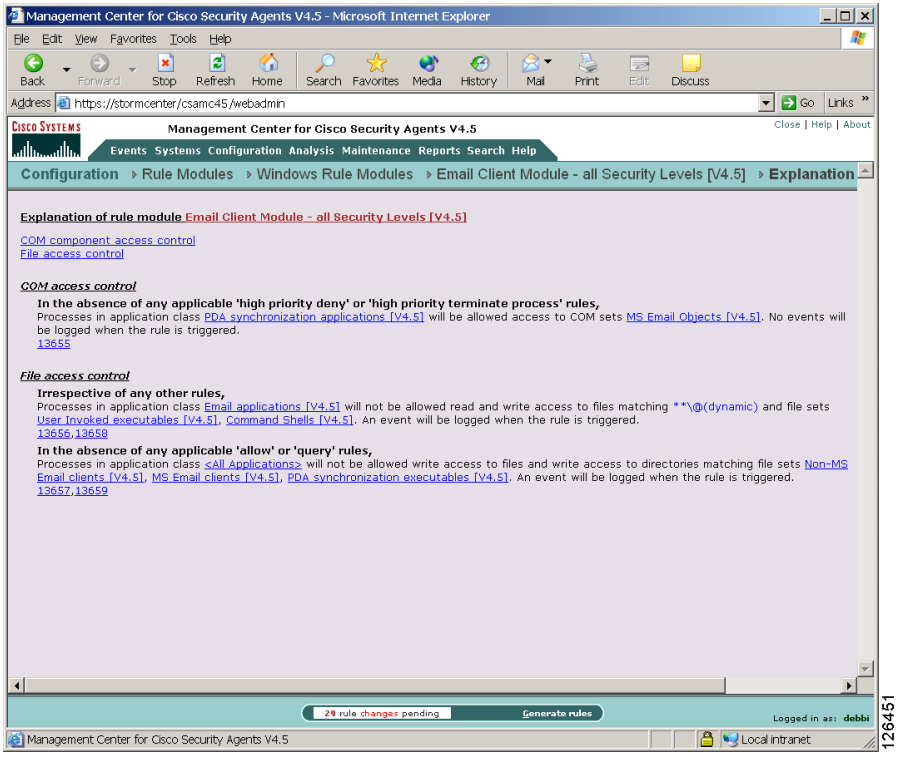

# View Change History

At the top of each rule page, there is a View change history link. Click this link to go to a page which lists all the changes that have been made to this rule. This View change history link is also available for Application classes, Variables, Rule Modules, and Policies.

# Explanation of Rules

CSA MC provides an explanation, in paragraph form, of the policy in question, describing each rule and its role in the policy. Clicking the **Explain rules** link in the Groups, Host, Rule Modules, or Policy page, takes you to this paragraph explanation. See Figure 4-13.

***Figure 4-13 Rule Explanation Page***



# Consistency Check

The main rule module page provides an OS consistency check for variables that are part of the rule. For example, it makes sure that Linux applications classes are attached to a UNIX module that has Linux or All UNIX as its target OS. If the rule module has a target OS of Solaris, the consistency check will fail if the application class is marked as Linux.

This consistency check also ensures that modules of a specified OS type are attached to similar OS policies. You are allowed to save modules that do not pass the consistency check so that you can clone items or make multiple policy edits, but you are not allowed to attach and deploy inconsistent items.

# Rules Common to Windows and UNIX

The following rule types are available for both Windows and UNIX policies.

## Agent Service Control

Use the Agent service control rule to control whether administrators are allowed to stop agent security (This is via a net stop command on Windows or via /etc/init.d/ciscosec stop on UNIX. See Chapter 10, "Using Management Center for Cisco Security Agents Utilities," for details) and whether end users can disable security via the agent UI security slide bar. Stopping agent security disables all rules until security is manually resumed or the system is rebooted.

If you use this rule to deny agent service stops, the agent service cannot be stopped on the system in question and therefore agents cannot be uninstalled.

**Note** Although agents cannot be uninstalled by administrative users if this rule denies the stopping of the agent service, this rule does not prevent agent software updates from occurring.

You can also use this rule to monitor, terminate, or tag a process that attempts to modify the agent configuration.

These instructions are a continuation of Configuring Rule Modules, page 4-22.

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **Agent service control** rule. This takes you to the configuration view for this rule type (see Figure 4-14).

**Step 3** In the Agent service control rule configuration view, enter the following information:

- **Description**—Enter a description of this rule. This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.) By not selecting this checkbox, you can save this rule, but it will not be active in the module and it will not be distributed to groups.

**Step 4** **Take the following action**—(Note that not all action types are available for this rule on Windows platforms.) Select an action type from the pulldown list. For further details on rule action types, see Rules: Action Options and Precedence, page 4-9.

**Step 5** and

- **Log**—Enable this checkbox to turn logging on for this rule. Generally, you will want to turn logging on for all deny rules. This means that the denied system action in question is logged and sent to the server at regular time intervals.
- **Take precedence over other <action type> rules**—Enable this checkbox to manipulate rule precedence so that this rule is evaluated before other similar rules. You should generally NOT require this checkbox. Do not use it without understanding how it works. See Rules: Manipulating Precedence, page 4-13 for details.

**Step 6** **when**

**Applications in any of the following selected classes**

Select *one or more* preconfigured application classes.
Note that the entry, <All Applications>, is selected by default. You can use this default or you can unselect it and create your own application classes. For application class configuration details, *see* Chapter 6, "Using Application Classes".

**Note** On UNIX systems, anyone with root access can stop the agent service. To prevent this, while still allowing administrators to stop the agent service, you would configure an Agent service control rule to Deny <All Applications> from stopping the service. Then configure another Agent service control rule which Allows only a UNIX Secured Management application class to stop the service.

**But not in the following class**—Optionally, select application classes here to exclude from the application class(es) you've selected in the included applications field. Note that the entry <None> is selected by default.

- **attempt to disable agent security**

  This checkbox controls whether users with administrator privileges can stop the agent service from the Service Control Manager or by running `net stop "Cisco Security Agent"` from a command prompt on Windows or via `/etc/init.d/ciscosec stop` on UNIX.

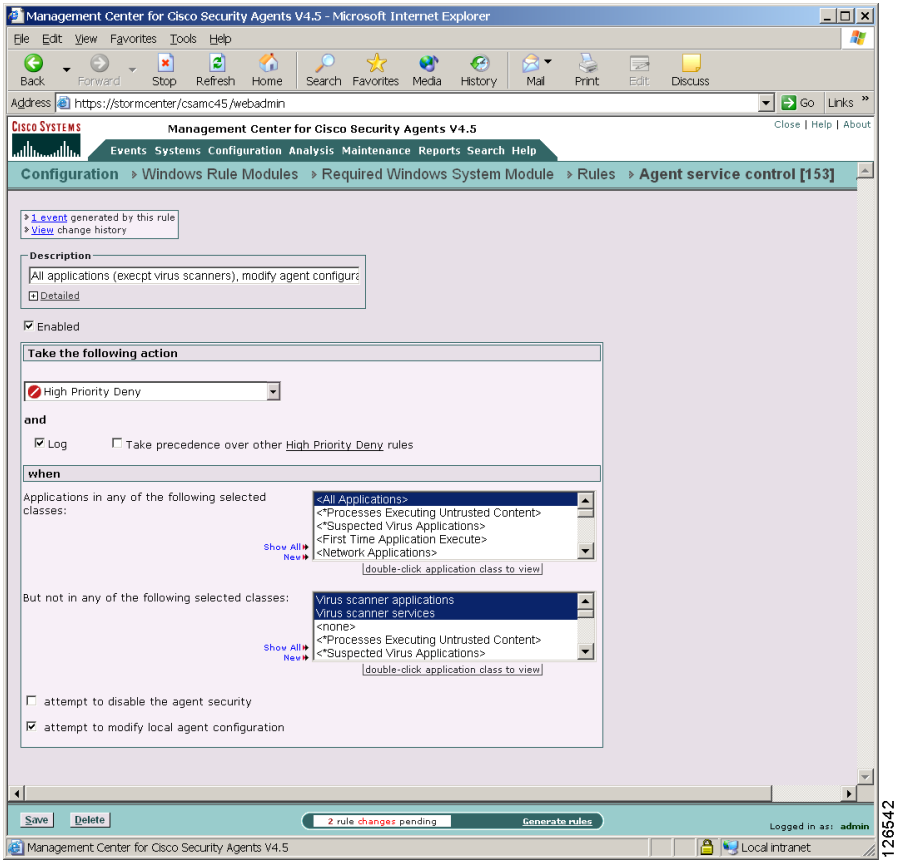
**Note** This also controls whether the "Off" setting on the agent security level slidebar allows the end user to turn agent security off. If you do not allow the stopping of the agent service, the Off level, if available, is ineffective. See Agent UI Control, page 4-48 for more information.

- **attempt to modify local agent configuration**

  The Cisco Security Agent has built-in global security policies which protect agent binaries and data. (Note that this protection is only offered when the agent service is running and is not stopped or in Test Mode.) While you cannot turn these non-logged, built-in rules off while the agent is active, you can use this rule to monitor, terminate, or tag a process that attempts to modify the agent configuration.

**Step 7** Click the **Save** button.

*Figure 4-14 Agent Service Control Rule (Windows)*



# Agent UI Control

**Note** This rule only applies to Windows and Linux platforms. The agent UI is not supported on Solaris systems.
Also note that Test Mode does not apply to this rule type.

Use the Agent UI rule to control how the agent user interface is displayed to end users. See Figure 4-15. In the absence of this rule, end users have no visible agent UI. If this rule is present in a module, you can select to display the agent UI and one or more controls to the end user. These controls give the user the ability to change certain aspects of their agent security. Optional controls are as follows:

- **Allow user to reset agent UI default settings**—On Windows, this is available from the **Start>Programs>Cisco Systems** menu. On Linux, this is available from **System Menu>Cisco Security Agent**. By selecting this option, users can reset agent UI functionality to the original factory default settings All user set controls are lost and all persistent query responses are removed. This is useful on Windows platforms where different users with varying user agent permission settings may log into the same machine.
- **Allow user interaction**—Selecting this checkbox causes the end user to have a visible and accessible agent UI, including a red flag in the system tray. With no other subsequent checkboxes selected, the agent UI contains a status view, a messages page to view agent events, and the ability to clear persistent and temporary query user responses. (If this rule is present in a module, but this checkbox is not selected, the end user will have no visible agent UI. In the presence of two or more Agent UI control rules, these rules are combined and selected checkboxes take precedence over unselected checkboxes.)

  Add one or more additional controls as follows:

  - **Allow user access to agent configuration and contact information**: Selecting this checkbox allows the end user to enter Contact information into the agent UI. They also have access to a Poll button which allows them to force a manual polling of the MC.
  - **Allow user to modify agent security settings**: Selecting this checkbox provides the end user with the ability to alter their security level by moving a slidebar between Off, Low, Medium, and High (in accordance with policies) and to manage the classification of untrusted content.

This checkbox provides an Off control on the agent UI. This Off control works in combination with the Agent service control rule (see Agent Service Control, page 4-44). You must both provide this slidebar to the end user and have an Agent service control rule in place which allows the agent security to be disabled in order for the Off setting to actually turn security off.

Allowing this action (moving the slidebar to Off) permits all users (including non-administrative users) to disable all rules on the agent until they are re-enabled by the user. (Note that if there is no agent UI present, agent security cannot be turned off.)

- **Allow user to modify agent personal firewall settings**—Selecting this checkbox provides the end user with the ability to dictate which applications are allowed network access. They also gain a file protection capability by which they can enter the names of local files that network applications are not allowed to access on their system. Note that if a user is allowed to configure personal firewall settings, resource access attempts on the system must pass both policy rules and firewall settings. (If you select this checkbox, you are providing the end user with controls that you have limited access to. Firewall queries and other information will not log to the CSA MC event log.)

## Hiding the agent UI

Not enabling the **Allow user interaction** checkbox in this rule has the following effects.

### Software updates

There are no effects. Hiding the agent UI and Software updates are independent features. You can provide a software update prompt when an agent UI is not present.

### Queries

When there is no agent UI present, there are no query user pop-up boxes displayed. The default is immediately taken on all query user rules and heuristics that are present in the assigned polices. (Note that this does not apply to cases where the end user manually exits the agent UI. Only the administrator controlled agent UI rule can affect query pop-up displays on the end user system.)

### Unavailable end user features

- No messages to inform user that actions have been denied and why.
- No ability to clear cache or re-enable logging.
- No fast polling ability.
- No end user contact information can be sent to CSA MC.

### Hidden agent UI feature notes

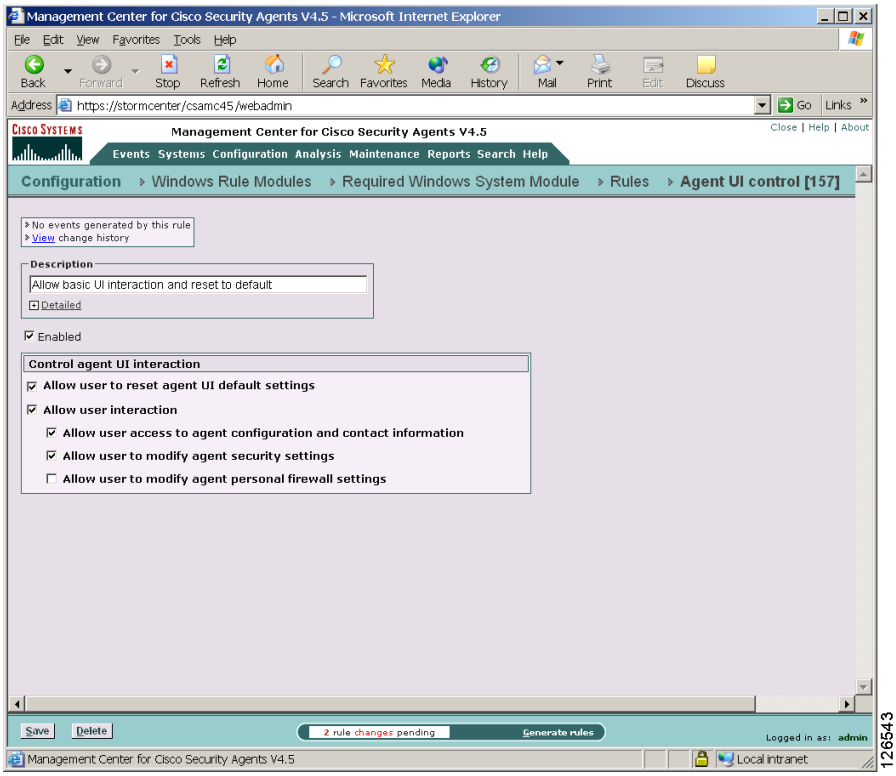
If a host belongs to multiple groups with multiple policies, having a visible agent UI setting, if present in any group for which the host is a member, takes precedence over a no user interaction agent UI setting.

Whether or not an end user system is going to have a visible agent UI or a hidden one, the end user (or administrator) must download and install the agent kit on the system. The initial installation of an agent kit cannot be done automatically (unless you have written your own script to do so, see Scripted Agent Installs and Uninstalls, page 3-18).

When there is no agent UI present, there are no query user pop-up boxes displayed. The default is immediately taken on all query user rules and heuristics that are present in the assigned polices.

If an end user system already has an agent UI installed, when you unselect the **Allow user interaction** checkbox and generate rules, the agent UI disappears when the new rules are downloaded.

*Figure 4-15 Agent UI Control Rule*



# Application Control

Use Application control rules to control what applications can run on designated agent systems. This rule type does not control what application can access what resources as do other access control rules. This rule type can stop selected applications from running on systems. If you deny an application class (in total) in this rule, users cannot use any application in that class.

With this rule, you can also prevent an application from running only if that application was invoked by another application you specify. This way, you could prevent a command prompt from running on a system if it is invoked by an application that has downloaded content from the network.

**Note** These instructions are a continuation of Configuring Rule Modules, page 4-22.

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **Application Control** rule. This takes you to the configuration view for this rule type (see Figure 4-16).

**Step 3** In the Application control rule configuration view, enter the following information:

- **Description**—Enter a description of this rule. This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.) By not selecting this checkbox, you can save this rule, but it will not be active in the policy and it will not be distributed to groups.

**Step 4** **Take the following action**—Select an action type from the pulldown list. For further details on rule action types, see Rules: Action Options and Precedence, page 4-9.

**Note** Creating dynamic application classes from the Application control rule is a bit different than creating them from other rule types. Because this rule has two application class fields, you can choose to add the current application to the dynamic class or choose to add the new application that is invoked by the first application to the dynamic class.

**Step 5** and

- **Log**—Enable this checkbox to turn logging on for this rule. Generally, you will want to turn logging on for all deny rules. This means that the denied system action in question is logged and sent to the server at regular time intervals.
- **Take precedence over other <action type> rules**—Enable this checkbox to manipulate rule precedence so that this rule is evaluated before other similar rules. You should generally NOT require this checkbox. Do not use it without understanding how it works. See Rules: Manipulating Precedence, page 4-13 for details.

**Step 6** when

- **Current applications in any of the following selected classes**—If you want to control an application (allow or deny) running on a system no matter how it is in invoked, allow "All Applications" to remain selected by default. (Then you will select the application you want to control from the second Application class list.)

  If you want to control which application(s) can invoke other applications, select one or more preconfigured application classes here to indicate the application that is doing the invoking (such as Network Applications).

  (When your rule is configured, currently selected application classes appear at the top of the list. See Configuring Static Application Classes, page 6-9 for configuration details.)
- **But not in the following class**—Optionally, select application classes here to exclude from the application class(es) you've selected in the included applications field. Note that the entry <None> is selected by default.

attempt to run

- **New applications in any of the following selected classes**—If you are controlling which applications can invoke other applications, this second field indicates the application class that you do not want to run when invoked by the application you chose in the top field.

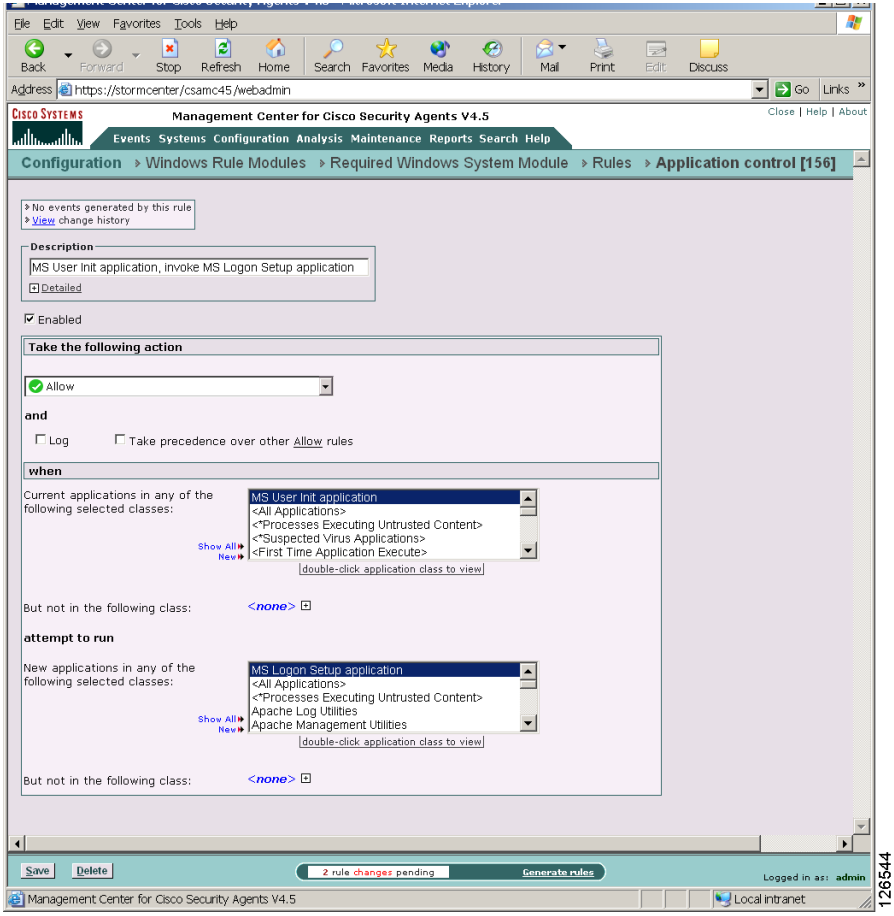
  If you selected "All Applications" in the top application field, you cannot select All Applications in this second field. If you did so, all applications would be completely prevented from running on systems if this is a deny rule.

- **But not in the following class**—Optionally, select application classes here to exclude from the application class(es) you've selected in the included applications field. Note that the entry <None> is selected by default.

**Note** Most dynamic application classes are not available in this second application class inclusion field.

**Step 7** When you are finished configuring your Application control rule, click the **Save** button.

*Figure 4-16 Application Control Rule*



# Connection Rate Limit

Use the connection rate limit rule to control the number of network connections that can be sent or received by applications within a specified time frame. This is useful in preventing attacks aimed at bringing down system services, e.g. denial of service attacks (server connection rating limiting). This is also useful in preventing the propagation of denial of service attacks (client connection rate limiting).

**Note** Multiple instances of the same application are counted together with respect to this rule. E.g. If a machine has several instances of Apache web server running, all Apache connections are counted together when applying this rule.

**Note** These instructions are a continuation of Configuring Rule Modules, page 4-22.

Click the **Modify rules** link at the top of the Rule Module page to go to the Rules page.

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **Connection rate limit** rule. This takes you to the configuration view for this rule type.

**Step 3** Enter the following information for the rule:

- **Description**—Enter a description of this rule.
  This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.)
  By not selecting this checkbox, you can save this rule, but it will not be active in the module and it will not be distributed to groups.
- **Log**—Use this checkbox to enable logging within the module.

**Step 4** **Take the following action**—Select an action type from the pulldown list. For further details on rule action types, see Rules: Action Options and Precedence, page 4-9. (Note that you cannot configure Query User Connection rate limit rules.)

**Step 5** **When Applications in any of the following selected classes**

Select *one or more* preconfigured application classes here to indicate the application(s) whose connection rate access you want to exercise control over.
Note that the entry, <All Applications>, is selected by default. You can use this default or you can unselect it and create your own application classes. For application class configuration details, *see* Chapter 6, "Using Application Classes".

**But not in the following class**—Optionally, selection application classes here to exclude from the application class(es) you've selected in the included applications field. Note that the entry <None> is selected by default.

**Note** When your rule is configured, currently selected application classes appear at the top of the list.

**Step 6** **Attempt to act as a**—Select server, client, or "client or server"

From the pulldown menu, select **server**, **client,** or **client or server** depending on the *direction* of the connection you are controlling.
If you are limiting a server's connection limit, select server here. If you are limiting a client connection, select client here.

**Step 7** **Communicating with**—Select specific hosts or all hosts

When the rate limit set here is reached, you can determine whether all subsequent service requests are dropped or only those received or sent by a specific host. If you select a "specific" host, this indicates that the host in question exceeded the rate limit. If you select all hosts, this indicates that the sum total of to and from all hosts exceeds the limit and all hosts are blocked.

**Step 8** **Over/Under a limit <100> network connections**

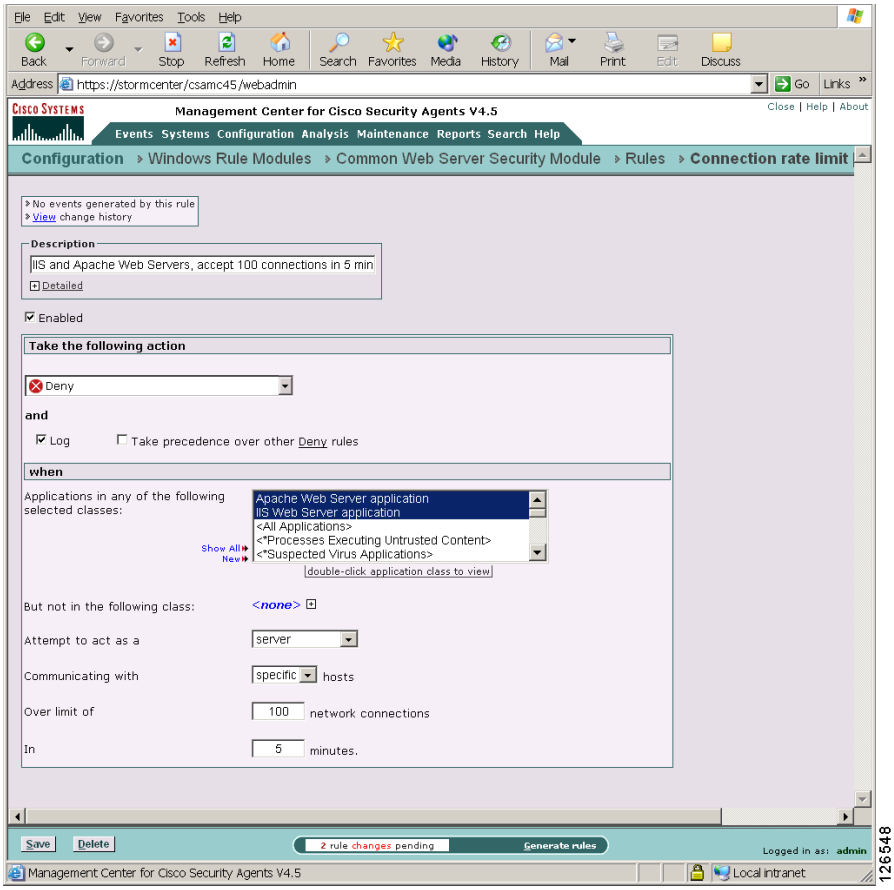
**in <5> minutes**

Reasonable values are entered into these fields by default. They define the number of connections that can normally be expected during a time frame from either specific hosts or all hosts.

- If you select an action type of “deny” or “terminate”, and the limit is exceeded (*Over*) in this time frame (abnormal amount of connections that could represent an attack of the system), subsequent connection requests are dropped. (The dropped connections can be those received to/from individual “specific” hosts or to/from all hosts. This setting is configured at the bottom of the page.)
- If you configure this as an “allow” rule, you are setting a limit *Under* which the number of connections must remain for the subsequent connections to be explicitly allowed.

**Step 9** When you are finished configuring your connection rate limit rule, click the **Save** button.

*Figure 4-17 Connection Rate Limit Rule*



# Data Access Control

Use data access control rules on Web servers to detect clients making malformed web server requests where such requests could crash or hang the server. A malformed request could also be an attempt by an outside client to retrieve configuration information from the web server or to run exploited code on the server. This rule detects and stops such web server attacks by examining the URI portion of the HTTP request.

An HTTP request consists of:

- the request method (a “get” or a “post”)
- the request URI (Uniform Resource Identifier—This includes the URL and related request parameters and arguments)
- the HTTP version (for example, HTTP/1.0)
- the HTTP header

The Data access control rule examines patterns in the URI portion of the HTTP request. The pre-configured Data sets (see Data Sets, page 7-7) group patterns to match based upon

- functional associations of meta-characters (e.g. "(" and ")")
- examples of known classes of attacks
- Web server specific exploits

Use the data access control rule to allow or deny specified underlying network data requests for the following web servers and platforms:

- Microsoft IIS (Windows platforms, version 4.0 or higher)
- Apache (Windows and UNIX platforms, versions 1.3, 2.0)
- IPlanet (UNIX platforms, version 6.0)

**Caution** On Windows platforms, if you install Web server software (IIS or Apache) after you install the Cisco Security Agent on the server system, or if you have installed the Web server in a directory other than the default, you must manually install the Cisco Security Agent data filter in order to use Data access control rules on the system in question.
If your Web server software is already installed (in its default directory) when you install the agent on Windows, the server software is detected by the agent and the

data filter capability is automatically installed with the agent.

On Solaris (Apache or IPlanet servers) and Linux (Apache servers), in order to use Data access control rules you must install the data filter manually after you install the Cisco Security Agent. Unlike Windows, the Solaris and Linux installations do not detect Web server software and do not install the data filter with the agent. You must always manually install it.
See Manual Agent Data Filter Installation, page 10-10 for instructions.

**Note** These instructions are a continuation of Configuring Rule Modules, page 4-22.

Click the **Modify rules** link at the top of the Rule Module page to go to the Rules page.

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **Data access control** rule. This takes you to the configuration view for this rule type.

**Step 3** Enter the following information for the rule:

- **Description**—Enter a description of this rule.
  This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.)
  By not selecting this checkbox, you can save this rule, but it will not be active in the module and it will not be distributed to groups.

**Step 4** **Take the following action**—Select an action type from the pulldown list.
For further details on rule action types, see Rules: Action Options and Precedence, page 4-9.

**Step 5** and

- **Log**—Enable this checkbox to turn logging on for this rule. Generally, you will want to turn logging on for all deny rules. This means that the denied system action in question is logged and sent to the server at regular time intervals.

- **Take precedence over other <action type> rules**—Enable this checkbox to manipulate policy rule precedence so that this rule is evaluated before other similar rules. You should generally NOT require this checkbox. Do not use it without understanding how it works. See Rules: Manipulating Precedence, page 4-13 for details.

**Step 6** **When—Applications in any of the following selected classes**

Select one or more preconfigured application classes here to indicate the application(s) whose access to the listed data sets you want to exercise control over.
Note that the entry, <All Applications>, is selected by default. You can use this default or you can unselect it and create your own application classes. For application class configuration details, *see* Chapter 6, "Using Application Classes".

- **But not in the following class**—Optionally, select application classes here to exclude from the application class(es) you've selected in the included applications field. Note that the entry <None> is selected by default.

**Note** When your rule is configured, currently selected application classes appear at the top of the list.

**Step 7** **Attempt to access these data sets**

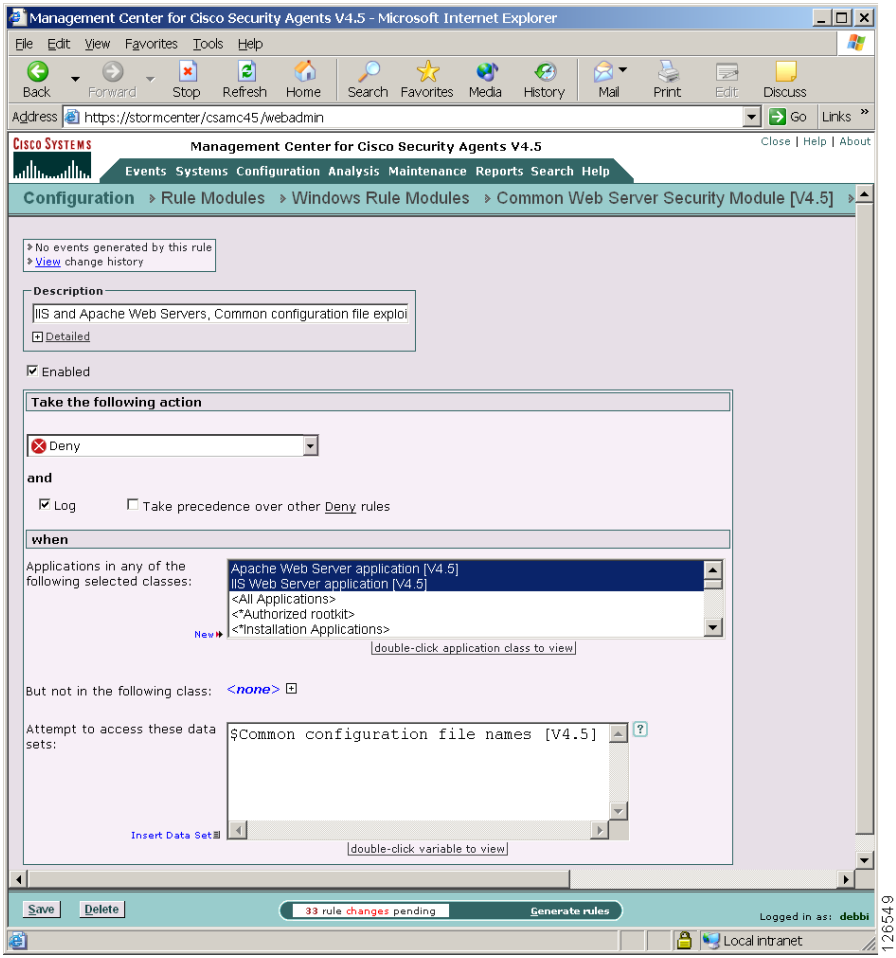
Click the **Insert Data Set** link to enter a pre-configured data set here. When you click this link, a list of the Data Sets you've configured appears here, allowing you to select one or more. Instead of data sets, you can list the literal data strings you want to protect. You can use a wildcard designation.

For information on configuring Data Sets, see page 7-6.

**Step 8** When you are finished configuring your Data access control rule, click the **Save** button.

**Note** If you specify an application here other than IIS, Apache, or iPlanet, this rule is ignored.

*Figure 4-18 Data Access Control Rule*



# File Access Control

Use file access control rules to allow or deny what operations (read, write) selected applications can perform on files. You should understand that file protection encompasses read/write access. Directory protection encompasses directory deletes, renames, and new directory creation.

**Note** These instructions are a continuation of Configuring Rule Modules, page 4-22.

Click the **Modify rules** link at the top of the Policy page to go to the Rules page.

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **File access control** rule. This takes you to the configuration view for this rule type.

**Step 3** Enter the following information for the rule:

- **Description**—Enter a description of this rule.
  This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.)
  By not selecting this checkbox, you can save this rule, but it will not be active in the module and it will not be distributed to groups.

**Step 4** **Take the following action**—Select an action type from the pulldown list. For further details on rule action types, see Rules: Action Options and Precedence, page 4-9.

**Step 5** and

- **Log**—Enable this checkbox to turn logging on for this rule. Generally, you will want to turn logging on for all deny rules. This means that the denied system action in question is logged and sent to the server at regular time intervals.

- **Take precedence over other <action type> rules**—Enable this checkbox to manipulate rule precedence so that this rule is evaluated before other similar rules. You should generally NOT require this checkbox. Do not use it without understanding how it works. See Rules: Manipulating Precedence, page 4-13 for details.

**Step 6** **When—Applications in any of the following selected classes**

Select one or more preconfigured application classes here to indicate the application(s) whose access to the listed files you want to exercise control over.
Note that the entry, <All Applications>, is selected by default. You can use this default or you can unselect it and create your own application classes. For application class configuration details, *see* Chapter 6, "Using Application Classes".

- **But not in the following class**—Optionally, select application classes here to exclude from the application class(es) you've selected in the included applications field. Note that the entry <None> is selected by default.

**Note** When your rule is configured, currently selected application classes appear at the top of the list.

**Step 7** **Attempt the following operations**

Select the operations **Read** and/or **Write** you are allowing/denying on the files named in the Files field. For directory protection, the actions you are allowing/denying are **Create**, **Delete**, and **Rename**. Refer to File and Directory protection in Using the Correct Syntax, page 2-28.

**Caution** Directory protection ignores the file portion of the specified path and only matches the directory portion of the path. If the directory portion is not well specified, the protection will be overly broad. For example, if you select to protect a directory in a deny rule and enter the directory path as follows: `**\Program Files\**Outlook.exe`, then no directories can be modified under Program Files. That is an overly broad protection to specify and would likely result in system instability. If you choose to protect directories, be sure to get very specific in your path string and understand the resulting behavior.

**Step 8** **On any of these files**

Click the **Insert File Set** link to enter a pre-configured file set here. When you click this link, a list of the File Sets you've configured appears here, allowing you to select one or more. Instead of file sets, you can list the literal files you want to protect, using the file paths (including wildcards).

For information on entering file path literals here rather than using pre-configured File Sets, see Using the Correct Syntax, page 2-28.

For local system paths, you must specify the disk drive. You can use a wildcard designation. When protecting directory creates, in particular, you should note that directory creation applies to an exact directory path match, but directory write and rename protection applies to all directories explicitly named in a path. If a directory name is completely wildcarded **\, no protections exist for that particular component of the directory. For example:

Windows:

```
*:\Program Files\winnt\*
```
or `@system\**` (this indicates all files below the system directory)

UNIX*:*

```
/etc/passwd
```

For network machines (Windows only), enter

```
\\<machine name>\<share>\<path>\<filename>
```
For example: `\\Backup_Server\finance\records\database.db`
You can enter more than one file path, but each entry must appear on its own line. For File Set configuration details, *see* page 7-10.

**Caution** **Symbolic Links and Hard Links**: For UNIX, if you create a File access control rule to protect a symbolic link, ONLY that symbolic link is protected. The underlying resource, unless also specified, is NOT protected. For example, a File access control rule written for /etc/hosts does not protect /etc/inet/hosts. Similarly, a File access control rule written for /etc/inet/hosts does not protect /etc/hosts. If you want to protect a symbolic link and its underlying resource, both must be specified in the rule.

Also note that on UNIX systems, if you attempt to create a hard link to an agent-protected file, that action is seen as a write attempt on the file.

**Note** Use **@dynamic** in the File set text field to indicate all files that have been quarantined by CSA MC as a result of correlated email worm events, correlated virus scanner log messages, or files that were added manually by the administrator. This list updates automatically (dynamically) as logged quarantined files are received.

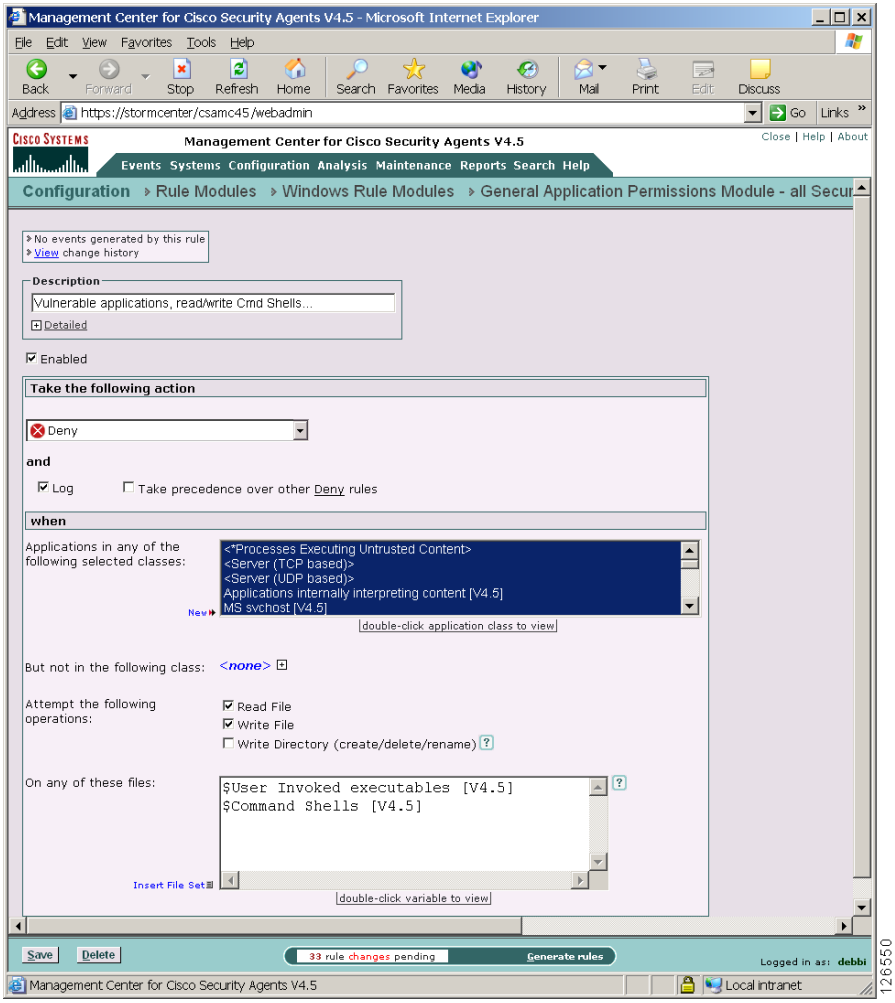
To view the files that are added to the dynamically quarantined files list and to manually add files to be quarantined, click the **Manage dynamically quarantined files** link on the Global Event Correlation page. See Manage Dynamically Quarantined Files and IP Addresses, page 5-23 for more information.

**Step 9** When you are finished configuring your File access control rule, click the **Save** button.

This rule is now part of your new policy. It takes effect when the policy is attached to a group and then downloaded by an agent on the network.

**Caution** In order to distribute rules to the correct hosts, you must associate policies with groups and then Generate rules. See page 4-111 and page 4-118 for instructions.

*Figure 4-19 File Access Control Rule*



# Network Access Control

Use network access control rules to control access to specified network services and network addresses. You can also use this rule type to listen for applications attempting to offer unknown or not sanctioned services.

**Note** The following instructions are a continuation of Configuring Rule Modules, page 4-22.

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **Network Access Control** rule. This takes you to the configuration view for this rule type.

**Step 3** Enter the following information:

- **Description**—Enter a description of this rule. This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.) By not selecting this checkbox, you can save this rule, but it will not be active in the policy and it will not be distributed to groups.

**Step 4** **Take the following action**—Select an action type from the pulldown list. For further details on rule action types, see Rules: Action Options and Precedence, page 4-9.

**Step 5** **and**

- **Log**—Enable this checkbox to turn logging on for this rule. Generally, you will want to turn logging on for all deny rules. This means that the denied system action in question is logged and sent to the server at regular time intervals.
- **Take precedence over other <action type> rules**—Enable this checkbox to manipulate rule precedence so that this rule is evaluated before other similar rules. You should generally NOT require this checkbox. Do not use it without understanding how it works. See Rules: Manipulating Precedence, page 4-13 for details.

**Step 6** **When—Applications in any of the following selected classes**

Select one or more preconfigured application classes here to indicate the application(s) whose access to the listed services and addresses you want to exercise control over.
Note that the entry, <All Applications>, is selected by default. You can use this default or you can unselect it and create your own application classes. For application class configuration details, *see* Chapter 6, "Using Application Classes".

- **But not in the following class**—Optionally, select application classes here to exclude from the application class(es) you've selected in the included applications field. Note that the entry <None> is selected by default.

**Step 7** **Attempt to act as a**—Select server or client or both, or select listener

From the pulldown menu, select **server**, **client, client or server,** or **listener** (see page 4-72 for more information on the listener option) depending on the direction or type of connection you are controlling or listening for.
If you are limiting a server's contact with clients, select server here and enter the client(s) address in the host addresses field. If you are limiting a client's contact with a server, select client here and enter the server(s) address in the host addresses field.

**Step 8** **for network services**

Enter the literal protocol/port number combination for the service you want to control access to or click the **Insert Network Service** link to enter a pre-configured network service variable here. When you click this link, a list of the Network Service Variables you've configured appears here, allowing you to select one or more.
This field refers to either a server providing this service or a client accessing this service. For Network Service configuration details, see page 7-18.

**Step 9** **Communicating with host addresses**

Enter the literal network address(es) for the client/servers you want to control access to or click the **Insert Network Address Set** link to enter a pre-configured network address set variable here.
If you select server in the previous pulldown list, you enter client addresses here. If you select client in the previous pulldown list, you enter server addresses here. Note that you can use Network Address Set variables.

- You also can use the following "short hand" entry in Network Address Sets and in Network Access Control rules to indicate all local addresses on the agent system in question. The @symbol must appear at the start of the short hand name.

Use **@local** to indicate all local addresses on the agent system. You would want to use this if you are allowing different applications on a single system to talk to each other without opening these applications up to network access.

Refer to Using the Correct Syntax, page 2-28 for more valid @ entries that can be used in this rule type.

**Step 10** **Using these local addresses**

Enter the literal network address(es) for the local system addresses you want to control (i.e. control clients making connections from or control servers making connections to). You can also click the **Insert Network Address Set** link to enter a pre-configured network address set variable here.

The addresses or address ranges you enter here can be used to control the host initiating the network connection. For example, you could write a Network access control rule which would only allow laptop users to connect to an internal network database if their connection is coming through a VPN (i.e. machine using an allowed/disallowed address to make a connection, incoming or outgoing). If the connection attempt comes in through an ISP-assigned address that is not part of this rule, it would not be allowed.

You could also use this field to impose a restriction that only trusted addresses can read an internal server. If the connection is received from an internal system or via a VPN from a fixed, trusted address, it is allowed.

Use **@dynamic** in the Addresses set field to indicate untrusted hosts that have been quarantined by CSA MC. Addresses are added to this list when they are seen as an untrusted host. (The built-in "Processes Communicating with Untrusted Hosts" is triggered in a rule.) This list updates automatically (dynamically) as logged quarantined addresses are received.

**Step 11** When you are finished configuring your Network access control rule, click the **Save** button.

This rule is now part of your rule module. It takes effect when the policy is attached to a group and then downloaded by an agent on the network. You should note that new rules only apply to new connections. See Preserving Application Process Classes, page 6-8 for details.

**Caution** In order to distribute rules to the correct hosts, you must associate policies with groups and then Generate rules. See page 4-111 and page 4-118 for instructions.

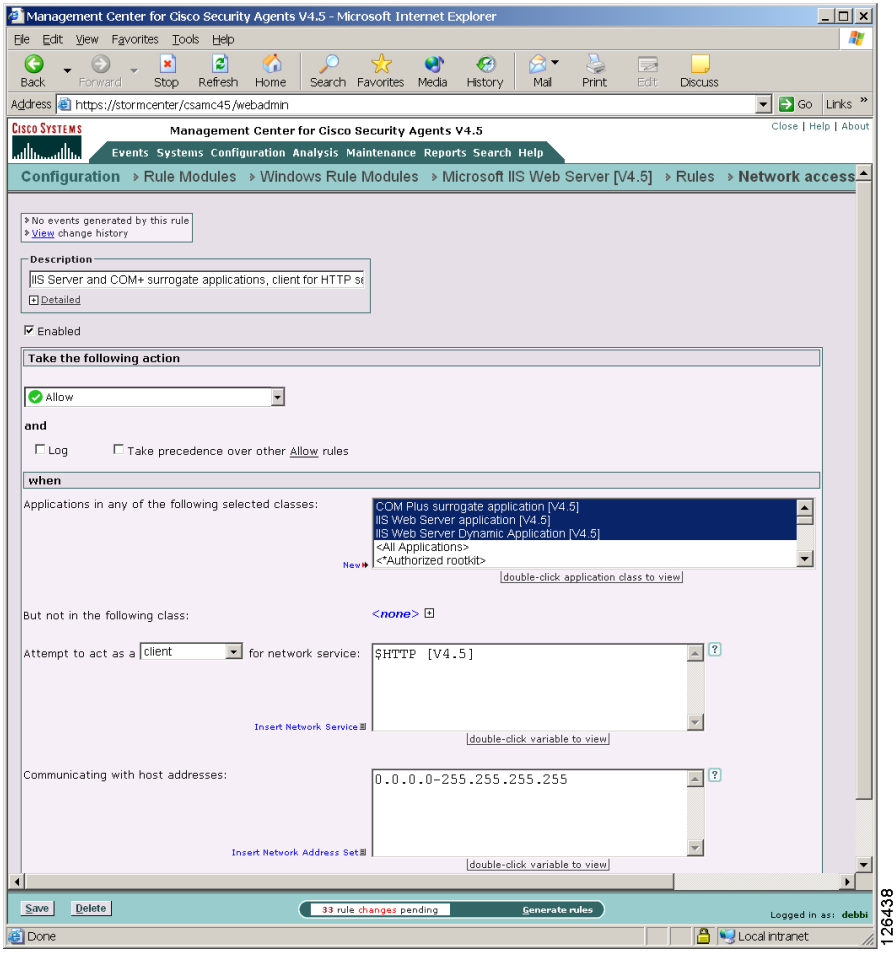
**Note** No network access control rule denial events are logged for any UDP port resulting from multicast packet signals. (If a collection of hosts have the same network access control rule and a broadcast such as UDP/138 were denied, then event messages would inundate CSA MC.)

**Note** When the system accepts a network connection on behalf on an application, the system requires an immediate answer to allow or deny the connection. Therefore, resource requests which trigger network access control server queries will immediately choose the query default. The user is still queried and the response will be cached for future connections.

### What is the "listener" option for?

You can use the listener option in a Network access control rule to indicate what applications have the ability to be a server before they are allowed to accept a server connection. This is in contrast to the "server" option which offers real-time per connection control. The listener option can be used in a monitoring capacity to reveal any applications that are attempting to offer a network service. For example, if a system is already infected with a Trojan, that Trojan may be listening on a high numbered port for a network server connection. A NACL listener rule would detect this occurring before a server connection is achieved. You could then craft a subsequent NACL rule to deny the server connection.

*Figure 4-20 Network Access Control Rule*



# Windows Only Rules

The following rules are only available for Windows Rule Modules.

## Clipboard Access Control

Use the clipboard access control rule to dictate which applications can access information that is written to the clipboard. When writing security policies, you may want to protect information from being accessed by other applications or network processes. To fully protect this information, you must consider preventing other applications from accessing protected information that may have been written to the clipboard.

This rule works in the following manner. When a process belonging to an application class specified in a clipboard rule writes to the clipboard, the data is marked as protected. Only processes which also match the specified application classes are allowed to read the data from the clipboard. When a process that does not belong to the application class specified writes to the clipboard, the data is marked as unprotected. Any process is allowed to read from the clipboard then.

For example, if Microsoft Excel (which is part of the Microsoft Office application class) saves data to the clipboard, other Microsoft Office applications will be able to read the clipboard data to allow cut and paste functionality between Office applications. Non-Office applications would be prevented from reading this clipboard data.

These instructions are a continuation of Configuring Rule Modules, page 4-22.

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **Clipboard access control** rule. This takes you to the configuration view for this rule type. See Figure 4-21.

**Step 3** Enter the following information for the rule:

- **Description**—Enter a description of this rule. This description appears in the list view for the module.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.) By not selecting this checkbox, you can save this rule, but it will not be active in the module and it will not be distributed to groups

**Step 4** Do not allow any other application to read from the clipboard data written by:

- **Applications in any of the following selected classes**—Select one or more preconfigured application classes here to indicate the application(s) whose data you want to exercise control over. Note that the entry <All Applications> is selected by default. You can use this default or you can unselect it and create your own application classes.

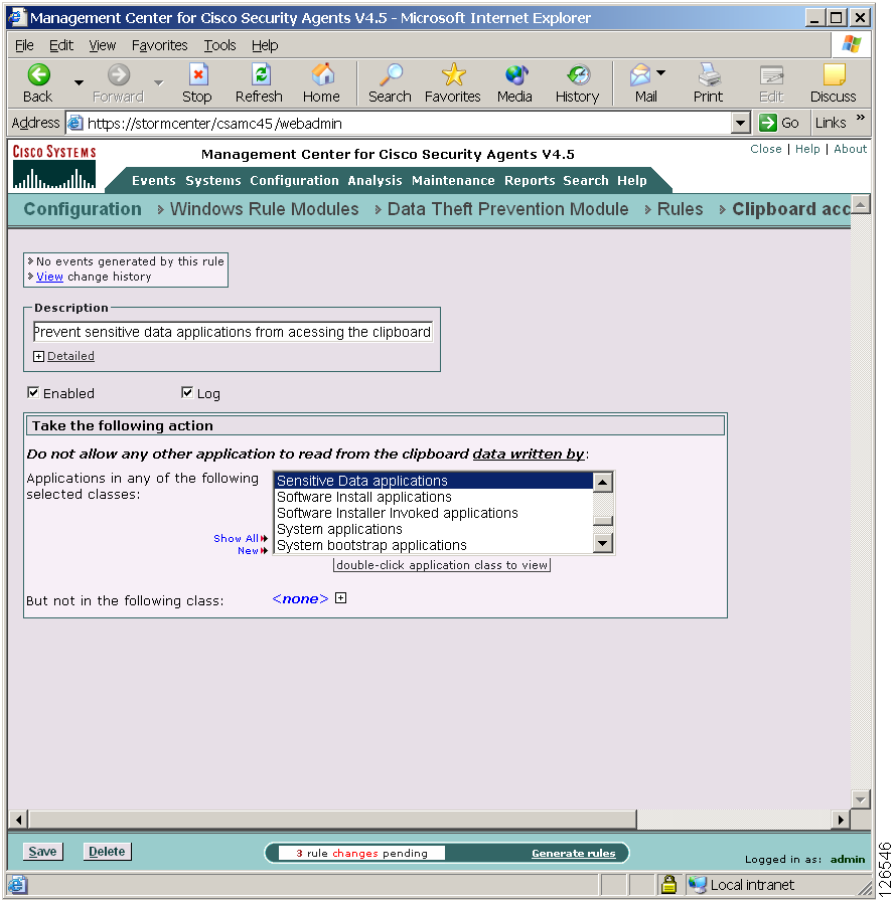
  When your rule is configured, currently selected application classes appear at the top of the list.

- **But not in the following class**—Optionally, select application classes here to exclude from the application class(es) you've selected in the included applications field. Note that the entry <None> is selected by default.

**Step 5** When you are finished configuring your Clipboard access control rule, click the **Save** button.

**Note** If you are using the Clipboard rule to restrict applications from accessing data on the clipboard, the system Print Screen functionality is also automatically disabled.

*Figure 4-21 Clipboard Access Control Rule*




# COM Component Access Control

Use COM component access control rules to allow or deny applications from accessing specified COM components. COM is the Microsoft Component Object Model, the technology that allows objects to interact across process and machine boundaries as easily as within a single process. Each of the Microsoft Office applications (Word, Excel, Powerpoint, etc.)

exposes an "Application" COM component which can be used to create macros or utility scripts. While this is useful functionality, it can be used maliciously by an inadvertently downloaded Visual Basic script.

An example would be the Mydoom virus, which propagated by using the "Outlook.Application" COM component to send itself to each entry in the local address book. Using the COM component access control rule, you can protect specific COM components. For example, you could create a rule which limits access to Office components (Word.*, Outlook.*, Excel.*, etc.)only to the Office applications themselves. Non-Office applications (such as the Visual Basic scripting engine) would therefore be denied access to these components.

**Note** CSA MC provides a COM component import utility which installs with each Cisco Security Agent. Running this utility extracts all COM component PROGID's and CLSID's for software running on the system in question. See Using the COM Extract Utility, page 10-9 for information.

These instructions are a continuation of Configuring Rule Modules, page 4-22.

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **COM component access control** rule. This takes you to the configuration view for this rule type (see Figure 4-26).

**Step 3** Enter the following information

- **Description**—Enter a description of this rule.
  This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.)
  By not selecting this checkbox, you can save this rule, but it will not be active in the policy and it will not be distributed to groups.

**Step 4** **Take the following action**—Select an action type from the pulldown list. For further details on rule action types, see Rules: Action Options and Precedence, page 4-9.

**Step 5** **and**

- **Log**—Enable this checkbox to turn logging on for this rule. Generally, you will want to turn logging on for all deny rules. This means that the denied system action in question is logged and sent to the server at regular time intervals.
- **Take precedence over other <action type> rules**—Enable this checkbox to manipulate rule precedence so that this rule is evaluated before other similar rules. You should generally NOT require this checkbox. Do not use it without understanding how it works. See Rules: Manipulating Precedence, page 4-13 for details.

**Step 6** **When—Applications in any of the following selected classes**

Select one or more preconfigured application classes here to indicate the application(s) whose access to the selected COM components you want to exercise control over.
Note that the entry, <All Applications>, is selected by default. You can use this default or you can unselect it and create your own application classes. For application class configuration details, see Chapter 6, "Using Application Classes".

- **But not in the following class**—Optionally, select application classes here to exclude from the application class(es) you've selected in the included applications field. Note that the entry <None> is selected by default.

**Step 7** **Attempt to access a COM component....matching any of the following component sets**

Click the **Insert COM Component** link to select one or more pre-configured COM component sets for this rule. If you do not want to use a COM component set variable, using the correct syntax, enter a literal PROGID or CLSID (one per line) here. CSA MC provides a utility for extracting PROGID and CLSID information from systems running agent software. See Using the COM Extract Utility, page 10-9 for instructions.

PROGID's, use the following syntax:

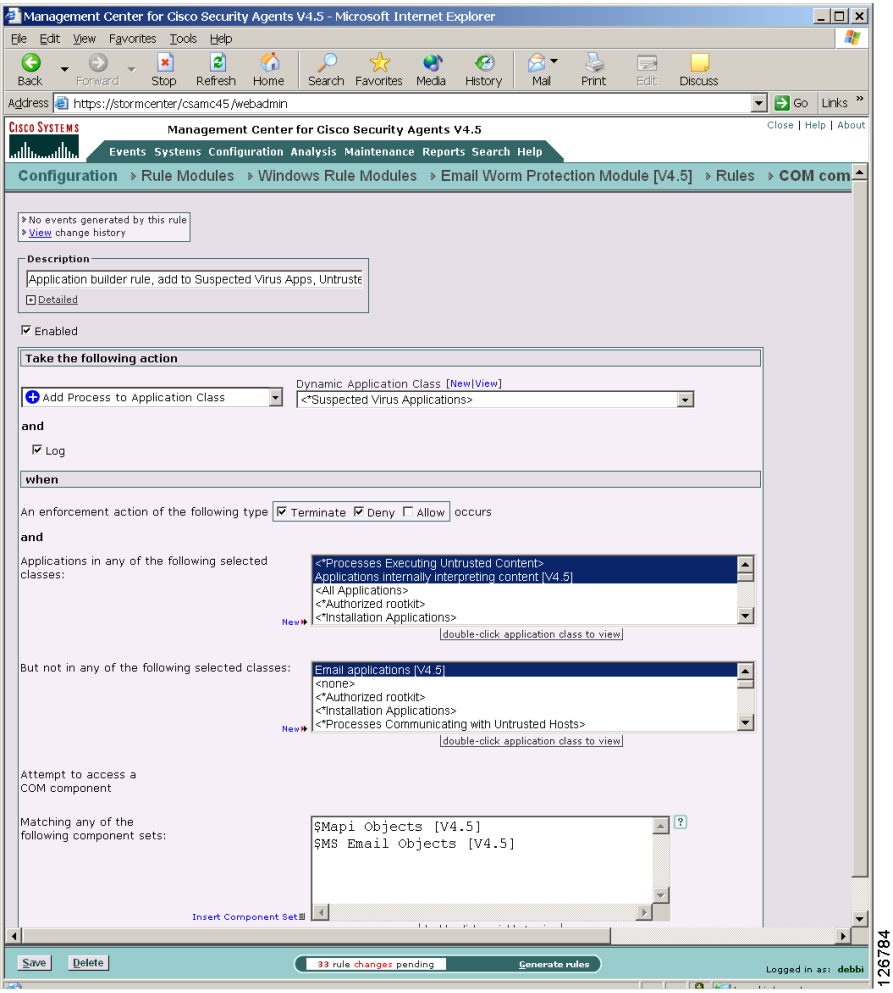
```
Outlook.Application
```

When entering CLSID's (uppercase hexadecimals) using the following syntax, you must include the brackets shown here:

```
{000209FF-0000-0000-C000-000000000046}
```

**Step 8** When you are finished configuring your COM component access control rule, click the **Save** button.

*Figure 4-22 COM Component Access Control Rule*




# File Version Control

Use the File version control rule to control the software versions of applications users can run on their systems. For example, if there is a known security hole in one or more versions of a particular application, this rule would prevent those

specific versions from running, but would allow any versions not included in this rule to run unimpeded.

One particular example where this type of rule would be beneficial is in the case of Microsoft Security Bulletin (MS01-020). This bulletin states the following: "Because HTML e-mail messages are Web pages, Internet Explorer can render them and open binary attachments in a way that is appropriate to their MIME type. However, there is a flaw in the type of processing that is specified for certain unusual MIME types. If a malicious user creates an HTML e-mail message that contains an attachment that can be run and then modifies the MIME header information to specify that the attachment is one of the unusual MIME types that Internet Explorer handles incorrectly, Internet Explorer may run the attachment automatically when it renders the e-mail message."

Microsoft has a patch to correct this security problem, but the patch is only available for Internet Explorer 5.01 Service Pack 1 and IE 5.5. If users are running an earlier version of IE, they must upgrade to 5.01 or 5.5 and install the correct service packs and patches to correct the problem. Therefore, earlier versions of IE contain an unfixable security problem and you will want to prevent users from running these versions. The following configuration information uses the IE security bulletin as an example.

**Note** Note that users can get around a File version control rule by copying the file in question to a different file name. Therefore you must assume that users are working in cooperation with you for these rule types to be successful. You could also create a File access control rule to prevent users from changing the application file name in question.

**Note** These instructions are a continuation of Configuring Rule Modules, page 4-22.

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **File version control** rule. This takes you to the configuration view for this rule type.

**Step 3** In the File version control rule configuration view, enter the following information:

- **Description**—Enter a description of this rule. This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the policy. (It is enabled by default.) By not selecting this checkbox, you can save this rule, but it will not be active in the module and it will not be distributed to groups.

**Step 4** **Take the following action**—Select an action type from the pulldown list. For further details on rule action types, see Rules: Action Options and Precedence, page 4-9.

**Step 5** and

- **Log**—Enable this checkbox to turn logging on for this rule. Generally, you will want to turn logging on for all deny rules. This means that the denied system action in question is logged and sent to the server at regular time intervals.
- **Take precedence over other <action type> rules**—Enable this checkbox to manipulate rule precedence so that this rule is evaluated before other similar rules. You should generally NOT require this checkbox. Do not use it without understanding how it works. See Rules: Manipulating Precedence, page 4-13 for details.

**Step 6** **When An execution of the following**

Enter the **File** you are prohibiting (You will enter the exact version in the next field.) This field accepts file entries for `.exe`, `.dll`, and `.ocx` files. Enter just the file name here. No path is required.

For example: `iexplore.exe`

You cannot use wildcard entries in this field.

**Step 7** **with version within these Version ranges**

Enter the version or version range (using a dash to indicate range) of the file you entered in the previous field.

For example: `0-5.00.3314.2100`
`5.00.3314.2100-5.50.4522.1800`

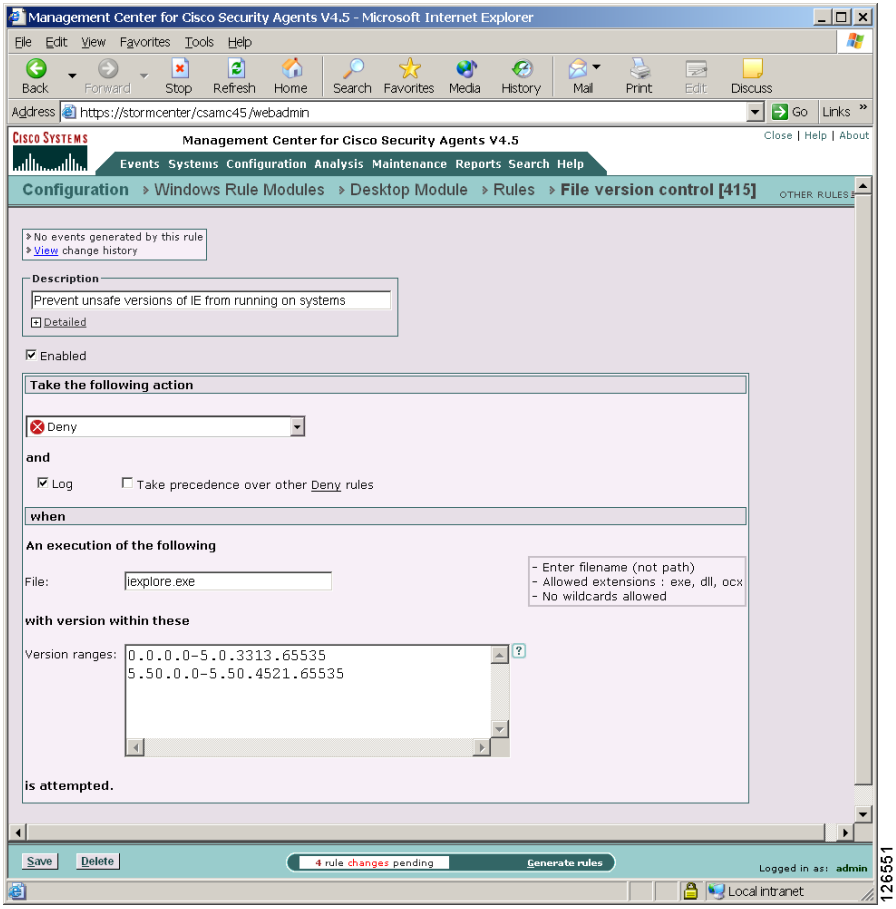
You can enter multiple, nonconsecutive ranges by entering versions on separate lines in this field.

To locate the version of a file (*.exe, *.dll, or *.ocx), select the file and right click. Select **Properties**. Click the **Version** tab. The File version is normally 4 values separated by dots.

**Note** When entering version numbers for Microsoft applications, refer to the Microsoft web site. Application version numbers accessible from the application itself sometimes correspond to slightly different version numbers in Microsoft version charts. For example, Microsoft Article number Q164539 was used to determine the version numbers for this File version control rule.

**Step 8** Click the **Save** button when you are finished.

*Figure 4-23 File Version Control Rule*



# Kernel Protection

Use the Kernel protection rule to prevent unauthorized access to the operating system. In effect, this rule prevents drivers from dynamically loading after system startup. You can specify exceptions to this rule for authorized drivers that you are allowing to load any time after the system is finished booting.

You can also use this rule to only detect unauthorized access to or modification of the operating system at any time.

**Note** These instructions are a continuation of Configuring Rule Modules, page 4-22.

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **Kernel protection** rule. This takes you to the configuration view for this rule type.

**Step 3** Enter the following:

- **Description**—Enter a description of this rule. This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.) By not selecting this checkbox, you can save this rule, but it will not be active in the module and it will not be distributed to groups.

**Step 4** **Take the following action**—Select an action type from the pulldown list. For further details on rule action types, see Rules: Action Options and Precedence, page 4-9. Note that High Priority Deny, Allow, Deny, Add Process to Application Class, and Monitor are the only action types available. If you select Add Process to Application Class, the two classes you are adding a given process to are either Authorized rootkit or Unauthorized rootkit.

**Step 5** and

- **Log**—Enable this checkbox to turn logging on for this rule. Generally, you will want to turn logging on for all deny rules. This means that the denied system action in question is logged and sent to the server at regular time intervals.

- **Take precedence over other <action type> rules**—Enable this checkbox to manipulate rule precedence so that this rule is evaluated before other similar rules. You should generally NOT require this checkbox. Do not use it without understanding how it works. See Rules: Manipulating Precedence, page 4-13 for details.

**Step 6** when

- **Modules load after system startup**

  The default here is <none>. You can use this rule type to prevent drivers from dynamically loading after system startup. You can also specify exceptions to this rule for authorized drivers that you are allowing to load any time after the system is finished booting.

**Caution** This part of the rule only detects unauthorized access to the operating system and does not prevent it. Upon this detection, you can impose stringent network restrictions by selecting the Restrict network connectivity... checkbox.

- **Modules modify kernel functionality**

  When modules are detected modifying the system, selecting this checkbox causes the system in question to log this event. You can use this detection to create dynamic rootkit application classes and to change the system state to a state that enforces a more restrictive policy.

  You should only create Allow exceptions for actions you believe are safe. For example, virus-scanners and kernel debuggers might legitimately trigger this rule. Enters module data in the following edit fields:

  – **Module hashes to be excluded**

    By default, this field contains <all>. Enter hashes and/or drivers that identify kernel modules (e.g. drivers) into this field in the following format: 20 character hash\file system path\driver name. You can use wildcards for entries, as well. You can also use the wizard from the event in question to enter the module hash and driver information here. Some examples of valid entries are as follows:

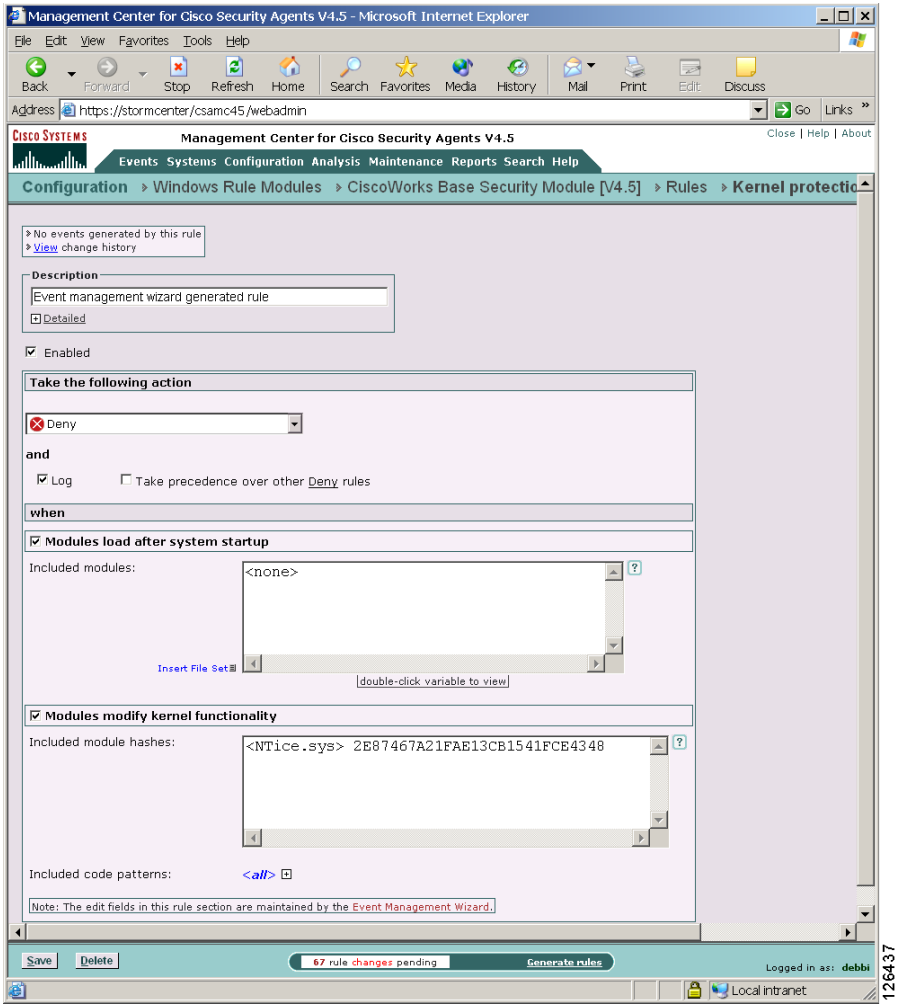
    ```
    *\**\system32\Drivers\uphcleanhlp.sys
    ae45e23b45093dffa899\**
    ae45e23b45093dffa899\**\uphcleanhlp.sys
    ```

  – **Code patterns to be excluded**

By default, this field contains <all> . The wizard enters code patterns (not inside any module) into this field.

**Step 7** Click **Save** when finished.

***Figure 4-24 Kernel Protection Rule***



# NT Event Log

Use the NT Event log rule to have specified NT Event Log items appear in the CSA MC Event Log for selected groups.

**Note** These instructions are a continuation of Configuring Rule Modules, page 4-22.

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **NT Event log** rule. This takes you to the configuration view for this rule type (see Figure 4-25).

**Step 3** Enter the following information:

- **Description**—Enter a description of this rule.
  This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.)
  By not selecting this checkbox, you can save this rule, but it will not be active in the module and it will not be distributed to groups.

**Step 4** **Log events from the event log**

- **Include events matching the following**—Select this radio button to specify the criteria for NT Event Log entries which you want to appear in the CSA MC Event Log.
- **Include all events except those matching the following**—Select this radio button to specify the criteria for NT Event Log entries which you do not want to appear in the CSA MC Event Log. (All criteria not specified here will appear in the CSA MC Event Log.)

**Note** You can configure CSA MC to correlate NT event types logged across multiple systems. You can also correlate NT events received from virus scanners running on agent systems and quarantine contaminated files. See Installation Applications Policy, page 5-19.

**Step 5** **Criteria** (You should select at least one for the rule to have any effect.)

- **Event Log Type**—Select one or more checkboxes here to indicate which NT Event Log entries you want to appear (first radio button above) or which entries you want to not appear (second radio button above) in CSA MC Event Logs.

  The choices are—**System**, **Application**, **Security**

- **Event Source**—In the text field, enter (one per line) event source parameters you want to filter by.
  The event source is the software that logged the event, which can be either an application name, such as `SQL Server`, or a component of the system or of a large application, such as a driver name. For example, `Elnkii` indicates the EtherLink II driver.

- **Event Severity (Type)**—Select one or more checkboxes to filter the viewing of events according to severity. If you select no checkboxes, all severity levels are included in the rule.

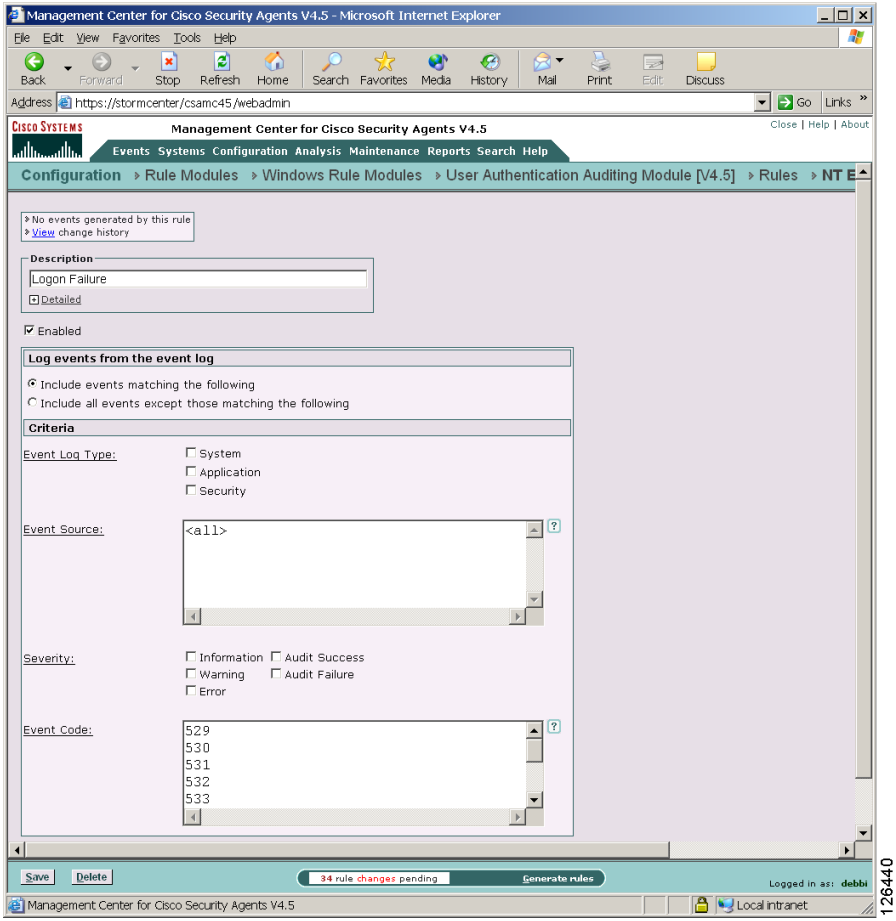
  The choices are—**Information**, **Warning**, **Error**, **Audit Success**, **Audit Failure**

- **Event Code (Event ID)**—In the text field, enter (one per line) event code parameters you want to filter by.
  The event code is the number identifying the particular event type. For example, 6005 is the ID of the event that occurs when the Event log service is started. You can find the event IDs for Windows security events by searching for the following articles on the Microsoft web site: Q174074, Q299475, and Q301677.

**Step 6** Click the **Save** button.

**Note** To receive messages logged by Norton AntiVirus and for global correlation, select the **Application** checkbox and enter `Norton AntiVirus` in the Event Source edit box. See Installation Applications Policy, page 5-19 for more information.

*Figure 4-25 NT Event Log Rule*



# Registry Access Control

Use registry access control rules to allow or deny applications from writing to specified registry keys.

**Note** These instructions are a continuation of Configuring Rule Modules, page 4-22.

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **Registry access control** rule. This takes you to the configuration view for this rule type.

**Step 3** Enter the following information:

- **Description**—Enter a description of this rule.
  This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.)
  By not selecting this checkbox, you can save this rule, but it will not be active in the module and it will not be distributed to groups.

**Step 4** **Take the following action**—Select an action type from the pulldown list. For further details on rule action types, see Rules: Action Options and Precedence, page 4-9.

**Step 5** and

- **Log**—Enable this checkbox to turn logging on for this rule. Generally, you will want to turn logging on for all deny rules. This means that the denied system action in question is logged and sent to the server at regular time intervals.
- **Take precedence over other <action type> rules**—Enable this checkbox to manipulate rule precedence so that this rule is evaluated before other similar rules. You should generally NOT require this checkbox. Do not use it without understanding how it works. See Rules: Manipulating Precedence, page 4-13 for details.

**Step 6** **When—Applications in any of the following selected classes**

Select one or more preconfigured application classes here to indicate the application(s) whose access to the selected registry keys you want to exercise control over.
Note that the entry, <All Applications>, is selected by default. You can use this default or you can unselect it and create your own application classes. For application class configuration details, *see* Chapter 6, "Using Application Classes".

- **But not in the following class**—Optionally, select application classes here to exclude from the application class(es) you've selected in the included applications field. Note that the entry <None> is selected by default.

**Step 7** **Attempt to write to any of these registry entries**

Click the **Insert Registry Set** link to select one or more pre-configured registry sets for this rule. See Included Registry Sets, page 7-23 for details on included operating system registry values.

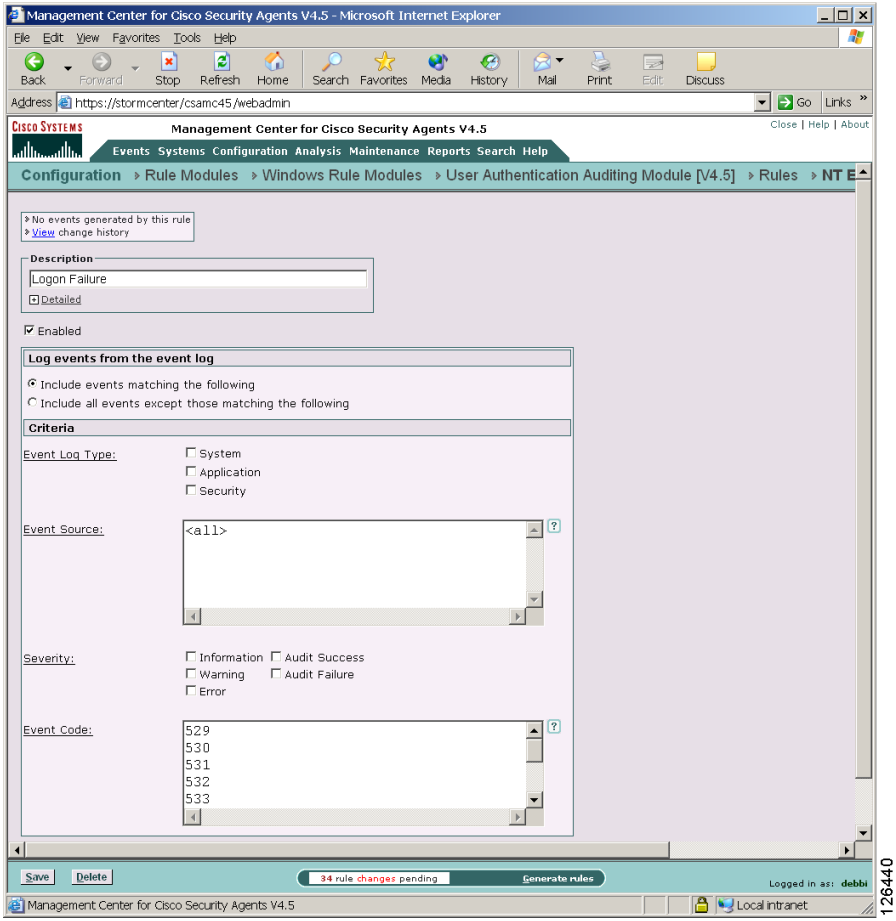
**Note** You cannot enter registry literals here. You must create a registry set variable if you are not using pre-configured registry sets.

**Step 8** When you are finished configuring your Registry access control rule, click the **Save** button.

This rule is now part of your rule module. It takes effect when the policy to which it is associated is attached to a group and then downloaded by an agent on the network.

**Caution** In order to distribute rules to the correct hosts, you must associate policies with groups and then Generate rules. See page 4-111 and page 4-118 for instructions.

*Figure 4-26 Registry Access Control Rule*



# Service Restart

Use the Service restart rule to have the agent restart Windows NT services that have gone down on a system or are simply not responding to service requests.

**Note** These instructions are a continuation of Configuring Rule Modules, page 4-22.

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **Service restart** rule. This takes you to the configuration view for this rule type (see Figure 4-27).

**Step 3** Enter the following information:

- **Description**—Enter a description of this rule.
  This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.)
  By not selecting this checkbox, you can save this rule, but it will not be active in the module and it will not be distributed to groups.
- **Log**—Enable this checkbox to turn logging on for this rule.

**Step 4** **Restart the following service**

Enter a service here you want the agent to automatically restart should it go down for any reason. When entering services here, use the syntax found in the following locations:

- On Windows XP and Windows 2003 and 2000: Start>Settings>Control Panel>Administrative Tools>Services "Name" field
- On Windows NT: Start>Settings>Control Panel>Services "Service" field

**Step 5** **When**

Select one or both of the following checkboxes.

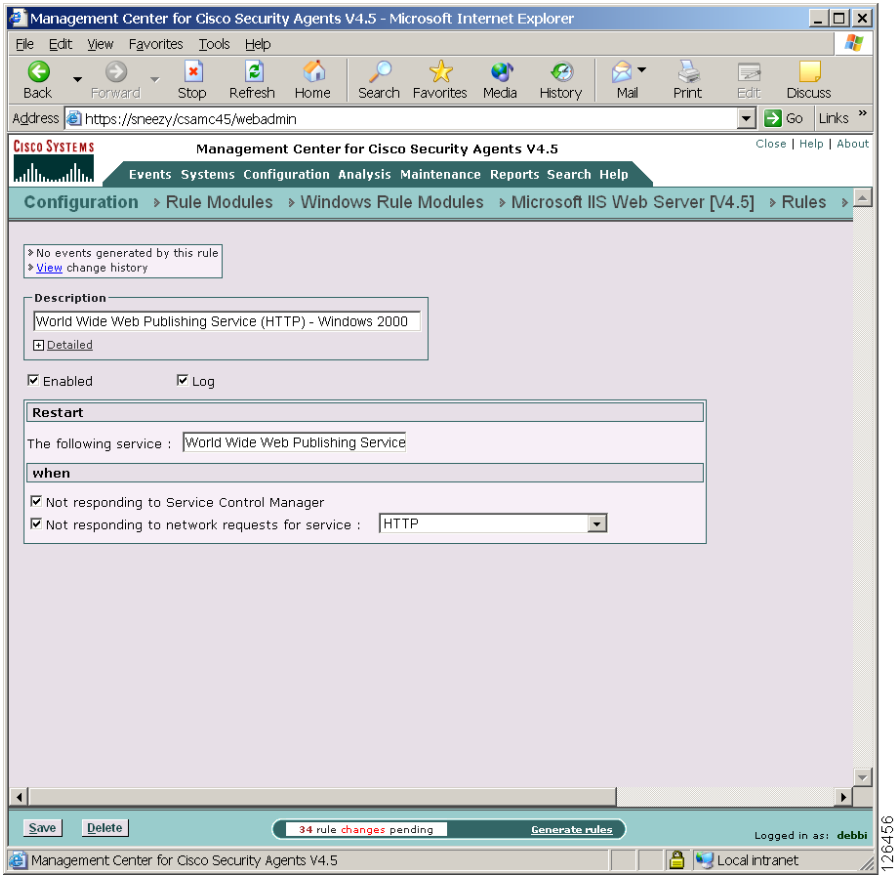
- Not responding to Service Control Manager The Windows Service Control Manager checks the status of system services and recognizes when a service is not responding. Selecting this checkbox causes the Cisco Security Agent to restart the specified service when it does not respond to the Windows Service Control Manager.
- Not responding to network requests for service: Select this checkbox and then choose a network service (such as HTTP) from the available pulldown list. The Cisco Security Agent will monitor whether the system is responding to network requests for the protocols in the network service. If not, it will restart the Windows NT service specified in this rule.

**Caution** An agent must have the network shim enabled in order for the "Not responding to network requests for service" feature to work.

**Step 6** Click **Save** when finished.

**Note** The Service Restart rule is different from the Windows NT configurable restart service. Windows NT only restarts processes that have gone away. The agent restarts a process that experiences a failure of any kind.

*Figure 4-27 Service Restart Rule*



# Sniffer and Protocol Detection

Use the Sniffer and protocol detection rule to cause an event to be logged when non-IP protocols and packet sniffer programs are detected running on systems.

Non-IP protocols, such as IPX, AppleTalk, and NetBEUI, are used to provide distributed computing workgroup functions between server and clients and/or sharing between peer clients.

A packet sniffer (also controlled by this rule type) is a program that monitors and analyzes network traffic. Using this information, a network manager can troubleshoot network problems. A sniffer can also be used illegitimately to capture data being transmitted on a network. Sensitive information such as login names and passwords can be extracted from this data and used to break into systems.

The Sniffer and protocol detection rule is a monitoring tool. By adding this rule to a policy, you are causing an event to be logged when any non-IP protocols and packet sniffer programs are detected running on systems which receive this rule.

**Note** You can use the Sniffer and protocol detection rule page to configure exceptions to this monitoring rule. If you select any non-IP protocols or enter any packet sniffer programs here, you are allowing them to run on systems without generating events. Only non-IP protocols and packet sniffer programs which you explicitly exclude as part of the rule will not cause events to be logged. Otherwise, all are monitored when you add this rule to a policy.

These instructions are a continuation of Configuring Rule Modules, page 4-22.

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **Sniffer and protocol detection** rule. This takes you to the configuration view for this rule type (see Figure 4-26).

**Step 3** Enter the following information:

- **Description**—Enter a description of this rule.
  This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.)
  By not selecting this checkbox, you can save this rule, but it will not be active in the policy and it will not be distributed to groups.

**Step 4** Select one or more preconfigured **Standard protocols** here to be excluded as part of this rule. The protocols you select here are the only non-IP protocols that will not generate events when they are detected.

If the non-IP protocol(s) you want to exclude are not included in the Standard Protocols list, enter your own in the **Non-standard protocols and packet sniffers** text field. By default, TCP/IP Protocol is already excluded.

This is also where you should enter any packet sniffer programs you want to exclude from this rule. (Find the names for these programs in Cisco Security Agent log files or in system registries.) For example, enter:

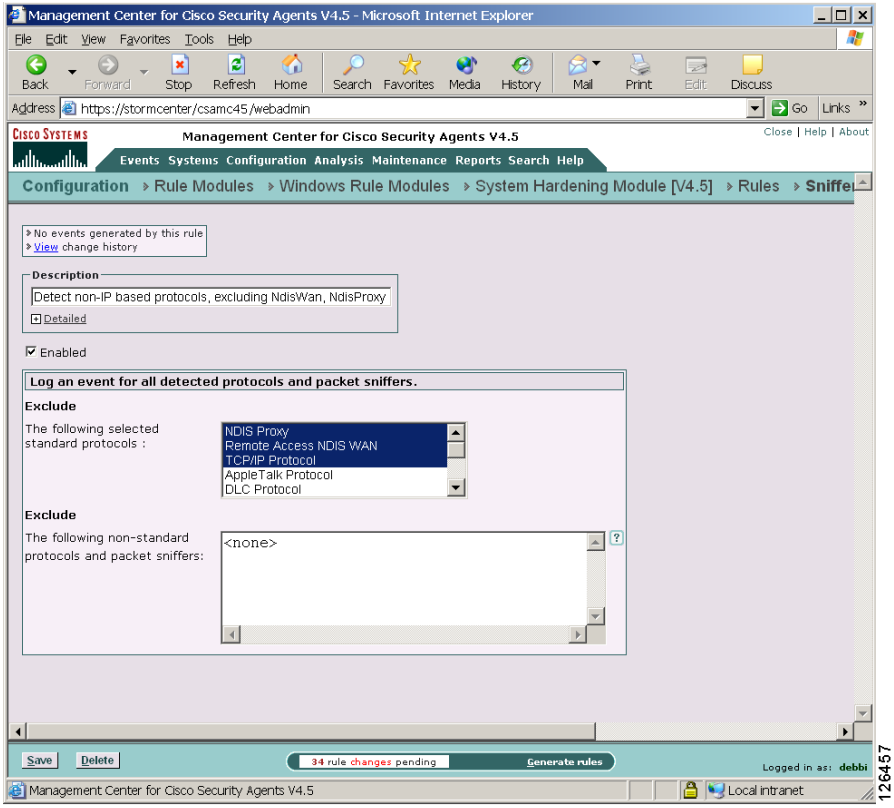
```
PacketDriver
```

In this example, Windump is the application. The libcap packet capture driver registers using the name PacketDriver.

**Step 5** Click the **Save** button.

**Note** If you have multiple sniffer and protocol detection rules, the exceptions are combined.

*Figure 4-28 Sniffer and Protocol Detection Rule*



# UNIX Only Rules

The following rules are only available for UNIX Rule Modules.

## Network Interface Control

Use the Network interface control rule to specify whether applications can open a device and act as a sniffer (promiscuous mode). A packet sniffer is a program that monitors and analyzes network traffic. Using this information, a network manager can troubleshoot network problems. A sniffer can also be used illegitimately to capture data being transmitted on a network. Sensitive information such as login names and passwords can be extracted from this data and used to break into systems.

These instructions are a continuation of Configuring Rule Modules, page 4-22.

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **Network interface control** rule. This takes you to the configuration view for this rule type (see Figure 4-29).

**Step 3** Enter the following information:

- **Description**—Enter a description of this rule.
  This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.)
  By not selecting this checkbox, you can save this rule, but it will not be active in the module and it will not be distributed to groups.

**Step 4** **Take the following action**—Select an action type from the pulldown list. For further details on rule action types, see Rules: Action Options and Precedence, page 4-9.

**Step 5** and

- **Log**—Enable this checkbox to turn logging on for this rule. Generally, you will want to turn logging on for all deny rules. This means that the denied system action in question is logged and sent to the server at regular time intervals.

- **Take precedence over other <action type> rules**—Enable this checkbox to manipulate policy rule precedence so that this rule is evaluated before other similar rules. You should generally NOT require this checkbox. Do not use it without understanding how it works. See Rules: Manipulating Precedence, page 4-13 for details.

**Step 6** **When—Applications in any of the following selected classes**

Select one or more preconfigured application classes here to indicate the application(s) whose access to the selected resource(s) want to exercise control over.
Note that the entry, <All Applications>, is selected by default. You can use this default or you can unselect it and create your own application classes. For application class configuration details, see Chapter 6, "Using Application Classes".

**Step 7** **Attempt the following operations**

Select one or more of the following checkboxes:

- Open a stream connection to the NIC driver

**Note** Open a stream connection to the NIC driver - For Linux systems, this only applies to modification of the interface characteristics, e.g. using ifconfig to modify an interface's network mask. This does not apply to simply reading the interface characteristics.

- Put the NIC into promiscuous mode

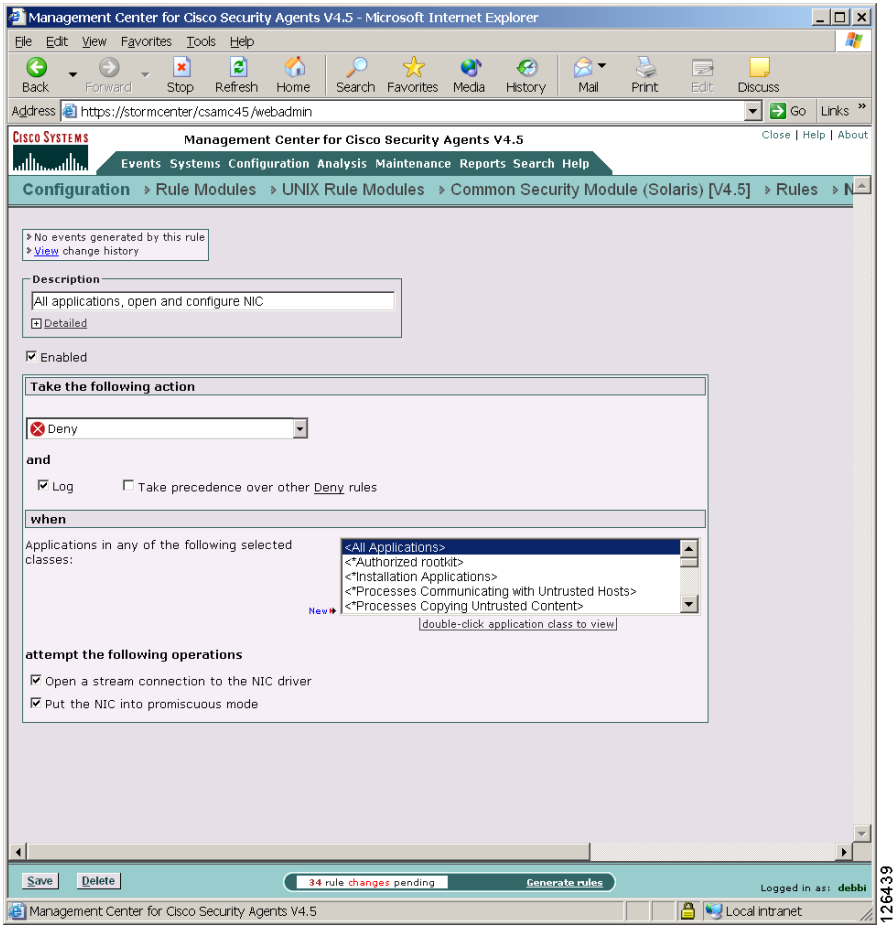
**Note** If you have selected the Allow radio button, when you select to "Put the NIC into promiscuous mode", the "Open a stream connection to the NIC driver" checkbox is also automatically selected. It must be enabled for promiscuous mode to work.

Conversely, if you have selected a Deny radio button, when you select the "Open a stream connection to the NIC driver" checkbox, the "Put the NIC into promiscuous mode" checkbox is also automatically selected. If you deny one, the other is automatically denied as well.

**Step 8** When you are finished configuring your rule, click the **Save** button.

**Note** If you are using remote management tools and you are configuring a Network interface control rule to deny "all applications" from opening a stream connection to the NIC and operating in promiscuous mode, you may want to make an exception for the remote management application (if you want to run snoop).

***Figure 4-29 Network Interface Control Rule***



# Resource Access Control

Use the Resource access control rule to protect systems from symbolic link attacks. In this type of attack, an attacker attempts to determine the name of a temporary file prior to its creation by a known application. If the name is determined correctly, the attacker could then create a symbolic link to the target file for which the user of the application has write permissions. The application process would then overwrite the contents of the target file with its own output when it tries to write the named temporary file.

For example, a directory such as /tmp is writable by everyone. An attacker could create a symbolic link in this directory to a protected file such as /etc/shadow. A superuser process may then unwittingly write to or copy from /etc/shadow. This would then grant the attacker access to this sensitive information via a symbolic link from the /tmp directory.

By enabling the resource access control rule, you can prevent "suspicious" symbolic links from being followed. A suspicious symbolic link is one that meets all of the following criteria:

- The parent directory is a temporary directory such as /tmp and /usr/tmp
- The symbolic link's owner is different from the parent directory's owner
- The symbolic link's owner is different from the effective UID of the process

These instructions are a continuation of Configuring Rule Modules, page 4-22.

---

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **Resource access control** rule. This takes you to the configuration view for this rule type (see Figure 4-31).

**Step 3** Enter the following information:

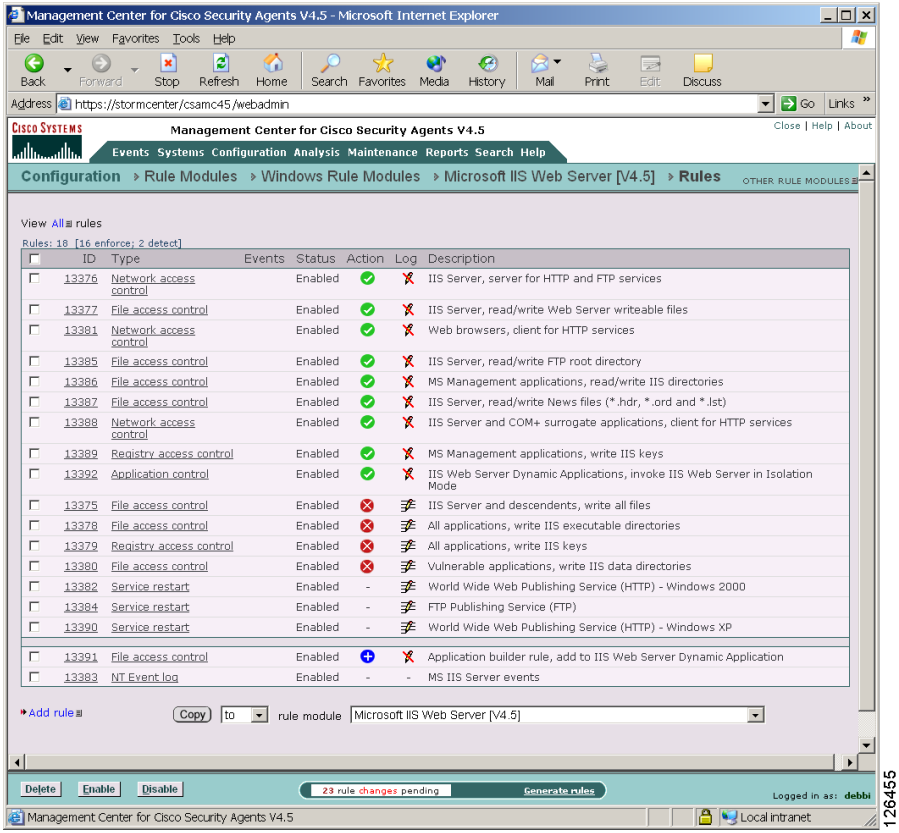
- **Description**—Enter a description of this rule.
  This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.)
  By not selecting this checkbox, you can save this rule, but it will not be active in the module and it will not be distributed to groups.

**Step 4** Select the **Symbolic Link Protection** checkbox to turn on that functionality.

**Step 5** Click the **Save** button.

**Caution** **Symbolic Links**: If you create a File access control rule to protect a symbolic link, ONLY that symbolic link is protected. The underlying resource, unless also specified, is NOT protected. For example, a File access control rule written for `/etc/hosts` does not protect `/etc/inet/hosts`. Similarly, a File access control rule written for `/etc/inet/hosts` does not protect `/etc/hosts`. If you want to protect a symbolic link and its underlying resource, both must be specified in the rule.

***Figure 4-30 Resource Access Control Rule***



# Rootkit / kernel Protection

Use the Rootkit / kernel protection rule to control unauthorized access to the operating system. In effect, this rule controls drivers attempting to dynamically load after boot time. You can use to this rule to specify authorized drivers that you are allowing to load any time after the system is finished booting.

**Note** These instructions are a continuation of Configuring Rule Modules, page 4-22.

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **Rootkit / kernel protection** rule. This takes you to the configuration view for this rule type (see Figure 4-31).

**Step 3** Enter the following information:

- **Description**—Enter a description of this rule.
  This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.)
  By not selecting this checkbox, you can save this rule, but it will not be active in the policy and it will not be distributed to groups.

**Step 4** **Take the following action**—Select an action type from the pulldown list. For further details on rule action types, see Rules: Action Options and Precedence, page 4-9.

**Step 5** and

- **Log**—Enable this checkbox to turn logging on for this rule. Generally, you will want to turn logging on for all deny rules. This means that the denied system action in question is logged and sent to the server at regular time intervals.
- **Take precedence over other <action type> rules**—Enable this checkbox to manipulate policy rule precedence so that this rule is evaluated before other similar rules. You should generally NOT require this checkbox. Do not use it without understanding how it works. See Rules: Manipulating Precedence, page 4-13 for details.

**Step 6** **When—Applications in any of the following selected classes**

Select one or more preconfigured application classes here to indicate the application(s) whose access to the selected resource(s) want to exercise control over.
Note that the entry, <All Applications>, is selected by default. You can use this default or you can unselect it and create your own application classes. For application class configuration details, see Chapter 6, "Using Application Classes".

- **But not in any of the selected classes**—Optionally, select application classes here to exclude from the application class(es) you've selected in the included applications field. Note that the entry <None> is selected by default.

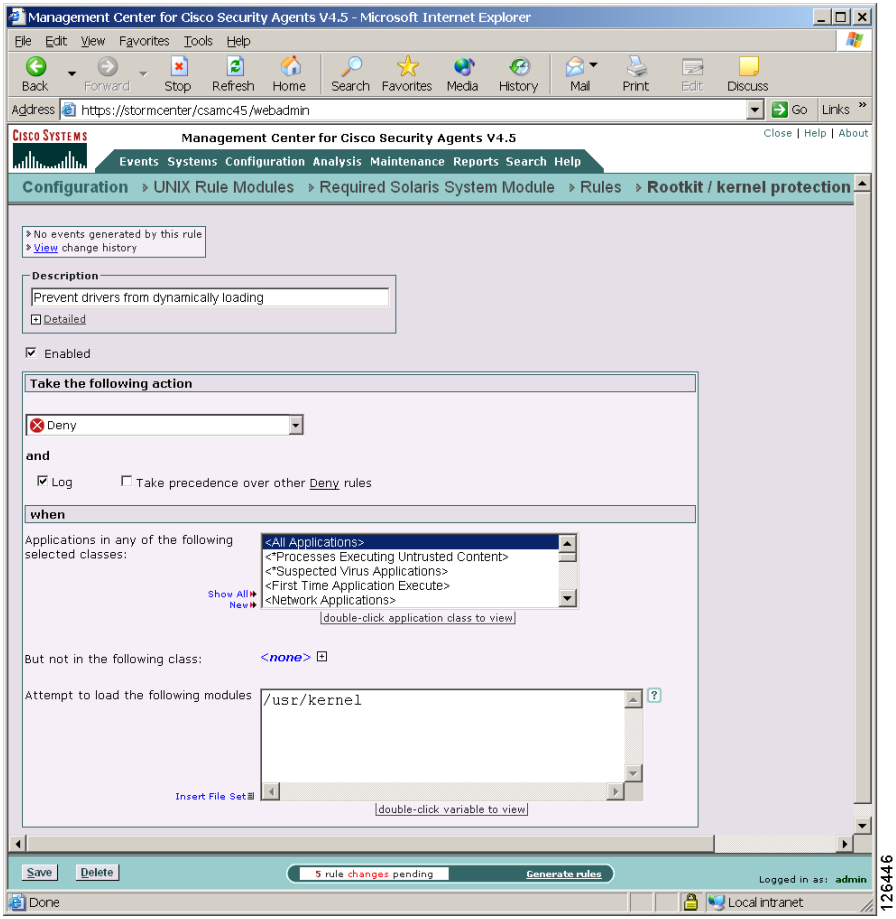
**Step 7** **Attempt to load the following modules**

By default, this field contains <none> which indicates no specified drivers. Enter the names of drivers you want to specify for this the rule and therefore allow, deny, or monitor the loading of at any time.

**Caution** If you enter file sets which use "content-matching" constraints, via the Insert File Set link, the content-matching constraints are ignored.

**Step 8** Click the **Save** button.

*Figure 4-31 Rootkit / kernel Protection Rule*



# Syslog Control

Use the Syslog control rule to have specified Solaris and Linux Syslog items appear in the CSA MC Event Log for selected groups.

**Note** These instructions are a continuation of Configuring Rule Modules, page 4-22.

**Step 1** To add rules to your module, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **Syslog control** rule. This takes you to the configuration view for this rule type (see Figure 4-32).

**Step 3** Enter the following information:

- **Description**—Enter a description of this rule.
  This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.)
  By not selecting this checkbox, you can save this rule, but it will not be active in the module and it will not be distributed to groups.

**Step 4** **Log events from syslog**

- **Include events matching the following**—Select this radio button to specify the criteria for Syslog entries which you want to appear in the CSA MC Event Log.
- **Include all events except those matching the following**—Select this radio button to specify the criteria for Syslog entries which you do not want to appear in the CSA MC Event Log. (All criteria not specified here will appear in the CSA MC Event Log.)

**Note** You can configure CSA MC to correlate Syslog events logged across multiple systems. See Installation Applications Policy, page 5-19.

**Step 5** **Criteria** (You should select at least one for the rule to have any effect.)

- **Event Source**—In the text field, enter (one per line) event source parameters you want to filter by.
  The event source is the software that logged the event, which can be an application name such as `/sbin/dhcpagent`, a kernel level driver module such as `scsi`, or the `unix` kernel itself.
- **Facility**—Select one or more items from the list box you want to appear (first radio button above) or which entries you want to not appear (second radio button above) in CSA MC Event Logs.
- **Priority**—Select one more checkboxes by which to filter the viewing of events according to priority. If you select no checkboxes, all priorities are included in the rule.
- **Message Pattern**—In the text field, enter (one per line) message patterns you want to match and filter by. To match, the string you enter must literally appear somewhere within the message.

**Step 6** Click the **Save** button.

**Note** On Linux platforms, the default syslogd does not embed the facility or priority level in the syslog messages. Using a different syslogd, such as syslog-ng, with correct message formatting, it is possible to use the facility and/or priority levels to report these events. Therefore, if syslog-ng is used, the message template must take the following form:

template("$DATE $HOST $PROGRAM: [ID 0 $FACILITY.$LEVEL] $MSG\n")

For example, the entry for content recorded into /var/log/messages would appear as follows:

```
destination d_1 {
file("/var/log/messages" create_dirs(yes) template("$DATE $HOST
$PROGRAM: [ID 0 $FACILITY.$LEVEL]
$MSG\n")); };
```

## General Syslog rule configuration examples

For Example:

Configure a syslog rule to log warning messages such as the one listed here:

```
Apr 29 13:46:35 myhost /sbin/dhcpagent[39]: [ID 929444
daemon.warning] configure_if: no IP broadcast specified
for eri0
```

To get every message of category “warning” from the /sbin/dhcpagent daemon, you would configure your syslog rule in the following manner (See Figure 4-32):

Select the "Include events matching the following" radio button and enter:

- Facility: daemon
- Event Source: /sbin/dhcpagent
- Priority: Warning checkbox
- Message Pattern: <all>

For Example:

Configure a syslog rule to log failed su root attempts such as the one listed here:

```
Apr 29 13:49:23 myhost su: [ID 810491 auth.crit] 'su
root' failed for haxor on /dev/pts/4
```

To get messages for failed su root attempts, you would configure your syslog rule in the following manner:

Select the "Include events matching the following" radio button and enter:

- Facility: auth
- Event Source: su
- Priority: Alert and Above checkbox
- Message Pattern: root

For Example:

Configure a syslog rule to include all events but exclude all lockstat-related messages such as the one listed here:

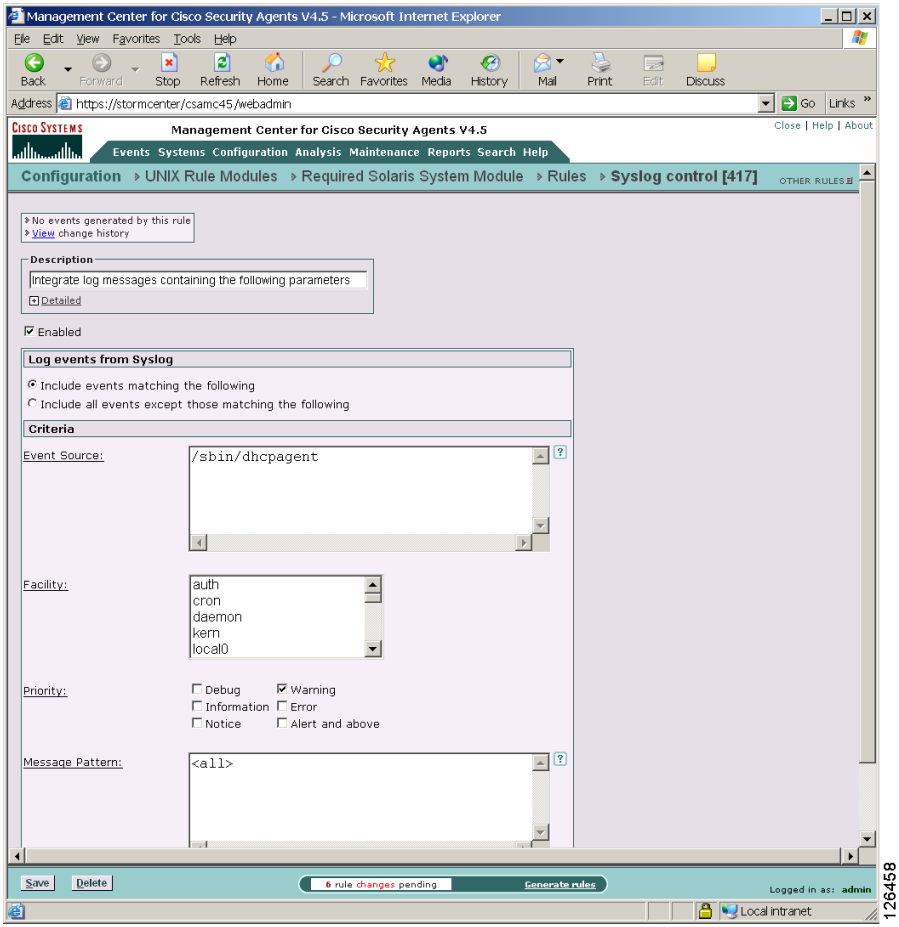
```
Apr 29 13:46:43 myhost genunix: [ID 936769 kern.info]
lockstat0 is /pseudo/lockstat@0
```

To log all events except for lockstat-related messages, configure your rule in the following manner:

Select the "Include events except those matching the following" radio button and enter:

- Facility: kern
- Event Source: <all>
- Priority: all checkboxes
- Message Pattern: lockstat

***Figure 4-32 Syslog Control Rule***



# Attaching Rule Modules to Policies

When you configure a rule module, you are combining access control rules and/or tagging and monitoring rules under a common name. That rule module name is then attached to a policy. That policy uses the rules that comprise the module to control the actions that are allowed and denied on hosts. See Configuring Rule Modules, page 4-22.

CSA MC gives you the option of attaching a rule module to a policy using the **Modify policy associations** link in the Rule Module configuration page or attaching a policy to a rule module using the **Modify rule module associations** link in the Policy list view page.

To attach a rule module or rule modules to an existing policy using the **Modify policy associations** link in the rule module configuration page, do the following.

**Step 1** Attach a rule module to a particular policy by accessing that rule module's edit view. From **Configuration** in the menu bar, click on **Rule Modules** for the OS type you want to access the list view for those modules.

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

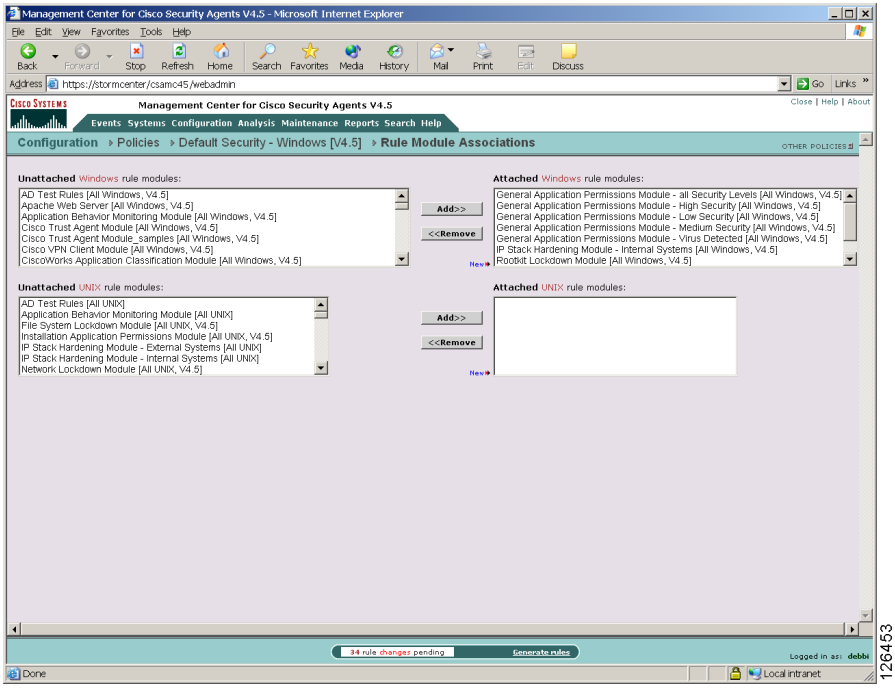
**Step 3** From the edit view, click the **Modify policy associations** link. This takes you to a page containing swap boxes. See Figure 4-33. The left box contains the policies the rule module is not attached to. The right box contains policies that the rule module is attached to.

**Step 4** To add this rule module to an existing policy, select the rule module in the left box and click the **Add** button. The selected rule module moves to the right box and is now attached to the policy.

**Note** You can attach rule modules of differing architectures to the same policy. This way, you can configure task-specific, self-contained, inclusive policies across all supported architectures for software that is supported on all platforms. For example, Apache is a web server software product that supports Windows, Linux, and Solaris platforms. You can attach three OS specific rule modules for Apache to one policy and only need to maintain that one Apache policy.

**Caution** In order to deploy rule modules to hosts, you must remember to attach the policy that the rule module is associated with to a group.

***Figure 4-33 Rule Module Associations***




# Attaching Policies to Groups

When you configure a policy, you are combining configured rule modules under a common name. That policy name is then attached to a group of hosts and it uses the rules that comprise the policy to control the actions that are allowed and denied on those hosts. See Configuring Rule Modules, page 4-22.

CSA MC gives you the option of attaching a policy to a group using the **Modify policy associations** link in the Group configuration page or attaching a group to a policy using the **Modify group associations** link in the Policy list view page.

(You can use the Modify policy associations link to attach multiple policies to a group and use the Modify group association link to attach one policy to multiple groups.)

To attach a policy or policies to an existing group using the **Modify policy associations** link in the Group configuration page, do the following.

**Step 1** Attach a policy to a particular group by accessing that group's edit view. From **Systems** in the menu bar, click on **Groups** to access the group's list view.

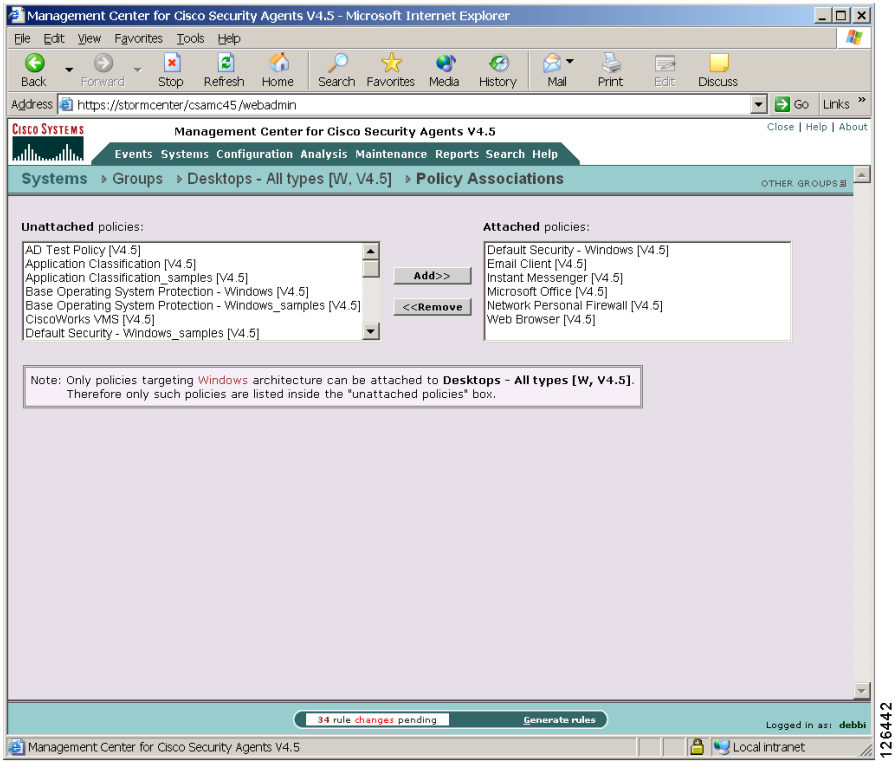
**Step 2** From the group list view, click the link for the group you want to attach a policy to. This brings you to that group's edit view.

**Step 3** From the edit view, click the **Modify policy associations** link. This takes you to a page containing swap boxes (see Figure 4-34). The left box contains the policies not attached to this group. The right box contains policies that are attached to this group.

**Step 4** To add an existing policy to this group, select the policy in the left box and click the **Add** button. The selected policy moves to the right box and is now attached to the group.

**Note** To remove a policy from a group, select the policy in the right box and click the **Remove** button. It moves back to the left box. (The policy is not deleted from the database, it is just no longer applied to the group.) Although the selected policy is no longer attached to the group, this is not apparent in the GUI until you click the **Generate rules** link in the bottom frame and then the **Generate** button.

*Figure 4-34 Attaching Policies*




**Note** You can try out policies on host systems by selecting Test Mode for a group or for a particular rule module. Selecting Test Mode and enabling logging on rules attached to “test mode” groups causes the agent to log designated denied events triggered by policies but not take any actions on those events.

# Using Test Mode

Test Mode is useful when you are installing a new host or are modifying a host configuration and want to understand the ramifications without actually impacting host operation. When operating in test mode, the agent will not deny any action or operation even if an associated policy says it should be denied.

Instead, the agent will allow the action but log an event if a deny or query rule is triggered (if logging is enabled for the rule) and log an event when an allow rule with logging enabled is triggered. This 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.

When using Group test mode, you'll likely also want to enable Verbose Logging mode. This way, the agent will not suppress any log messages as it normally does when several of the same log messages are received.

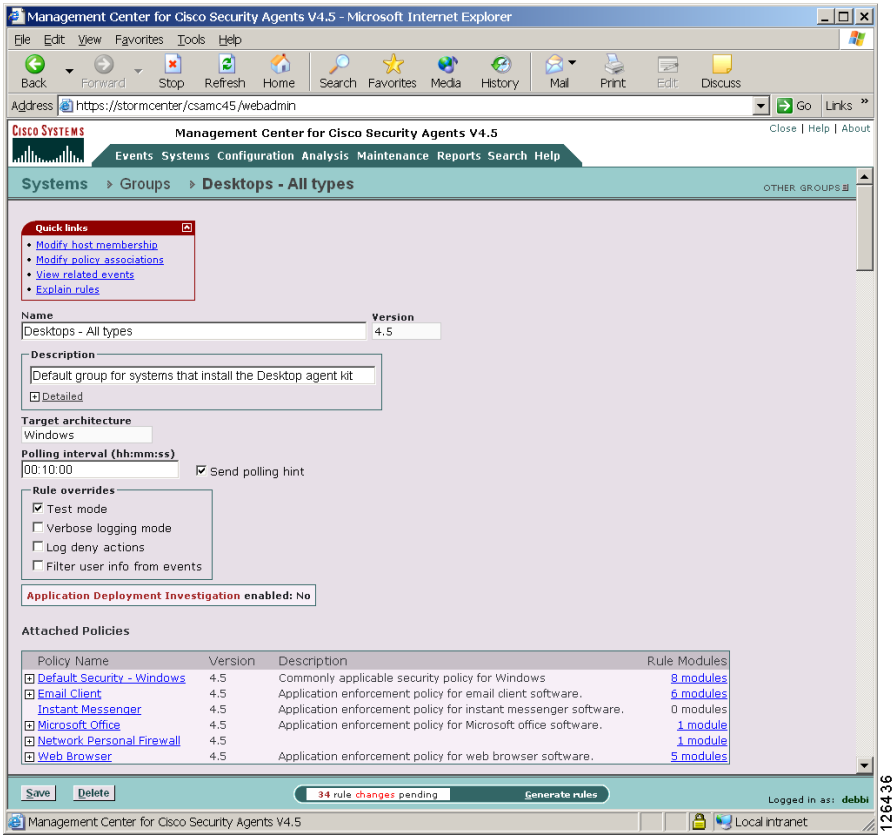
When an agent running in test mode sends events to CSA MC, event log messages are preceded with the words "Test mode". There are some exceptions to this. For example, event log messages related to detected events such as port scans and malformed packets are not preceded by the words "Test mode." Event detection (not prevention) messages appear the same in the event log regardless if test mode is on or off.

## Group Test Mode

You can turn on test mode in two places within the MC. If it is enabled on the group level (see Figure 4-35), all rules on hosts within test mode groups are in test mode.

If a host belongs to a group with test mode selected, all policies associated with that host are in test mode (even if the host is part of another group that does not have test mode selected), not just the policies applied to the test group. Therefore, test mode applies to the host as a whole, not to specific policies.

*Figure 4-35 Group Test Mode*

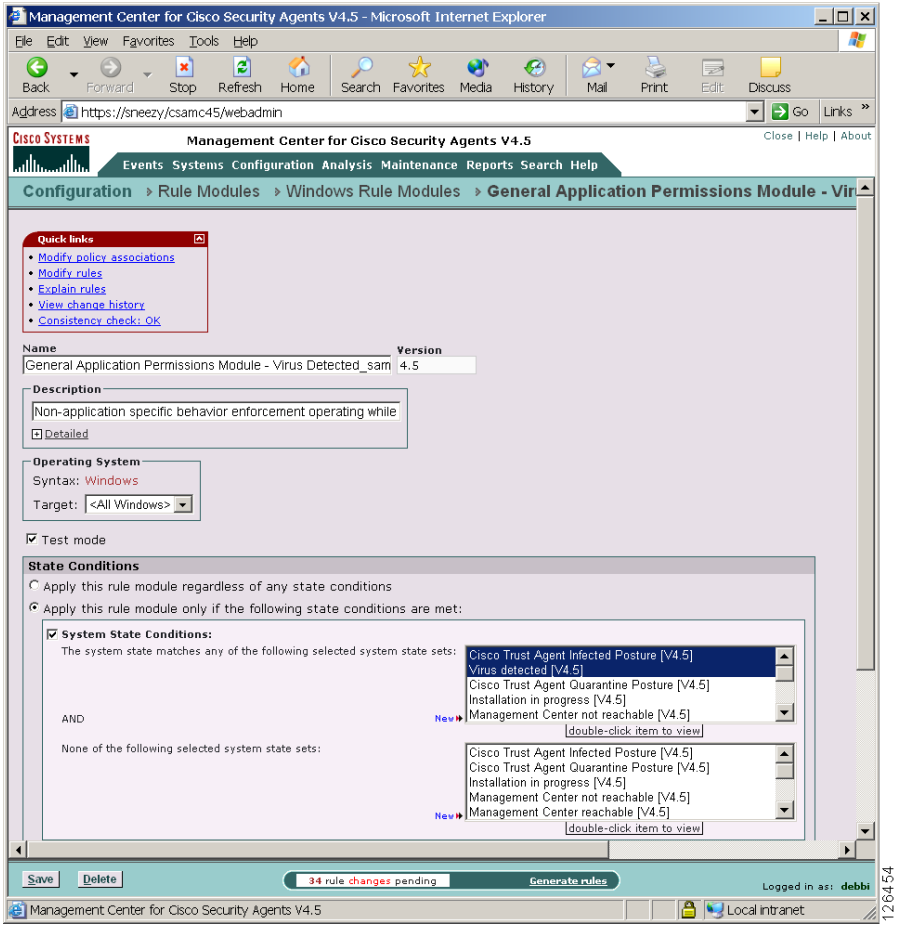



## Rule Module Test Mode

You can also use test mode on the rule module level (see Figure 4-36). This way, you can have the rules within the test mode module operating in test mode while rules from other modules assigned to the same host are operating in a live mode. This is useful for testing new rule modules or changes to existing modules without having to turn off all protections for the hosts in question.

**Caution** You should be aware that putting a deployed "live" policy into test mode turns off all security that the policy in question had been providing. Keep this in mind when using test mode to analyze how policies are working.

***Figure 4-36 Rule Module Test Mode***



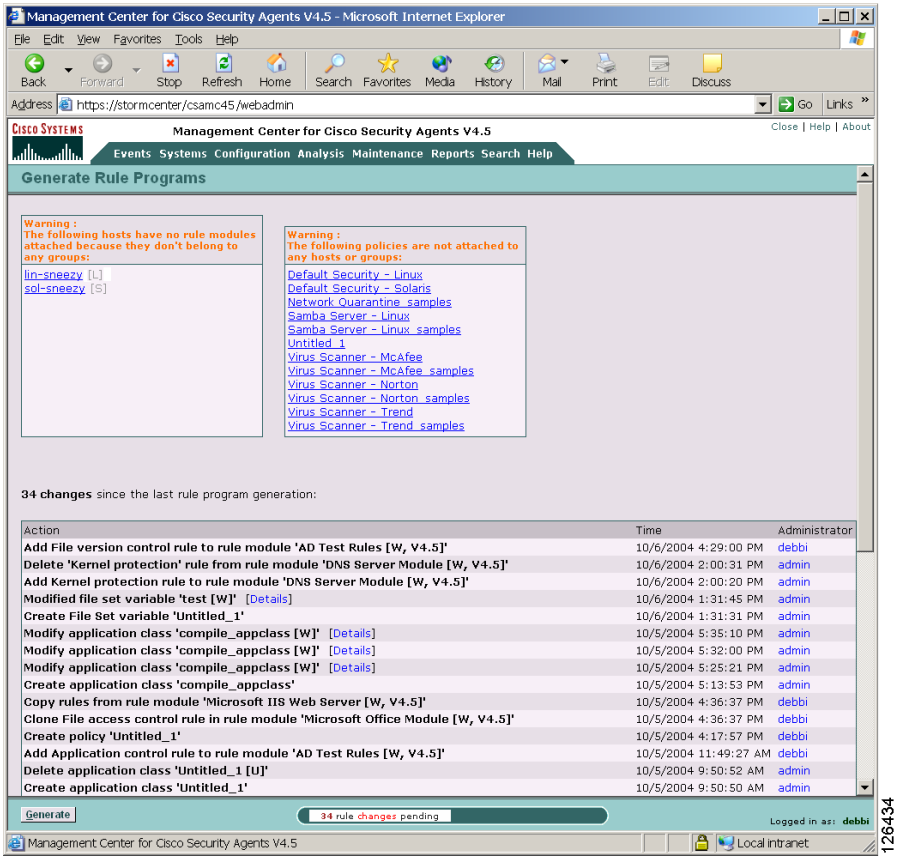
# Generating Rule Programs

**Caution** When you make changes to existing CSA MC configurations, they are saved in the database, but they are not yet distributed to the agents across your network. You *must* click the **Generate rules** link in the bottom frame of CSA MC to first view all new and edited configurations and then distribute them to the agents. (When you have pending changes, the line beneath Generate rules link flashes.)

The Generate rule programs view displays the status of all non-distributed database items with the name of the administrator who made the configuration changes. A **Details** link appears beside each edited configuration item. Click this link to view what modifications were made to the configuration in question.

**Note** Before you generate rule programs and distribute them to agents, you can view all database changes, including the time the changes were made and the administrator who mad them, by accessing the Audit Trail view from the Reports drop-down list. (See the"Using Audit Trail" section on page 2-11 for information on the audit trail.)

*Figure 4-37 Generate Configuration*




# Using System Correlation Rules

## Overview

Management Center for Cisco Security Agents provides rule modules and individual rules you can add to your policies that allow CSA MC to categorize processes and correlate events across multiple systems. When these rules are triggered by one or more system actions across a network, the MC registers this occurrence and automatically builds application classes and sends out new process categories to Cisco Security Agents. In some cases, the MC can prevent actions from executing on any additional systems. The Cisco Security Agent also uses heuristics to detect and terminate suspicious activities on systems, such as buffer overflows and password stealing attempts. These rule types differ from other action control rules in that multiple internal system events must trigger before these rules fire.

Use the rules and rule modules described in this chapter to protect systems just as you would other rules. For details on adding rules modules to policies and attaching policies to groups, refer back to Chapter 4, "Building Policies".

This section contains the following topics.

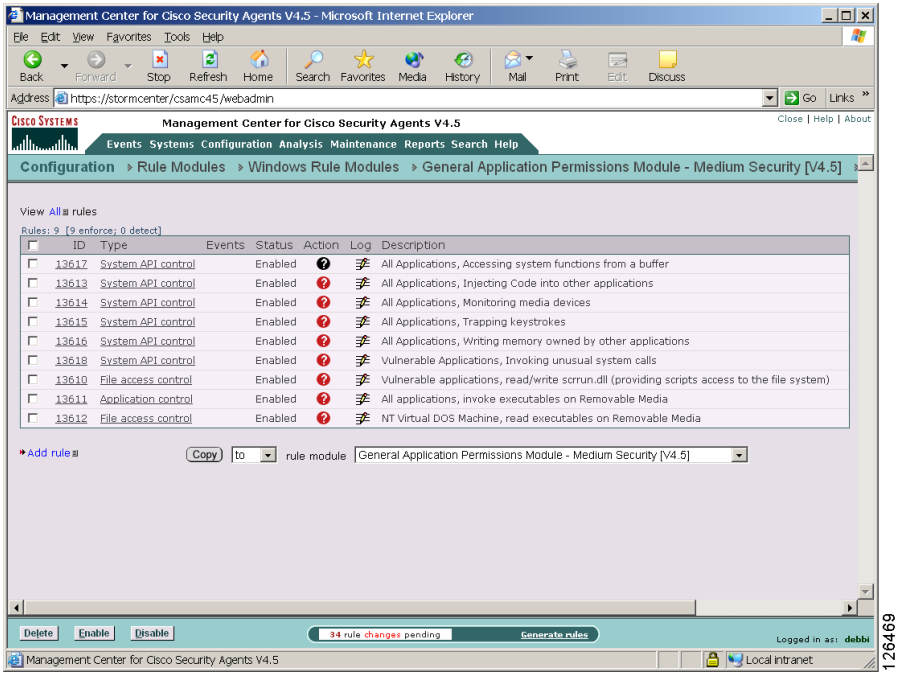

- Event Correlation and Heuristics, page 5-2
- System API Control Rule, page 5-3
- Network Shield Rule, page 5-7
- Buffer Overflow Rule, page 5-14
- Email Worm Protection Rule Module, page 5-18
- Installation Applications Policy, page 5-19

- Global Events, page 5-20
- Correlation, page 5-21


# Event Correlation and Heuristics

The Network shield rule which controls SYN flood protection and port scan detection and the System API control rule are some examples of preconfigured rules you can add to your modules in the same way you add other rules. These are basic system hardening, event correlation, and heuristic features that should be applied in most cases. Some are used in the General Applications Permissions module shown in Figure 5-1.

***Figure 5-1 General Applications Permissions Module***



# System API Control Rule

The System API control rule detects several forms of malicious programming code that is installed on a system by an unsuspecting user either thinking that he or she is running some other type of program, or as a result of some other activity such as reading an attachment to an email message. Once installed, these malicious programs (for example, Trojans) may allow others to access and virtually take over a system across the network. Other errant programs may be set up to automatically send mail messages or other types of network traffic (including system passwords) while the system owner is unaware of what is occurring.

**Note** This rule type is not available for UNIX policies. Refer to the Buffer overflow rule information on page 5-14 for similar UNIX functionality.

It could be useful, especially in the case of server systems, to use a service restart rule in conjunction with a System API control rule. This way, if you are forced to press the Terminate button if queried by a triggered rule and you subsequently terminate the application in question, a service restart rule will cause the application to automatically restart.

Use the System API control rule in a policy to detect and prevent errant programs from performing malicious acts on individual systems and networks. The included System API control rule lets you enable several different types of system detection. See Figure 5-2.

## System Information Checks

- Access local configuration information

  Detect applications that attempt to read system registry settings.
- Access local password information

  Detect applications that attempt to steal local system passwords.

## System Monitoring Checks

- Trap keystrokes

  Detect applications that attempt to capture system keystrokes.

- Monitor media devices

  This checkbox lets you control which applications can monitor media devices on the system. Media device “inputs” can be exploited by Trojans which can, for example, turn on the microphone on a system and covertly listen to a conversation.

  Patterns to be included: Use the Wizard from the Event log message in question to include particular devices in a System API “allow” rule. You must specify media devices as “device\port”. For example, `plantronics\microphone`.

**Note** Monitor media devices is not supported on Windows NT systems. It is also not supported for parallel port media devices on any operating system.

## System Modification Checks

- Access physical memory

  Detect applications that attempt to directly access physical memory while bypassing virtual memory restrictions.

- Download and invoke ActiveX controls

  Detect applications that download ActiveX controls and immediately attempt to execute them.
  This functionality limits applications from downloading ActiveX controls (signed and unsigned). This type of behavior is generally typical of a web browser and sites that require the downloading of ActiveX can trigger this rule. Note that this rule may be unnecessary if system web browser settings are configured with a "High" security level that would restrict the downloading of ActiveX controls.

- Inject code into other applications

  Detect applications that are attempting to write code to space owned by other applications. e.g. injecting a malicious .dll into a privileged process.

- Write memory owned by other applications

  Detect applications that attempt to interfere with the memory space of other applications or detect Trojans attempting to hide in another executable to escape detection and gain permissions to access other resources.

## Atypical System Behavior Checks

- Access system functions from code executing in data or stack space

  Although this behavior is sometimes exhibited by downloaded/executable content (e.g. license checking software), this may be symptomatic of a buffer overflow attack.

  - Patterns to be included: Use the Wizard from the Event log message in question to include a particular pattern in a System API “allow” rule when you are seeing buffer overflow events you believe are harmless.

- Handle exceptions

  Detect processes running exception handling routines. This typically occurs due to bugs in the application software. But this may be a sign of an attack if this occurs with an application that does not generally exhibit this behavior.

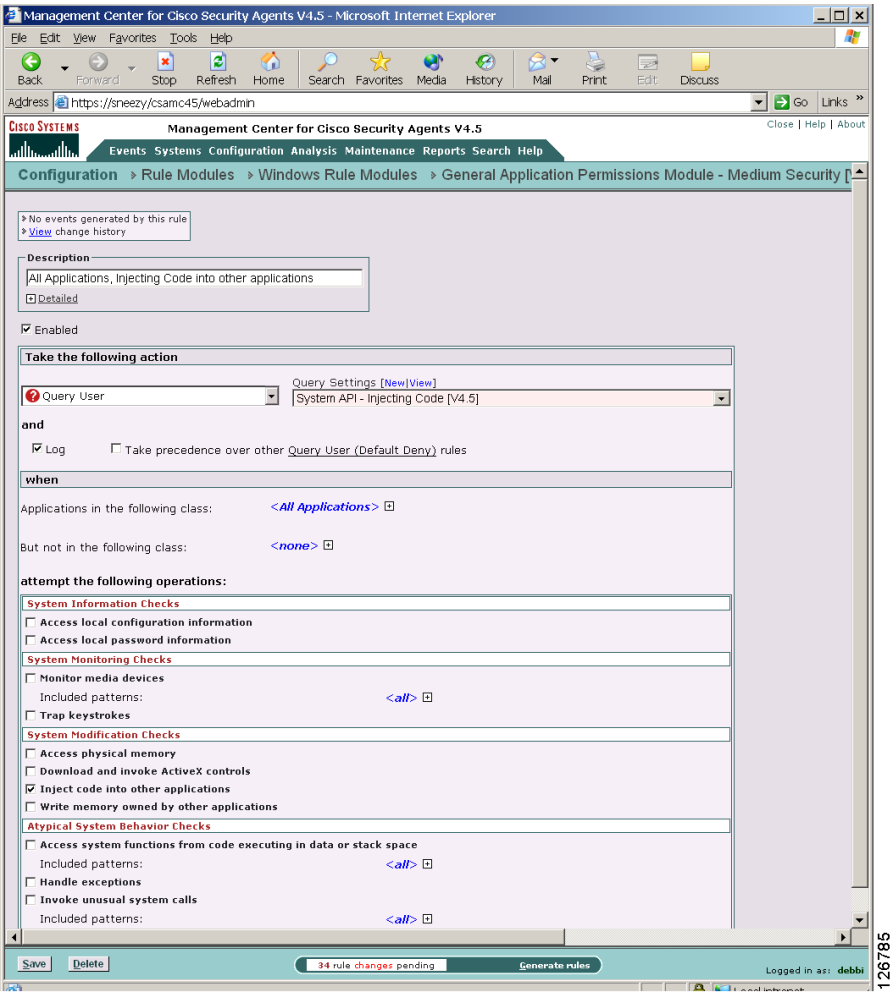
- Invoke unusual system calls

  Use this checkbox to detect processes invoking system calls that are rarely used. In normal system operation, many system calls are either never used or may only be used infrequently by a specific system application performing a service. Attempting to exploit undetected flaws in these unusual system calls is common attack vector for malware.

  - Patterns to be included: Use the Wizard from the Event log message in question to include a particular module in a System API “allow” rule when you are seeing events you believe are harmless.

You also have the ability to select specific **application classes to exclude** from the various System API control rules you designate. For example, in some cases, debuggers may perform actions that can be misconstrued as malicious behavior. Therefore, you would want to create an application class, and select it as an exclusion to one or more System API control rule features.

*Figure 5-2 System API Control Rule*



## Replicate Feature

When you make rule changes and click the Save button for rule types that contain multiple checkboxes, such as System API control rule (Network shield and Buffer overflow rules also provide this feature) a "replicate" link appears beside the "Saved changes" message at the top of the rule page. Click on **replicate** to access a pop-up box. From this box, you select other policies that contain System API control rules and choose to propagate the same change(s) you made on the current page to System API control rule pages in other policies. If the change you make to one System API control rule page is a change you need to make to all System API control rules in all your policies, this is a quick way to propagate those changes on a wide or even global scale.

# Network Shield Rule

The Network shield rule provides network protocol stack hardening capabilities. The features available here require that the network shim be enabled on an agent system. If the network shim is not enabled, these rules have no effect when applied. See Network Shim Optional, page A-7.

**Note** The information provided in this manual, in this section especially, assumes a basic knowledge of TCP/IP. A good source for further reading on the topic is the book *Internetworking with TCP/IP*, Douglas R. Comer and David L. Stevens, Prentice Hall, Inc.

**Step 1** In the Network shield rule configuration view, enter the following information:

- **Description**—Enter a description of this rule. This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.) By not selecting this checkbox, you can save this rule, but it will not be active in the module and it will not be distributed to groups.

**Step 2** **Take the following action**—(Note that only High Priority Deny, Allow, Deny, Monitor, and Add process action types are available for this rule. You can choose to add the system process to the Processes communicating with Untrusted Hosts application class which causes the remote host IP address to be sent to the MC for

global correlation. This may result in the address being added to the @dynamic address list for quarantining. See page 6-7 for information on the Processes communicating with Untrusted Hosts application class. Also see Correlation, page 5-21 for details on quarantining IP addresses.) Select an action type from the pulldown list. For further details on rule action types, see Rules: Action Options and Precedence, page 4-9.

**Note** Because IP addresses can be spoofed, we don't recommend using this capability for this rule type. It is more applicable for NACL-based rules where you are sure you are communicating with the address. (i.e. an established TCP connection.)

**Step 3** and

- **Log**—Enable this checkbox to turn logging on for this rule. Generally, you will want to turn logging on for all deny rules. This means that the denied system action in question is logged and sent to the server at regular time intervals.
- **Take precedence over other <action type> rules**—Enable this checkbox to manipulate rule precedence so that this rule is evaluated before other similar rules. You should generally NOT require this checkbox. Do not use it without understanding how it works. See Rules: Manipulating Precedence, page 4-13 for details.

**Step 4** when detecting (Select one or more of the checkboxes described here. Please note any address and/or state condition restrictions that are called out beside each check.)

**Caution** You cannot use network shield rules in rule modules that have user state conditions set. If you attempt to attach a user state to a rule module that contains a network shield rule, you will be notified of a configuration error.

## IP Security checks

- Invalid IP header

  Enabling this feature causes the Cisco Security Agent to perform an integrity check on the IP packet header. This includes performing a consistency check on the IP header, on the length of the IP header, and on the number of bytes in the packet. If you configure this as a Deny rule, the following occurs: if

any of these checks fail, the packet is dropped, if an IP checksum fails, the packet is dropped, IP options and IP fragments are validated as well and dropped if they are found to be invalid. (This defeats attacks such as Teardrop, Boink, and Ping of Death.)

- Invalid IP address

  IP addresses are determined to be invalid for several reasons: if the source address is a multicast address, if the TCP connection is to a broadcast address. You can select this checkbox as part of a Deny rule to protect against these types of attacks.

- Source routed packet

  This detects IP options which control explicit routing instructions for packets. With IP source routing (an IP header option) the originator of a packet can try to partially or completely control the path through the network to the destination.

- Trace route

  This detects the mapping of network topology via trace route.

### Transport Security checks

- Invalid TCP/UDP/ICMP header

  This check ensures that transport headers are the proper length and that they are consistent (have enough data in the packet for them to fit). This includes verifying that certain fields have valid values and that certain combinations of TCP flags are legal. This defeats attacks such as a Christmas Tree scan.

- TCP SYN floods

  SYN flooding is a type of denial of service attack. It occurs when a TCP/IP connection request is received from a return address that is not in use (i.e. a non-existent host for a spoofed address) resulting in a half open connection. An abundance of half open states on a server can prevent legitimate connections from being established. Detecting and preventing SYN floods stops this attack from succeeding.

  (This rule type is not available for UNIX policies as the UNIX OS already provides this protection.)

  Servers that are external to your network and not protected by a firewall should be protected against SYN floods. Firewalls generally provide this protection.

**Note** If you enable the "TCP SYN floods" and the "TCP blind session spoofing attempts" checkboxes, you cannot enter address restrictions into the address field for this rule. You must use all addresses.

- TCP blind session spoofing attempts

  If you configure this as a Deny rule, this check causes agents to make TCP sequence numbers unpredictable.

  A server accepting connections using predictable TCP sequence numbers may be tricked into accepting a connection from a malicious source that is spoofing a trusted host. This prevents that vulnerability.

  (This rule type is not available for UNIX policies as the UNIX OS already provides this protection.)

**Note** If you make any changes to the "TCP blind session spoofing attempts" feature, these changes are not enforced until after the agent system(s) is rebooted.

- TCP/UDP port scan

  Port scanning is a common method for finding weaknesses at a site by determining what network services are being run. An attacker attempts to connect to port after port on a target system, mapping ports to identify network services and machine type vulnerabilities. Configure this rule to log an event when an attempt is made to scan the system for an open port. Information is also gathered on the number of different source IP addresses perpetrating the scan and it reveals the source. In most cases, you should apply port scan detection to servers and end-user systems in your enterprise.

  Configure this rule as a Deny rule to prevent unauthorized port scans, effectively cloaking a system on the network. Denying port scans causes a system to not respond to connectivity tests and to not respond to service requests with connectivity error messages.

  A system generally sends out error messages when a remote machine sends a request for a service which is not running on the system. Often, this is how remote machines locate other systems and obtain network information about

the system in an attempt to target it for an attack. By not responding, this prevents both UDP and TCP-based port scans of the system and basically hides it on the network.

If you are running an allowed service on a system and you are denying port scans, connection requests to this service are honored and your machine is viewable for the service you're offering.

**Note** If you select the network scans correlation checkbox in the Global Event Correlation page (see Correlation, page 5-21), when scans are detected and denied across several machines, CSA MC correlates these events and generates an additional event to warn of this correlation. Note that this correlation only occurs when Deny rules are triggered.

- ICMP ping message

  This check works similar to the TCP/UDP port scan feature, but for ping scans. See the port scan description for information.

- ICMP configuration message

  If you configure this rule as a Deny, this feature restricts messages which can change the configuration of a machine. For example, a redirect can be used to cause routing tables to be updated.

- ICMP information message

  Some ICMP messages may be used to gather information about a machine in an attempt to attack it. This data, when obtained, can be used to gather system information which can be used to exploit the system. If you configure this rule as a Deny, this feature restricts messages which report back on system or network configuration.

- ICMP covert channel

  Configuring this rule as a Deny, causes agents to drop unsolicited echo responses.

  The Cisco Security Agent validates that the echo response data matches the echo request data. This way, ping cannot be used as a transport for communications.

- Malicious packet

Configuring this rule as a Deny causes agents to block packets which are technically legal but are known exploits against protocol stacks (e.g. UDP packet storm or RF poison).

### System Startup Security checks

- Unrestricted network connectivity during boot

  Configuring this feature as a Deny, prevents non-essential network connections during system startup. This check is automatically disabled when the agent service starts and policies (including those which govern allowed network connections) are enforced. This protects the system from network-based attacks at boot-time before the agent service has started.

  (This rule type is not available for UNIX policies.)

**Note** If you enable the Unrestricted network connectivity during boot checkbox, you cannot enter address restrictions into the address field for this rule. You must use all addresses.

**Note** You cannot use a rule that has the Unrestricted network connectivity during boot checkbox selected in policies with rule modules that have system and/or user state conditions set.

**Step 5** and Communicating with host addresses

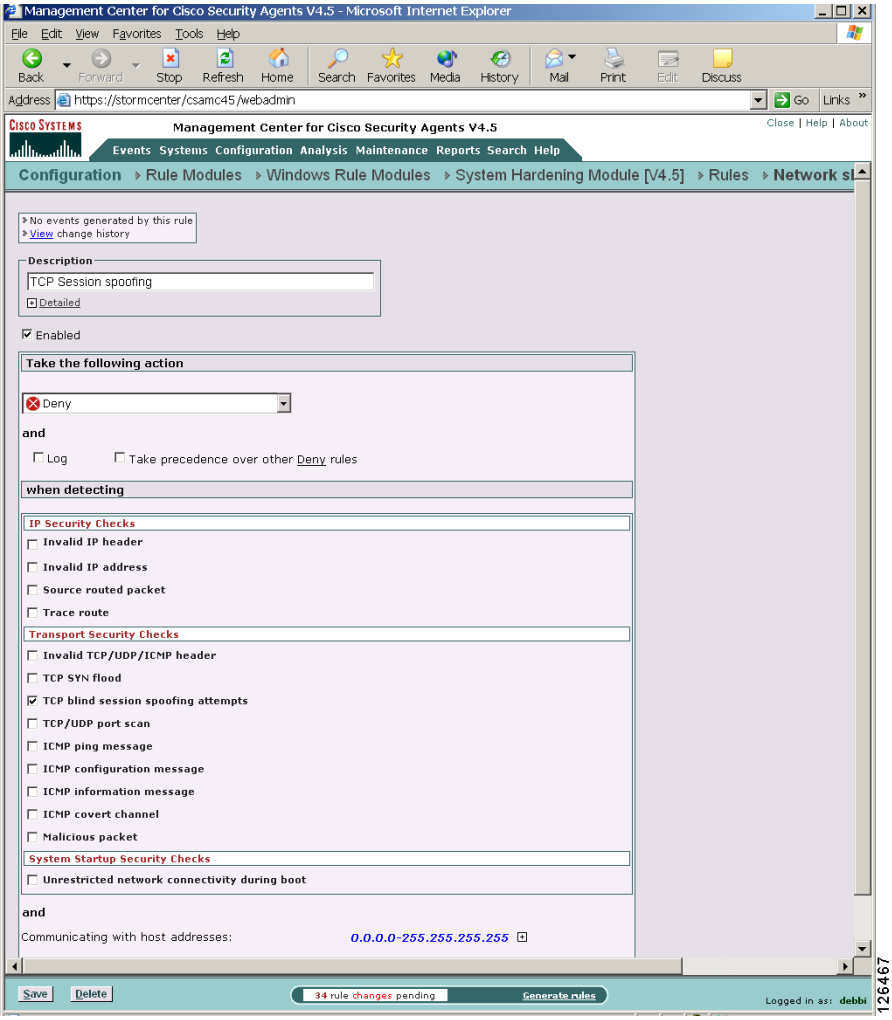
Optionally, you can enter specific addresses here for those checkbox features in this rule that support addressing parameters.

**Step 6** Using these local addresses

By default, this field indicates all local addresses on the agent system. You would want to use this to identify specific network interfaces, if necessary.

**Step 7** Click **Save** when finished.

*Figure 5-3 Network Shield Rule*




**Note** Refer to Replicate Feature, page 5-7 for details on easily propagating the changes you make to one Network shield rule to other Network shield rules in other policies.

# Buffer Overflow Rule

A buffer overflow is what happens when two conditions are met: Firstly, an application is coded in a manner such that it trusts that all users of that application will provide the application with reasonable and expected data. Secondly, the application is provided larger quantities of data than it is capable of correctly handling. When these events come together, an application can behave in unexpected and unintentional ways.

For applications with special privileges, this can result in external users gaining access to machine resources and privileges which they normally would not be able to acquire. In other words, a hostile, network-based attack on a privileged, trusted application via buffer overflows can result in undesirable parties gaining access to your system.

In the case of UNIX operating systems, there are three distinct types of buffer overruns which can occur, based upon the type of memory space involved: stack, data, and heap.

- Stack space is used to store data and information which is local to the piece of code currently being executed in an application, and contains stored away control flow information for the application.
- Data space is used to store data with fixed sizes which needs to be shared among different parts of an application. Often, content in data space has been given initial values.
- Heap space is dynamically given out to applications, with the intent that it is relatively short-lived, of varying size based upon the input datasets, and is frequently visible to numerous sub-components of an application.

**Note** This rule is UNIX specific. Some corresponding Windows functionality is available from the System API control rule page.

Configure the Buffer overflow rule as follows.

**Step 1** To add rules to your policy, click the **Add rule** link at the bottom of the rule list. A pop-up list of the available rule types appears.

**Step 2** Select the **Buffer overflow** rule. This takes you to the configuration view for this rule type (Figure 5-4).

**Step 3** In the Buffer overflow rule configuration view, enter the following information:

- **Description**—Enter a description of this rule. This description appears in the list view for the module. Optionally, expand the **+Detailed** field to enter a longer description.
- **Enabled**—Use this checkbox to enable this rule within the module. (It is enabled by default.) By not selecting this checkbox, you can save this rule, but it will not be active in the module and it will not be distributed to groups.

**Step 4** **Take the following action**—Select an action type from the pulldown list. For further details on rule action types, see Rules: Action Options and Precedence, page 4-9. (Note that High Priority Deny and Deny actions are not available for this rule.)

**Step 5** and

- **Log**—Enable this checkbox to turn logging on for this rule. Generally, you will want to turn logging on for all deny rules. This means that the denied system action in question is logged and sent to the server at regular time intervals.
- **Take precedence over other <action type> rules**—Enable this checkbox to manipulate rule precedence so that this rule is evaluated before other similar rules. You should generally NOT require this checkbox. Do not use it without understanding how it works. See Rules: Manipulating Precedence, page 4-13 for details.

**Step 6** **when**

**Applications in any of the following selected classes**

Select *one or more* preconfigured application classes here.
Note that the entry, <All Applications>, is selected by default. You can use this default or you can unselect it and create your own application classes. For application class configuration details, *see* Chapter 6, "Using Application Classes".

**But not in the following class**—Optionally, select application classes here to exclude from the application class(es) you've selected in the included applications field. Note that the entry <None> is selected by default.

**Step 7** Select one or more of the following checkboxes to prevent the associated buffer overflow attack from occurring.

- Attempted buffer overflow detected

Enable this checkbox to detect buffer overflow conditions which occur in UNIX executables. This feature provides protection from stack buffer overflows to a number of commonly used libc routines. As a large number of attacks on UNIX systems are based upon buffer overflow attacks, it is recommended that you enable this feature. Processes terminated by operating system due to executing code in stack space.

- Executing a system call in an unsafe context

  Use this checkbox to prevent certain system calls (e.g. those which grant extra privileges or start new processes) from occurring if they are invoked in an unsafe manner, or if they appear to have come from a corrupted or invalid context.

- Processes terminated by operating system due to executing code in stack space

  This checkbox enables the "noexec_user_stack" system variable for all processes or for processes added to the <*Processes requiring OS Stack Execution Protection>. See Built-in Configurable Application Classes, page 6-7 for details. This checkbox monitors the execution of instructions from stack memory. This only provides logging.

- Process terminated due to signal or internal error

  Processes can be killed on a system by either another process or by an internal error occurring on the system. This checkbox causes the agent to monitor when this occurs. The only action type available when this checkbox is enabled is Monitor.

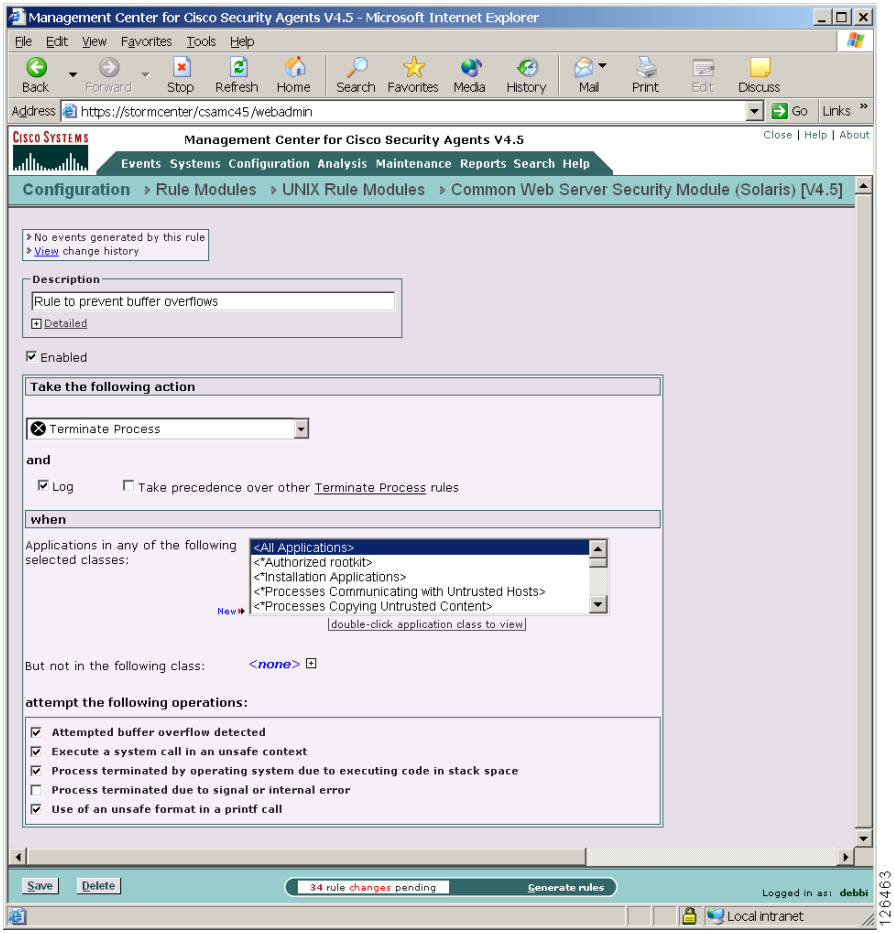
- Use of an unsafe format in a printf call

  Use this checkbox to prevent the usage of the '%n' *printf() format qualifier. Numerous attacks utilize the '%n' format on *printf() routines to gain access to program control flow information.

You also have the ability to select specific **application classes to exclude** from the various Buffer overflow types you designate. If you select an application in the available list beside a checkbox rule, that rule does not apply to the selected application class. If you have multiple, similar Buffer overflow rules, the application class exceptions are combined.

**Note** Refer to Replicate Feature, page 5-7 for details on easily propagating the changes you make to one Buffer overflow rule to other Buffer overflow rules in other policies.

***Figure 5-4 Buffer Overflow Rule***



# Email Worm Protection Rule Module

Email worms are some of the most commonly spread and costly attacks affecting corporate networks today. Some well-known worms of the past include Mydoom, Anna Kournikova, and variations thereof. These worms easily infected systems, passing undetected through most security software until virus scanner vendors provided updates to detect these virus signatures. Even with this detection capability, if the worm is modified in any way, it is again undetectable by virus scanners.

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. This makes file recovery difficult and it can cause users to invoke the virus again when they attempt to open these infected files.

The Cisco Security Agent ships with a preconfigured email worm protection rule module. You must have this module deployed to take advantage of email worm network event correlation and quarantine capabilities.

The email worm protection module works through a combination of steps including dynamically building an application class through the detection of a suspicious action occurring on a system. If this suspicious action detection is seen by the MC as occurring on more than one system, a quarantine of the detected malicious process will also occur.

More specifically, it is through two sets of rule types that the detection and tagging of a virus or email worm occurs. In fact, these rules can be used more widely to identify and stop any type of virus, not only email. Although, this does require some different parameters to be set in the first group of rules.

The email worm protection rule module works this way:

- The first set of rules are written to deny or terminate processes or to query the user when a set of actions are attempted. Those actions are something along the lines of “a process that downloaded content over the network is now attempting to access an email COM component, such as the address book.” This action is suspicious. It is either denied or terminated or the user is queried about it.
- If the action is denied or terminated (automatically or by the user), the second set of rules tags the offending process and adds the process to the dynamically built “Suspected Virus Applications” class. Once a process is in this class,

other rules prevent all processes that are dynamically added to this class from accessing any resources on a system. If these processes are seen on more than one system, it also quarantines the processes in question. See Global Events, page 5-20 for quarantine details.

The methodology used in the email protection module can be applied to any virus type you're protecting against. By altering the parameters of the first rule set (in this example, downloaded contented accessing the COM component for the email application address book) you can configure parameters to categorize any process as suspicious and subsequently stop any type of errant action.

## Email Worm Event Correlation

If you select one of the options to add dynamically quarantined files to the list in the Global Event Correlation page (see Correlation, page 5-21), when a worm is detected, other agents will be notified to prevent the spread of this virus. Under these circumstances, the agent(s) report the file name the worm was written into. If at least two agents report worms writing to the same file name within an hour, the file is added to a dynamic list (@dynamic) of quarantined files. If you have a rule configured to stop dynamically quarantined files in a deployed policy, no further agents can open the contaminated file during the quarantine time frame. See also, page 4-64 for information on using @dynamic in File access control rules.

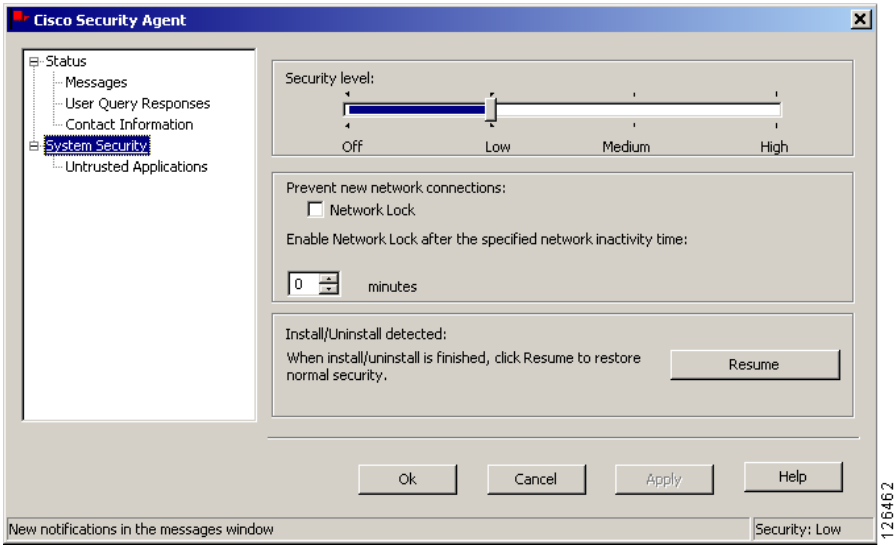
# Installation Applications Policy

There is a preconfigured policy that you can apply to systems to detect when a software installation occurs and to add the install process or processes to a dynamically built application class. If dynamic tagging occurs, another set of rules would apply to the install processes added to this dynamic class. You may need to use this installation detection rule module in order to enforce a less strict set of rules to the system while an approved software installation is occurring. Under normal conditions, other rules on the system may prevent the install from occurring.

The built-in dynamic application class in question is called "Installation Applications." The rule module may build this application class under the following circumstances: A set of rules determines that setup.exe is detected on a system and it is added to the dynamic built-in Installation Applications class. As a result, a System State installation condition is triggered (see System State Sets,

page 4-25) and a new policy is applied to the system. The system should automatically return to its original policy when the install exits. If this does not occur, the user can manually indicate when the installation is complete (a Resume button, see Figure 5-5, is made available if the end user has an agent UI) and return the system to the initial stricter policy. The installation state may also time out and the system then automatically returns to its initial policy.

***Figure 5-5 Agent UI Resume Button***




# Global Events

The Management Center for Cisco Security Agents lets you enable correlation functions for particular types of events. In each case, you must have a corresponding rule enabled in a policy for the global event correlation to take place. If you do not enable global event correlation, individual events are logged by system agents but similar events across multiple agents are not correlated by the central CSA MC.

# Correlation

The **Event Correlation** page, accessible from the menu bar as follows **Configuration>Global Event Correlation** (see Figure 5-6), provides the following capabilities:

- Correlate network scans

  With this checkbox enabled, correlated port scans and ping scans across multiple agent systems are logged separately as a correlated event in addition to the individual port scan and ping scan events that continue to be logged.

  Note that you must have a Network shield rule with Port scan detection and Ping scan enabled in a policy deployed to the agent(s) in question for these event types to be detected and logged.

  The threshold and time frame for correlating network scans are values you can configure.

- Correlate events received from operating system event logs and generate a summary event
  - Log individual events in addition to summary event

  With this checkbox enabled, events from multiple systems are correlated based on the NT event code, NT event severity, NT event source, and NT event log type. If 2 systems log the same NT event type within 30 minutes, a correlated summary event is logged.

  Note that you must have an NT event log rule in a policy deployed to the agent(s) in question for these events to be uploaded to the CSA MC log.

  If you do not enable this checkbox, NT event correlation does not take place, but individual NT events are logged in accordance with the NT event log rule you have configured.

**Note** In this case, there is an additional checkbox (Log individual events in addition to summary events) to control whether the individual events are logged in addition to the summary event. If you do not enable this checkbox, but you do enable the Correlate events checkbox, only correlated summary events will log, NOT individual events. This can be useful if NT event log messages are filling up your CSA MC logfile.

- Correlate suspected virus application events and add contaminated files to list of dynamically quarantined files

  With this checkbox enabled, when processes are added to the dynamic <Suspected Virus Applications> application class (see Built-in Configurable Application Classes, page 6-7) and this event is logged across multiple agent systems, these events are correlated and the contaminated file that triggered the event is added to a dynamic list of quarantined files that CSA MC maintains. If you have a rule configured to stop dynamically quarantined files in a deployed policy, no further agents can access the contaminated file. See page 4-64 for information on using @dynamic in File access control rules.

  If you do not enable this checkbox, suspected virus correlation does not take place, but individual virus events are logged.

  Note that you must have a a corresponding policy deployed to the agent(s) in question for these event types to be detected and logged.

- Correlate events received from virus scanners and add contaminated files to list of dynamically quarantined files

  With this checkbox enabled, events logged by virus scanners running on agent systems are received and correlated by CSA MC. Contaminated files detected by virus scanners are added to the list of quarantined files. If you have a rule configured to stop access to dynamically quarantined files in a deployed policy, no further agents can receive the contaminated file. See page 4-64 for information on using @dynamic in File access control rules.

**Note** This feature works with Norton, McAfee, and Trend AntiVirus. To receive these virus events, you must have an NT event log rule in a policy deployed to the agent(s) in question for these events to be uploaded to the CSA MC logfile. In the NT event log rule, you must enter the name of the antivirus software in the Event Source field. See NT Event Log, page 4-87 for details.

The threshold and time frame for correlating events received from virus scanners are values you can configure.

**Note** To view the files that are added to the dynamically quarantined files list, click the numbered link beside **dynamically quarantined files**. It takes you to the pertinent event log messages. Read the messages there to locate the names of quarantined files. You can also click the **Manage dynamically quarantined files** link at the bottom of the page.

- Correlate communications with untrusted hosts and add peer addresses to list of dynamically quarantined IP addresses.

  With this checkbox enabled, when processes are added to the dynamic <Processes communicating with Untrusted Hosts> application class (see Built-in Configurable Application Classes, page 6-7) and this event is logged across multiple agent systems, these events are correlated and the untrusted peer address that triggered the event is added to a dynamic list of quarantined IP addresses that CSA MC maintains. If you have a rule configured to stop dynamically quarantined IP addresses in a deployed policy, no further agents can communicate with this peer address. See page 4-69 for information on using @dynamic in Network access control rules.

  If you do not enable this checkbox, untrusted host correlation does not take place, but individual untrusted host events are logged.

**Note** You must have a a corresponding policy deployed to the agent(s) in question for these event types to be detected and logged.

**Note** To view the IP addresses that are added to the dynamically quarantined addresses list, click the numbered link beside **dynamically quarantined IP Addresses**. It takes you to the pertinent event log messages. Read the messages there to locate the quarantined IP addresses. You can also click the **Manage dynamically quarantined IP addresses** link at the bottom of the page.

## Manage Dynamically Quarantined Files and IP Addresses

You can use the **@dynamic** token in the File set text field and in the Network address set text field to control access to files and addresses that have been quarantined by CSA MC. Files are quarantined as a result of suspected virus

application events, correlated virus scanner log messages, or files that were added manually. This list updates automatically (dynamically) as logged quarantined files are received. Addresses are quarantined as a result of communication with a suspected untrusted host (this updates dynamically) or by being added manually.

To view the files that are added to the dynamically quarantined files list and to manually add files to be quarantined, click the **Manage dynamically quarantined files** link on the Global Event Correlation page. See Figure 5-7. Add and Remove files from this list using the provided buttons on the bottom of the window that appears.

To view the addresses that are added to the dynamically quarantined IP addresses list and to manually add addresses to be quarantined, click the **Manage dynamically quarantined IP addresses** link on the Global Event Correlation page. Add and Remove IP addresses from this list using the provided buttons on the bottom of the window that appears. See Figure 5-8. The “Source” column in this window describes how the address was added to the list (manually by the administrator or through a correlation event).

Changes made to the quarantined file and IP address lists are not received by agents until they next poll in to the management center. You can send a hint message to hosts to poll in sooner than the set interval. See Configuring Groups, page 3-3 for poll hint details.

*Figure 5-6 Global Event Correlation Page*

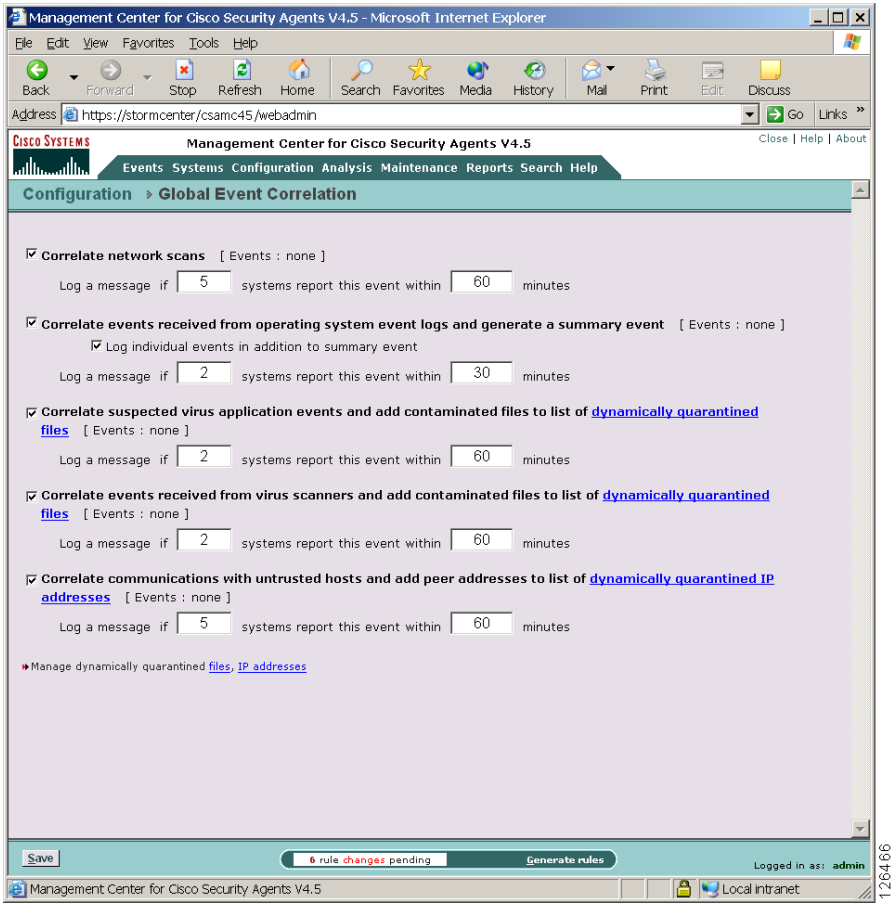


*Figure 5-7 Quarantine Files Window*

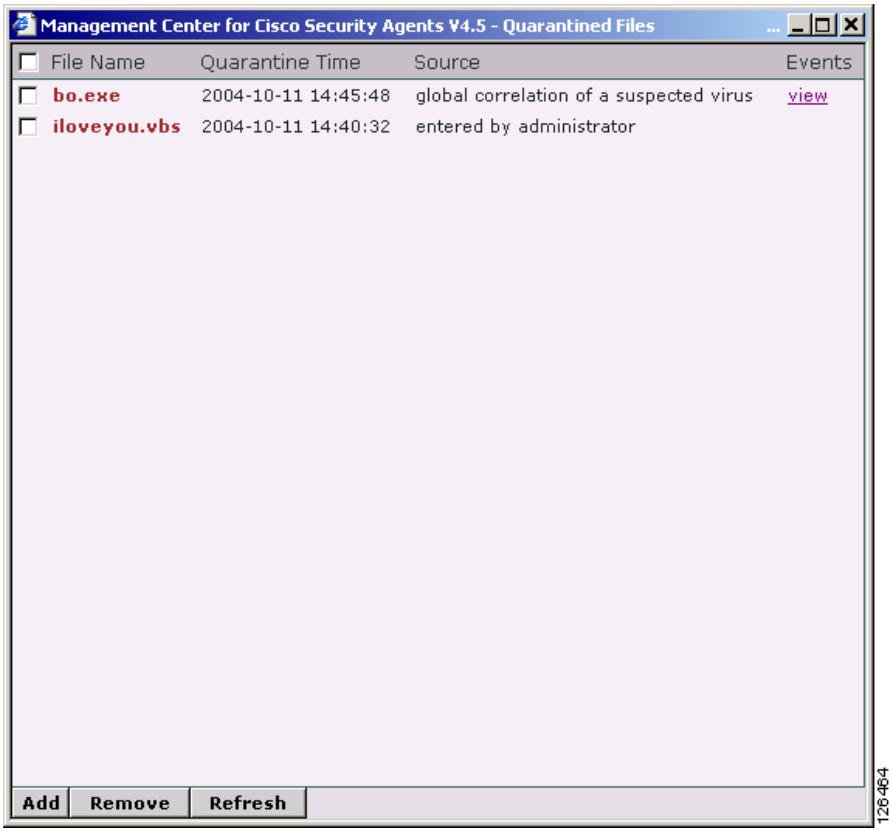
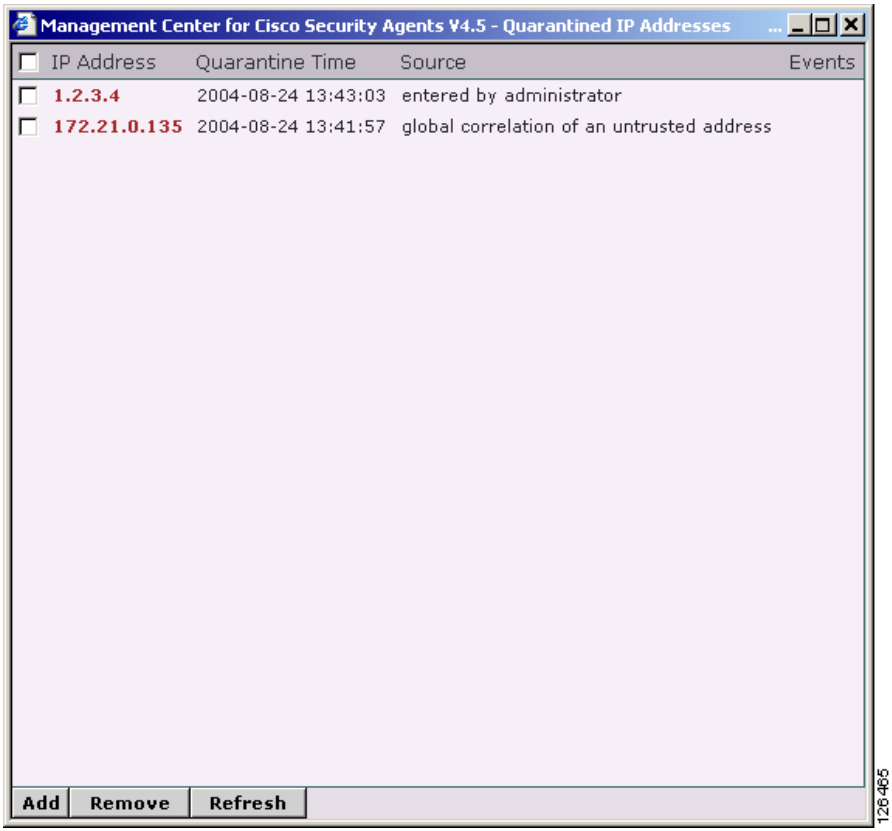


*Figure 5-8 Quarantine IP Addresses Window*




# Using Application Classes

## Overview

Access control rules are application-centric. The application classes, those shipped with CSA MC and the ones you configure yourself, are the key to the rules you build as part of your security policies.

This chapter explains the application classes shipped with CSA MC and provides instructions for creating new static and dynamically defined application classes.

This section contains the following topics.


- About Application Classes, page 6-2
- Processes Created by Application Classes, page 6-2
- Removing Processes from Application Classes, page 6-2
- Shell Scripts and Application Classes, page 6-3
- Built-in Application Classes, page 6-4
- Built-in Configurable Application Classes, page 6-7
- Configuring Static Application Classes, page 6-9
- Dynamic Application Classes, page 6-13
- Defining Dynamic Classes, page 6-14
- Configuring Dynamic Application Classes, page 6-15
- Configure an Application-Builder Rule, page 6-18
- Configure a Rule Using a Dynamic Application Class, page 6-22

- Create New Application Classes from Rule Pages, page 6-23
- Application Class Management, page 6-24

# About Application Classes

When you create rules, you must decide which applications are performing the operations you are allowing or denying as part of the rule. Once you know this, you configure the application as an "application class" in CSA MC and select it as part of your rule.

Application classes are groupings of application executable files that you combine under one name, generally as part of a File Set Variable, see File Sets, page 7-10. For example, you can enter netscape.exe and iexplore.exe under the heading of Web Browsers. Then you can select Web Browsers in the application field for your rule and apply restrictions to the actions that both Netscape and Internet Explorer can perform on specified resources.

## Processes Created by Application Classes

When applications are invoked, they often spawn other processes as part of the action they are performing. Therefore, when you create an application class, CSA MC gives you the option of including or excluding child processes created by the original applications you define as part of the application class (see page 6-8 for details).

## Removing Processes from Application Classes

Processes are part of a configured application class when they are running on the system. When the process stops running, the CSA MC application classification for that process also ends. Should the process begin again, it may or may not fall into the same application class depending on the process's behavior and on the definition of the application class. Therefore, all application classifications are ephemeral and are constantly being re-evaluated and classified on the system.

The application class configuration page lets you control how long a process maintains a certain application classification. In general, you do not have to specify a time frame. You should only put a time limit on an application

classification if you are configuring rules that require it for a particular reason. For example, you may want to create special process start rules for an application. The classification of the process could be configured to time out once the system is finished booting.

# Shell Scripts and Application Classes

On UNIX systems, the agent allows control over shell scripts which satisfy both of the following conditions:

- the script begins with an interpreter string (e.g., #!/bin/bash)
- the script is executed directly on a command line, e.g., "$foo.sh".

Therefore, if you have an application class "foo.sh", a process satisfying the above conditions becomes a member of that application class.

Note that a shell may be launched by various methods which do not meet those conditions, e.g., "`$ . foo.sh`", or "`$ cat foo.sh | /bin/sh`". Note also that if you happen to have an application class for a script's interpreter -- say, `/bin/bash` -- when you invoke the script, the process becomes a member of the `/bin/bash` application class.

If a user has write access to the disk, and can execute commands, then using the name of a shell script in a rule to DENY actions may not make sense. For example, denying access by foo.sh to modify `/etc/hosts` does not improve the protection of `/etc/hosts` as the user could just run '`vi /etc/hosts`'. It would make more sense to deny everything access to a file, and then permit known good scripts access to that file.

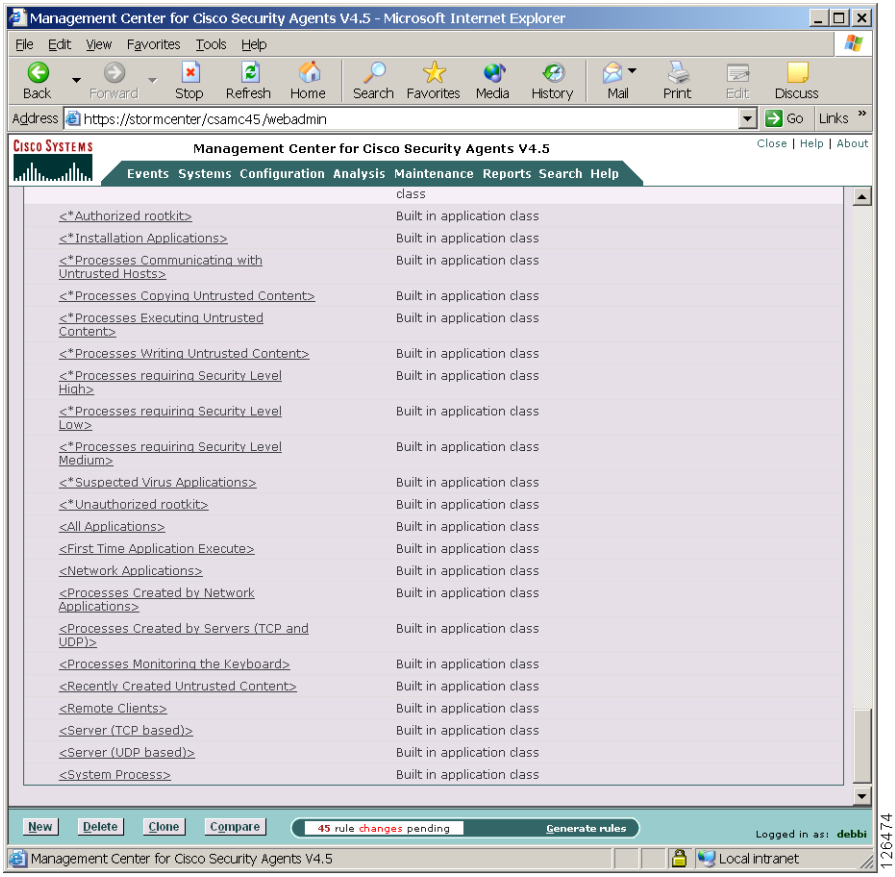
**Caution** If the user can copy a script (or re-implement it) to a file of their choice, then any Deny rules would be avoided.

**Note** On Windows, when writing rules for script application classes, you can create the rule for either the script itself or for the interpreter. (Scripts are handled by script interpreters.) If you write the rule for the interpreter, it will include the script handled by that interpreter.

# Built-in Application Classes

CSA MC ships with several built-in application classes. Those application classes appear inside brackets (see Figure 6-1) in the rule application class selection list boxes. Some built-in class are also marked with asterisks. When there is an asterisk present, that indicates that the built-in class is configurable. See Built-in Configurable Application Classes, page 6-7. You can view all application classes in the Application Class list page. Access this page from **Configuration**>**Applications** in the CSA MC menu bar.

*Figure 6-1 Built-in Application Classes*




Some included application classes are:

- First Time Application Execute—This includes the first invocation of any application which has never been observed to execute on the system.
- Network Applications—A network application would include any process that connects as a client or accepts a connection as a server and has in some manner accessed the network. The process would fall into this network application class after it has accessed the network. (This does not include applications that communicate only with other applications on the same system.)

- Processes created by Network Applications—This includes any process that is launched by a network application. For example, one network process may create another process that attempts to download code. This is one way viruses are propagated.
- Processes created by Servers (TCP and UDP)—This includes any TCP or UDP process invoked by a server (falling into the categories detailed in the two following bullet points).
- Server (TCP based)—This application class includes all processes that have accepted an inter-box connection on a non-ephemeral port.
- Server (UDP based)—This application class includes all processes that have accepted an inter-box connection on a non-ephemeral port.
- Processes Monitoring the Keyboard—This includes all processes which continuously monitor keystrokes over an extended period of time.
- Processes with elevated privileges—This application class is only available for UNIX rule types. It includes processes that have elevated user privileges for users other than root, such as ping. Using such processes is a common way to attempt a system break-in. Note that this elevated privilege designation does not apply to processes when the user is logged in as root.
- Recently created untrusted content—This includes executables that are newly created by <Processes writing untrusted content> and are immediately invoked.
- Remote clients—When a remote machine accesses resources over the network that are protected locally by an agent, the agent sees the remote access attempt as coming from a "remote application." The actual application that is used to open the resource in question cannot be determined on the local system. All remote access attempts are seen by the local system as being invoked by a remote application.

  Therefore, if you are writing rules for a machine that other machines can access over the network, you must include <All Applications> or <Remote clients> as your application class. Otherwise, the rule will not work as expected in regard to remote access to those resources.
- System Process (available only in Network Access Control rules)—Using this application class, you can control network access for the operating system itself (as opposed to applications running on the operating system).

**Caution** Any application class that you define does not include the system process. If you want to include the system process in a rule, you must select the included, built-in <All applications> or <System process> classes.

# Built-in Configurable Application Classes

The Management Center for Cisco Security Agents also ships with built-in application classes that are built by policy rules. These application classes appear inside brackets with asterisks before them (*) in the rule application class selection list boxes (see Figure 6-1). This means that you should only use them in conjunction with a rule module that dictates the parameters that causes processes to become classified as one of these application types. CSA MC ships with pre-configured policies to define these classes. You can change these policies, if necessary.

- Authorized rootkit—This is intended to identify modules loading after boot time or to identify modules attempting to modify kernel functionality. Processes are classified as belonging to this application category when a Kernel protection rule detects and tags the process as an authorized rootkit. See Kernel Protection, page 4-84. Note that if a rootkit gets tagged as both authorized and unauthorized (as a result of tagging rules) an authorized rootkit tag gets precedence over and unauthorized tag.
- Installation Applications—This includes processes installing software.
- Processes Communicating with Untrusted Hosts—This is intended to capture the IP addresses of hosts that are viewed as violating security policies or exhibiting malicious behavior. Being classified as belonging to this application category causes a host to be quarantined from the network. See Correlation, page 5-21 for more IP address quarantine details.
- Processes Copying Untrusted Content—This is intended to identify processes that copy executables that need to be treated as untrusted and tracked.
- Processes Executing Untrusted Content—This includes any downloaded executable or any process that is interpreting downloaded content.
- Processing requiring Kernel Only Protection—This is intended to remediate interoperability issues with CSA's user component and other third party software products. Processes in this class will not enforce COM component checks and some buffer overflow checks.

- Processes requiring OS Stack Execution Protection—This application class is only available for UNIX rule types. This is intended to enable native Solaris operating system stack execution protection emulation. This enables additional buffer overflow protection.
- Processes requiring Security Level <High, Medium, Low>—Move applications into this dynamic class to programmatically change the agent security level based on the current running state of the system. For example, if the agent security level is low and a virus is detected on the system, this can trigger a system state policy that will automatically move the security level to high. On a high setting, you may enforce a rule that denies the virus-infected system from making outgoing network connections.
- Processes Writing Untrusted Content—This is intended to identify processes that write executables which need to be treated as untrusted and tracked. e.g., This could identify a network application that downloads an executable and saves it to disk. The process is the network application and the untrusted content is the downloaded executable.
- Suspected Virus Applications:—This application class includes processes dynamically defined as being suspect by specified, exhibited behavior. Being classified as belonging to this application causes a quarantine message to be sent to CSA MC.
- Unauthorized rootkit—This is intended to identify modules loading after boot time or to identify modules attempting to modify kernel functionality. Processes are classified as belonging to this application category when a Kernel protection rule detects and tags the process as an unauthorized rootkit. Then, for example, a system state can take effect as a result of a process being classified as an unauthorized rootkit. See Kernel Protection, page 4-84.

## Preserving Application Process Classes

You should be aware that all application process classes are preserved when your policies are changed if those processes (application classes) are used in an existing policy. For example, processes that have been classified by CSA MC as descendents or as network applications are preserved if the application classes that included them are changed in any way.

On policy changes, process name-based application classes are re-evaluated. Old application class memberships are not lost, only new memberships are gained.

# Configuring Static Application Classes

Access control rules are application-centric. Meaning that when you write your rules, you should understand that the application(s) you select are really the heart of each rule. In your file, network, registry, and COM rules, you are controlling what applications can do to the files, addresses, registry keys, and COM components you specify. So, when you begin creating rules, think in terms of the applications your enterprise as a whole uses and the manner in which you want to limit an application's ability to perform undesired actions.

See also Built-in Application Classes, page 6-4.

To create an application class, do the following:

**Step 1** Move the mouse over **Configuration** in the menu bar and select **Applications>Application Classes** (Windows or UNIX) from the drop-down list that appears. The list of existing Application classes is displayed. CSA MC ships with several pre-configured applications. Some Application classes appear within brackets. These are built-in CSA MC application classes and you cannot edit them.

**Step 2** Click the **New** button to create a new application class. This takes you to the application class configuration view (see Figure 6-2).

**Step 3** Enter a **Name** for the application class you are creating.
It is important to use a descriptive name that you can easily recognize in the application selection list that appears in the rule views.

**Step 4** Enter a **Description** for your application class. This description becomes visible in the application class list view.

**Step 5** **Operating System**—When you create an application class, you must select to either create a UNIX or a Windows application class. Your application class is then designated for all UNIX or all Windows platforms. Optionally, you select to target an operating system more narrowly by selecting a specific UNIX or Windows operating system from the **Target** pulldown menu.

**Step 6** If your lists of application classes are growing too long in rule pages, clicking the **Display only in Show All mode** checkbox on an application class page causes that item to no longer appear in list pages and selection lists. This feature works in conjunction with Admin Preference settings. You must go the Admin Preferences page to make the item reappear. See Administrator Preferences, page 2-6.

**Step 7** Under **Add process to application class**, for a static application class, do the following:

Leave the default **when created from one of the following executables** radio button selected. Then enter the executable file names (one per line) for the applications you are grouping together in this application class.

See Configuring Dynamic Application Classes, page 6-15 for details on that feature.

**Note** You can enter preconfigured File Set variables in the executables edit field by clicking the **Insert File Set** link. To learn more about File Sets, see File Sets, page 7-10.

**Step 8** **Remove process from application class**—Select the checkbox beside **After** and enter a time frame in **seconds** to configure an application classification which expires after a period of time. Only use this feature if you have a rule that requires it. In general, you do not have to specify a time-out for application classifications. See Removing Processes from Application Classes, page 6-2 for details.

For UNIX application classes, you have the additional option of selecting the **When session association is voided** checkbox. Selecting this checkbox causes the application classification to be removed when a process disassociates itself from the current TTY session. For example, when an application class exists for applications descended from "superuser", you might not want the process to continue having the application class of the superuser shell.

**Step 9** When applications are invoked, they often spawn other processes as part of the action they are performing. When you create an application class, select one of the following radio buttons to determine when processes spawned by the applications in the application class are also included.

- Only this process
- This process and all its descendents
- Only descendents of this process

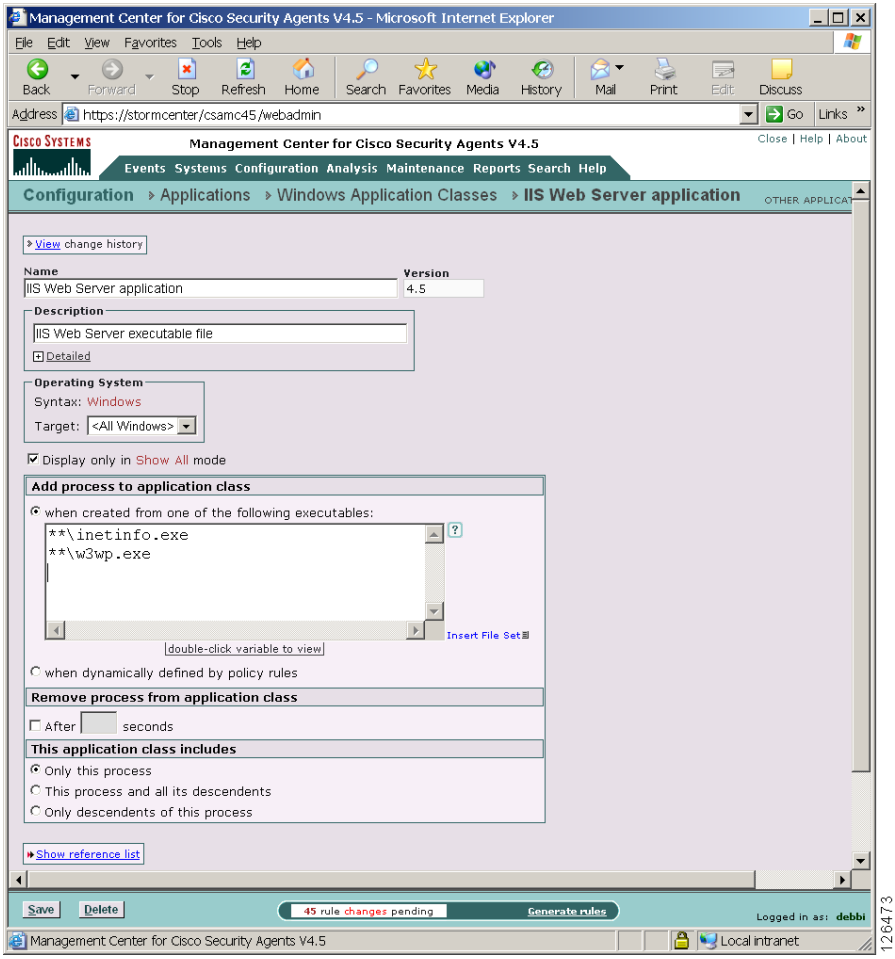
  (Creating an application class for "Only descendents of this process" is useful when making exceptions to a rule that is written for the main process itself. For example, you can write a rule allowing IIS to talk on the network, but create another rule denying descendents of the IIS process from talking on the network.)

**Step 10** When you are finished, click the **Save** button. This application class name, IIS Web Server application, now appears in the application list view and in the application selection fields for rule configurations. When you select it in a rule, you are indicating all the executables that comprise it.

**Note** You can use the Compare button in the Application Class list view to compare and merge similar application classes. See Comparing Configurations, page 4-39 for details on using the Compare tool.

See Dynamic Application Classes, page 6-13 for information on that application class type.

*Figure 6-2 Static Application Class*



# Dynamic Application Classes

The configurable application classes described in the previous pages are considered static application classes. Basically, in a static application class, a process is added to the class based on the name of its executable file (or the process name). Alternatively, you can build an application class based on an application's behavior rather than by a specific application executable name. This would be a dynamic application class defined by process behavior on a system. There are already built-in dynamically defined application classes in CSA MC. For example, the <Processes executing untrusted content> application class is a "built-in" dynamically configured class.

One example of an instance in which you might need a dynamic application class would be if you are writing rules for email clients but you do not know all the different email applications that are being used throughout your corporate network. In this case, you could use a dynamic application class. Any process appearing to act as a client for SMTP (you can use whatever criteria you decide to define what an email application is) would fall into a dynamic email application class that could be used in rules quarantining dangerous email messages.

## Building Classes as Rule Consequences

You can also build a dynamic application class as a consequence of rules triggering. This way, for example, you can configure a query user rule in which a process is added to an application class as a result of a specific user response (yes, no, terminate). For example, you can build a "suspected virus" application class based on the end user being queried when untrusted content arrives on the desktop and the Terminate button on a query box is clicked to disallow it. But if the user clicked Yes to allow it, the process would not be added to the suspected virus application class.

## Removing Processes from Classes

You can also use a dynamic "remove process" capability in conjunction with dynamically adding a process. For example, you can dynamically add a process to a "suspicious web server descendents" class if a web server spawns a process. Then, if that spawned process attempts to read a script from a normally accessed directory, you can decide this isn't a dangerous process and have the process

removed from the class after the attempt. But if the spawned process attempts to read a script from a directory it should not be accessing, the process should remain in the suspicious web server descendents class.

# Defining Dynamic Classes

**Note** A dynamically defined application class can be used in any rule where a static application class can be used.

Define a dynamic application class by doing the following:

- Create a new application class and select the **Processes dynamically defined by policy rules** radio button. (Do not enter any process names in the Application class page edit field.)
- Configure an application-builder rule to define your dynamic application class.

**Note** Configuring the dynamic application class is only the first step. It does not become populated by processes until it is selected in a rule that will be used to define it.

For example, create a new File access control rule and select **Add process to application class** from the pulldown list as the rule action. Then choose the name of the dynamic application class (created in the first bullet point) from the pulldown list. Configure the remaining rule parameters. This rule type takes precedence over all others in the policy, but it does not override other rules in the policy the way allow, deny, and query rules do when triggered.

- Configure another rule to control the actions of this dynamic application class. As processes are added to this dynamic application class, those same processes will be used in all other rules in which the dynamic class is selected.

The following section provides an example of defining and using a dynamic application class in a policy

# Configuring Dynamic Application Classes

Continuing to use the email client example, we will create an application class that will be dynamically populated by email client applications. You might want to do this if you are writing rules to protect email applications, but you do not know what email applications are being used across your network. Using this dynamic class, rules will restrict email clients based on detected behavior, such as using SMTP to access an email server, rather than by explicitly defining email application executables.

To create a dynamic application class, do the following:

**Step 1** Move the mouse over **Configuration** in the menu bar and select **Applications>Application Classes** (Windows or UNIX) from the drop-down list that appears. The list of existing Application classes is displayed.

**Step 2** Click the **New** button to create a new application class. This takes you to the application class configuration view (see Figure 6-3).

**Step 3** Enter a **Name** for the dynamic application class you are creating. It is important to use a descriptive name that you can easily recognize in the application selection lists that appear in the rule views.
For this example, we will create a new dynamic class called *Email clients_dynamic*. We will use this class to determine what email client applications are running on systems. Then we will add this dynamic class to an existing email quarantine rule.

**Step 4** Enter a **Description** for your application class.

**Step 5** If your lists of application classes are growing too long in rule pages, clicking the **Display only in Show All mode** checkbox on an application class page causes that item to no longer appear in list pages and selection lists. This feature works in conjunction with Admin Preference settings. You must go the Admin Preferences page to make the item reappear. See Administrator Preferences, page 2-6.

**Step 6** Under **Add process to application class**, for a dynamic application class, do the following:

- Select the **when dynamically defined by policy rules** radio button. (Do not enter any process names in the edit field.)

**Step 7** **Remove process from application class**: Select the checkbox beside **After** and enter a time frame in **seconds** to configure an application classification which expires after a period of time. Only use this feature if you have a rule that requires it. In general, you do not have to specify a time-out for application classifications. See Removing Processes from Application Classes, page 6-2 for details.

For UNIX application classes, you have the additional option of selecting the **When session association is voided** checkbox. Selecting this checkbox causes the application classification to be removed when a process disassociates itself from the current TTY session. For example, when an application class exists for applications descended from "superuser", you might not want the process to continue having the application class of the superuser shell.

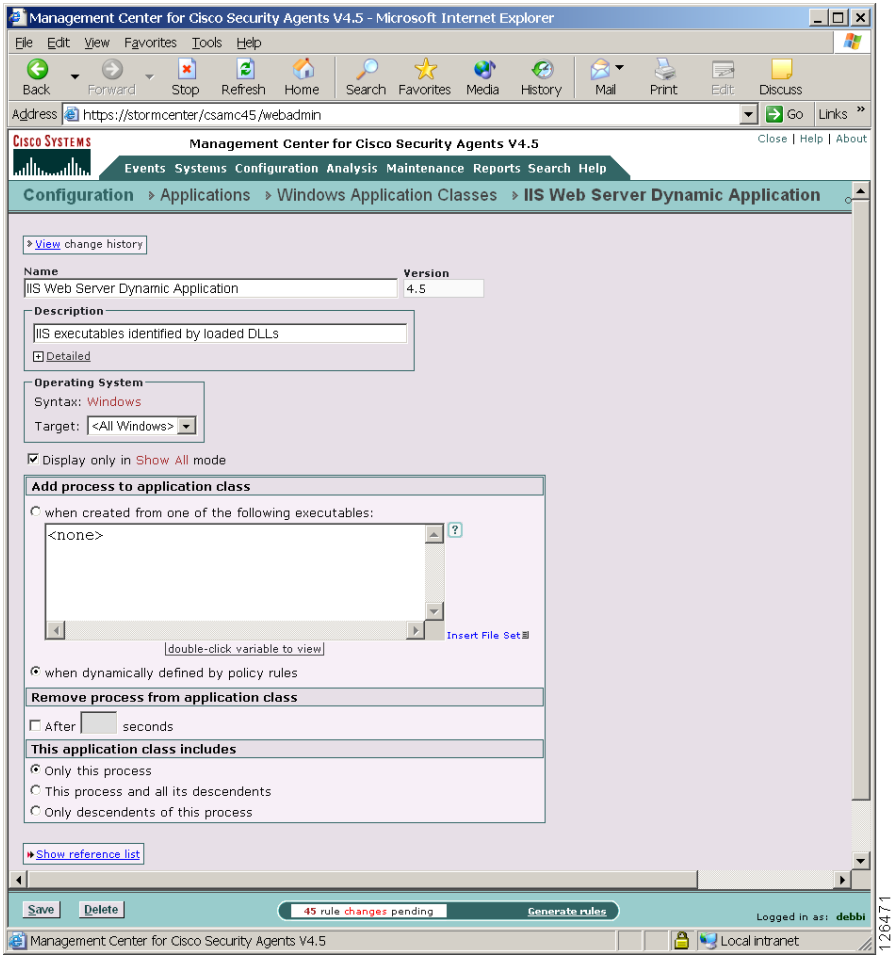
**Step 8** When applications are invoked, they often spawn other processes as part of the action they are performing. When you create a dynamic application class, you can select one of the following radio buttons (just as you can when you create a static application class) to determine when processes spawned by the applications in the dynamic application class are also included.
For this example, we will leave the default, Only this process, selected.

- Only this process
- This process and all its descendents
- Only descendents of this process

**Step 9** When you are finished, click the **Save** button. This dynamic application class name now appears in the pulldown list beside the **Add to application class** radio button in access control rules and in all application selection fields.

Next we will use this dynamic class in an application-builder rule that will define the class.

*Figure 6-3 Dynamic Application Class*



# Configure an Application-Builder Rule

In this example, we are going to use a Network access control rule to define our dynamic application class. You can use any access control rule type as your application-builder rule. We are adding this rule to the Desktop Module that ships with CSA MC. (Remember, your dynamic application class is not populated with applications until an application-builder rule is triggered by the process's behavior and added to the class.)

**Note** Defining dynamic application classes from the Application control rule is a bit different than creating them from other rule types. Because this rule has two application class fields, you can choose to add the current application to the dynamic class or choose to add the new application that is invoked by the first application to the dynamic class.

**Caution** Dynamic application class process membership is temporary and is based on a running process meeting the criteria in the application-builder rule. When the process is no longer running on a system, it is no longer included in the dynamic class.

To prevent errors or unexpected behavior, you should avoid selecting the dynamic application class for a rule within a policy that does not also include the corresponding application-builder rule. Both the application-builder rule and the subsequent rule(s) that use the dynamic application class should co-exist within the same policy—although this is not required.

**Step 1** To configure the application-builder rule which will dynamically create a new Email client class, access the Desktop rule module and click the **Modify rules** link.

**Note** This is only an example. This is not intended to recommend that you add this rule to the Desktop module. This simply shows you what you can do if you do not know all the Email clients being used on systems across your network.

**Step 2** Click **Add rule** and select **Network access control**.

**Step 3** In the Network access control rule, configure the following (see Figure 6-4):

- Enter a description
- Select the **Add process to application class** radio button. Select the dynamic application class, *Email clients_dynamic*, from the corresponding pulldown list.

**Note** This rule type takes precedence over all other types but it does not override them. The only action of this rule is to build the application class for any subsequent rules within the policy that make use of it.

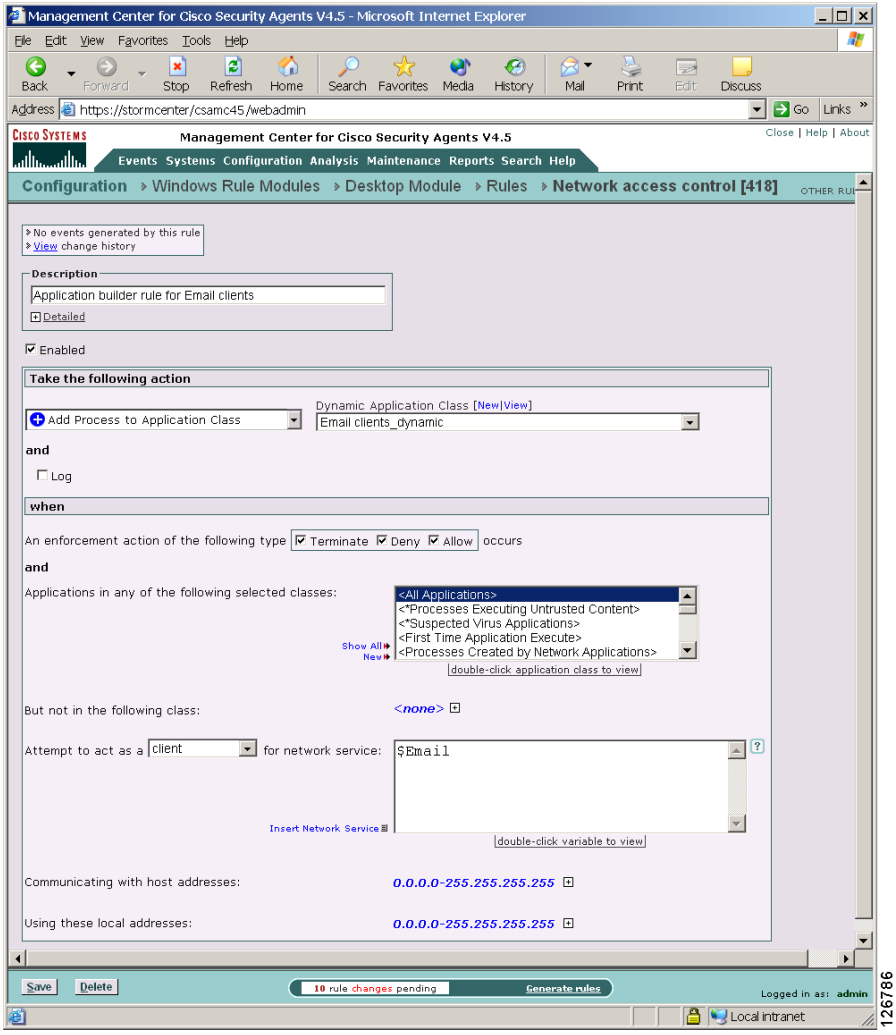
- **When—An enforcement action of the following type occurs**. Optionally, you can select one more of the available checkboxes. (Terminate, Deny, Allow) All entries are selected by default meaning that the tag will apply when the request is made regardless of the action that occurs. All actions apply. If you make a specific selection here, you are determining to create your dynamic application class based on that action occurring when the request is made (perhaps via another configured rule). You should note that all resource requests always result in either an allow, deny, or terminate occurring. Even if there is no rule governing the resource, for example, the implicit action is allow. See Building Classes as Rule Consequences, page 6-13.
- Leave the default, **<All Applications>**, selected in the Application class field.
  This way, all applications that trigger the rule have the potential of being added to the dynamic class. You could select another application class here if you only want specific applications to fall into the dynamic class.
- Select **client** from the pulldown list and select the pre-configured variable, $Email, from the list of configured Network services.
- Leave the default of 0.0.0.0-255.255.255.255 entered in the host addresses field.
- Leave the default of 0.0.0.0-255.255.255.255 entered in the Use these local addresses field.

**Step 4** Click **Save**.

Now, based on the application-builder rule we've just configured, any application which uses the network services, SMTP, POP3, IMAP3 or IMAP2 as a client to access any system on the network, will fall into the Email clients_dynamic application class.

Next we will select this dynamic application class in a rule within this same policy.

*Figure 6-4 Application-Builder Rule*



# Configure a Rule Using a Dynamic Application Class

In this example, we are going to use a File access control rule to control the actions of a dynamic application class.

**Step 1** Configure this rule in the same manner in which you configure any other rule. For this example, once again access the Desktop Module policy (This is the policy already containing our application-builder rule.) and click the **Modify rules** link.

**Step 2** Click **Add rule** and select **File access control**.

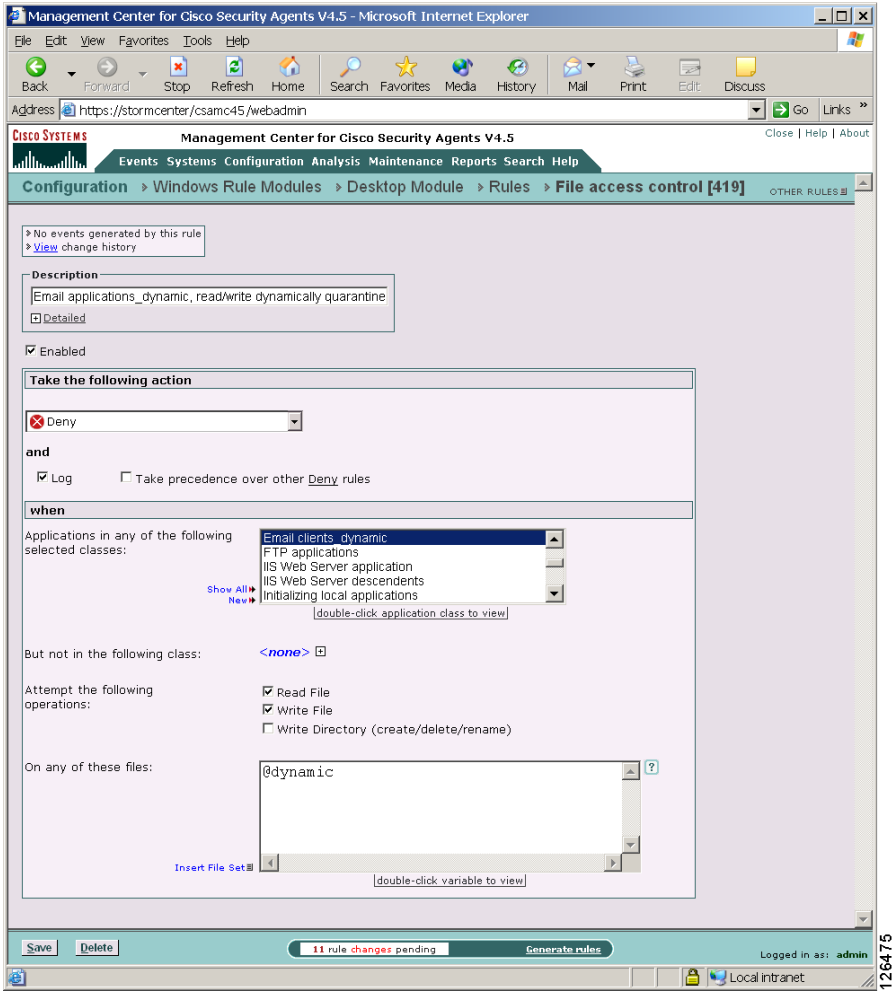
**Step 3** In the File access control rule, configure the following (see Figure 6-5):

- Enter a description
- Select the **Deny** radio button.
- Select the dynamic application class, **Email clients_dynamic**, in the Application class list box.
- Select the **read file** and **write file** checkboxes.
- Enter **@dynamic** in the files field.

**Step 4** Click **Save**.

This rule will prevent any email application that falls into the selected dynamic email client class from reading or writing any dangerous, quarantined files.

*Figure 6-5 Rule with Dynamically Defined Application*




# Create New Application Classes from Rule Pages

You can create a new application class from a rule page and have that application class be available to the rule you're currently configuring and to all other rules as well.

From the rule page, click the **New** link beside the Application class selection field to access configuration window. Configure your new application class and click **Save**. It is now available for selection in the rule page.

Also available for Application classes from the rule page, is the ability to view the configuration parameters for a selected application class. Double-click an application class in the rule page to view its configuration page.

# Application Class Management

The Application Class Management page (available from the **Configuration** option in the menu bar) allows you to pare down the application class selection fields in the rule pages and in the Analysis feature pages. If you have a long list of application classes and you only want to view specific classes in rule configuration pages or only view them in the rule pages or only view them for analysis, you can choose to have application classes appear or not appear in features you select.

Note that selecting certain application classes to not appear in certain products does not delete those application classes. They will still appear in the main Application Class list page. They simply will not appear in the application class selection fields in the feature in question. By default, all application classes appear in all application class fields in all feature sets.

To enable or disable an application for general configuration or for analysis purposes, do the following:

**Step 1** Move the mouse over **Configuration** in the menu bar and select **Applications**>**Application Class Management** from the drop-down list that appears. In the Application Class Management page (see Figure 6-6) there are swap box fields for CSA MC and for Application Behavior Investigation and Application Deployment Investigation.

The application classes appearing in the white swap box(es) (the bottom swapbox for each category) are enabled for the feature in question. Those appearing in the gray swap box(es) (the top swapbox for each category) will not appear in the feature in question.

**Step 2** Select an application class and click the up arrow or down arrow buttons to move the selected class to the other swap box. This action enables or disables the application for the product. (It does not delete the application class.)

**Note** Use the "Show [All, UNIX, Windows] application classes that apply to [<All features>, Management Center for Cisco Security Agents, Application Behavior Investigation, Application Deployment Investigation]" to narrow the application class categories to specific product components.

***Figure 6-6 Application Class Management Window***


# Configuring Variables

## Overview

Configuration variables are named configuration data items that you create for repeated use in other configuration items such as file access control rules, network access control rules, and alerts. You can group files together, as well as network addresses, and network services. Once configured, you enter these global variables in corresponding fields for other CSA MC items.

You use configuration variables to help build the rules that form your policies. Using variables makes it easy for you to maintain policies by letting you make any necessary modifications in one place and having those changes instantiated across all rules and policies.

This section contains the following topics.


- Where Variables are Used, page 7-2
- COM Component Sets, page 7-3
- COM Component Extract Utility, page 7-6
- Data Sets, page 7-7
- File Sets, page 7-10
- Network Address Sets, page 7-15
- Network Services, page 7-18
- Registry Sets, page 7-21
- Query Settings, page 7-25
- Localized Language Version Support, page 7-29

# Where Variables are Used

Figure 7-1 displays how variables relate to access control rules. In the diagram, variables (Event Sets, Query Settings, File Sets, Network Address Sets, Network Services, Registry Sets, COM Component Sets, and Data Sets) are shown on the left and the rule types they can be applied to are shown on the right.

***Figure 7-1 Variable Use in Rules***

**Note** Using variables is optional (note that Application Classes are included in this diagram, but they are not optional). Nearly all the information used in variable configurations can also be entered directly into corresponding rule configuration fields. Variables are simply a tool meant to simplify the creation of rules, especially if the same configurations are used in multiple rules.

**Note** You can use the Compare button in Variable list views to compare and merge similar variables. See Comparing Configurations, page 4-39 for details on using the Compare tool.

See for Chapter 8, "Event Logging and Alerts" details on configuring Event Sets.

## Display only Show All mode Option

Each individual variable page (including Application Classes) contains a Display only in Show All mode checkbox. If your lists of variables are growing too long in rule or application configuration pages, clicking the Display only in Show All mode checkbox on a variable page causes that variable to no longer appear in lists for that variable type. To display hidden items, you must go to the Admin Preferences page and choose another admin preferences that Always uses Show All mode or change the preference assigned to you. See Administrator Preferences, page 2-6.

# COM Component Sets

Configure COM component sets for use in COM component access control rules. COM objects are groupings of COM Program IDs (PROGID's) and/or COM Class IDs (CLSID's) under one common name. This name is then used in COM component access control rules to allow or deny access to the COM component set name. All COM components that match the entries of a given component set are relevant to the rule in which the set is used.

You can also use pattern matching when creating COM component sets. For example, entering "Word.*" would match "Word.Application" and "Word.Document".

CSA MC ships with several pre-configured COM component sets you can use as well.

**Note** This is not available for UNIX configurations.

**Note** CSA MC provides a COM component import utility which installs with each Cisco Security Agent. Running this utility extracts all COM component PROGID's and CLSID's for software running on the system in question. See page 7-6 for instructions.

To configure a COM component set, do the following.

**Step 1** From the menu bar **Configuration** drop-down list, move the mouse over **Variables**. A cascading menu with further selections appears.

**Step 2** Select **COM Component Sets** from the cascading menu. Any existing COM component set configurations are shown.

**Step 3** Click the **New** button to create a new COM component set. This takes you to the configuration view (see Figure 7-2).

**Step 4** In the available edit fields, enter the following information (See Using the Correct Syntax, page 2-28. You can also click the Quick Help question mark beside each field for syntax information.):

- **Name**—This is a unique name for this COM component set. Generally, it's a good idea to adopt a naming convention that lets you quickly enter COM component set names in a corresponding rule configuration field.
- **Description**—This is a line of text that is displayed in the list view helping you to identify this particular COM component set configuration.
- **Display only in Show All mode**—If your lists of variables are growing too long in rule or application configuration pages, clicking the Display only in Show All mode checkbox on a variable page causes that variable to no longer appear in selection lists for that variable type. This feature works in conjunction with Admin Preference settings. You must go the Admin Preferences page to make the item reappear. See Administrator Preferences, page 2-6.

**Step 5** **PROGID's/CLSID's matching**—Enter the COM component PROGID's or CLSID's here (one per line) to which you want to impose restrictions.

By default, this field has an <all> entry indicating all PROGID's and CLSID's. When you click inside this field, the <all> disappears so that you can enter your own restrictions.

When entering PROGID's, use syntax as shown in the following example:

```
Outlook.Application
```

When entering CLSID's (uppercase hexadecimals), using the following syntax (You must include the brackets shown here.):

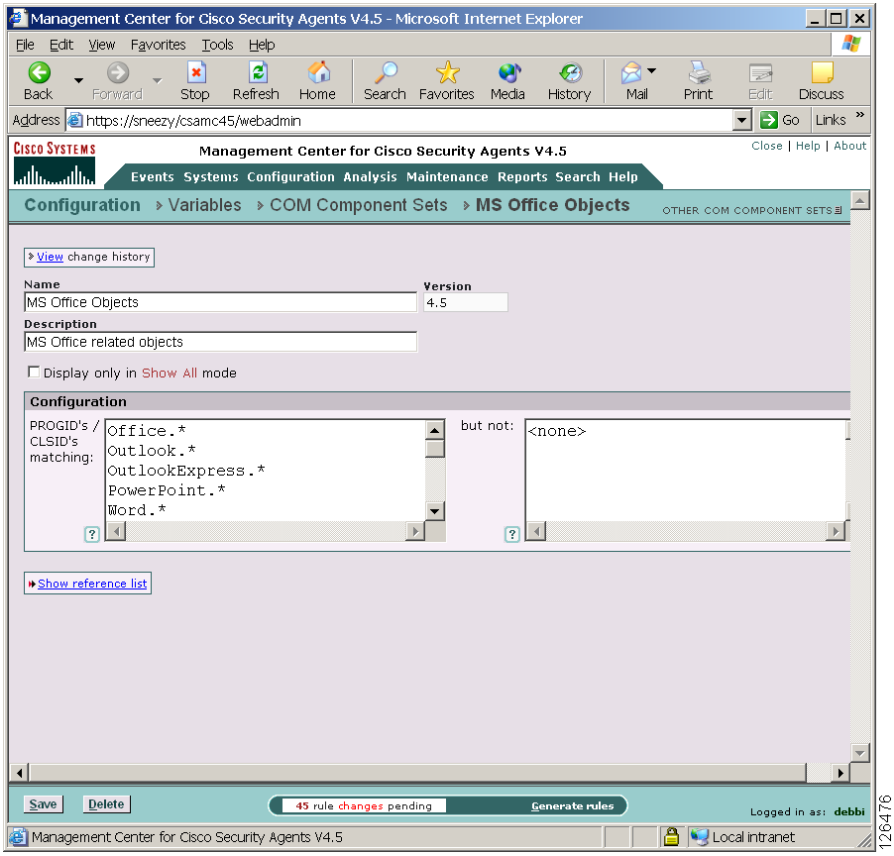
```
{000209FF-0000-0000-C000-000000000046}
```

**Step 6** **but not**—Make exceptions to PROGID's or CLSID's you've entered in the PROGID's/CLSID's matching field.

By default, this field has a <none> entry indicating no exceptions. When you click inside this field, the <none> disappears so that you can enter your own exceptions.

When all required information is entered, click the **Save** button to save your COM component set in the CSA MC database.

*Figure 7-2 COM Component Set Configuration View*




# COM Component Extract Utility

CSA MC provides a COM component extraction utility, called `extract_com`, which installs in the Cisco\CSAgent\bin directory with each Cisco Security Agent. Running this utility extracts all COM component PROGID's and CLSID's for software installed on the system in question and places this data into a text file. You can cut and paste these ID's from the text file into your COM component sets and access rules.

See Using the COM Extract Utility, page 10-9.

# Data Sets

Configure data sets for use in data access control rules. Data sets are groupings of data strings under one common name. These strings represent a set of patterns that will be matched against the URI portion of HTTP requests. The name of the data set is then used in rules that control data access permissions and restrictions. All the data parameters that exist under that name are then applied to the rule where the name is used.

CSA MC ships with several pre-configured Data Sets you can use. The pre-configured data sets group patterns to match based upon the following:

- functional associations of meta-characters (e.g. "(" and ")")
- examples of known classes of attacks
- Web server specific exploits

The following is an example of an HTTP request attempting to execute an attack by invoking a command shell to obtain a directory listing. A data set of this syntax, *cmd.exe*, would stop not only this exploit but any other exploit trying to make use of a command shell.

```
GET /scripts/..%255c%255c../winnt/system32/cmd.exe?/c+dir
```

**Note** Not all pre-configured data sets are used in pre-configured policies. For example, some attack fingerprints or command arguments might be acceptable on one deployment of a web server, but not be acceptable for a different deployment. Therefore, pre-configured data sets used in shipped policies may require modification if legitimate, but blocked meta-characters are being used by a web server.

**Note** Additionally, modifying the preconfigured data sets allows you to block a pattern which specifically matches a new/old exploit or attack.

To configure a data set, do the following.

**Step 1** From the menu bar **Configuration** drop-down list, move the mouse over **Variables**. A cascading menu with further selections appears.

**Step 2** Select **Data Sets** from the cascading menu. Any existing data set configurations are shown.

**Step 3** Click the **New** button to create a new data set. This takes you to the data set configuration view.

**Step 4** In the available edit fields, enter the following information. (Note that you can click the Quick Help question mark beside each field for syntax information.):

- **Name**—This is a unique name for this data set. Generally, it's a good idea to adopt a naming convention that lets you quickly enter data set names in a corresponding rule configuration field.
- **Description**—This is a line of text that is displayed in the list view helping you to identify this particular data set configuration.
- **Display only in Show All mode**—If your lists of variables are growing too long in rule or application configuration pages, clicking the Display only in Show All mode checkbox on a variable page causes that variable to no longer appear in selection lists for that variable type. This feature works in conjunction with Admin Preference settings. You must go the Admin Preferences page to make the item reappear. See Administrator Preferences, page 2-6.

**Step 5** **Patterns matching**—Enter the data strings here (one per line) to which you want to impose restrictions. By default, this field has an <all> entry indicating all strings. When you click inside this field, the <all> disappears so that you can enter your own data. This pattern is used by HTTP Web servers to match against the requested URI (Uniform Resource Identifier) to enforce allow/deny Data access control rules.

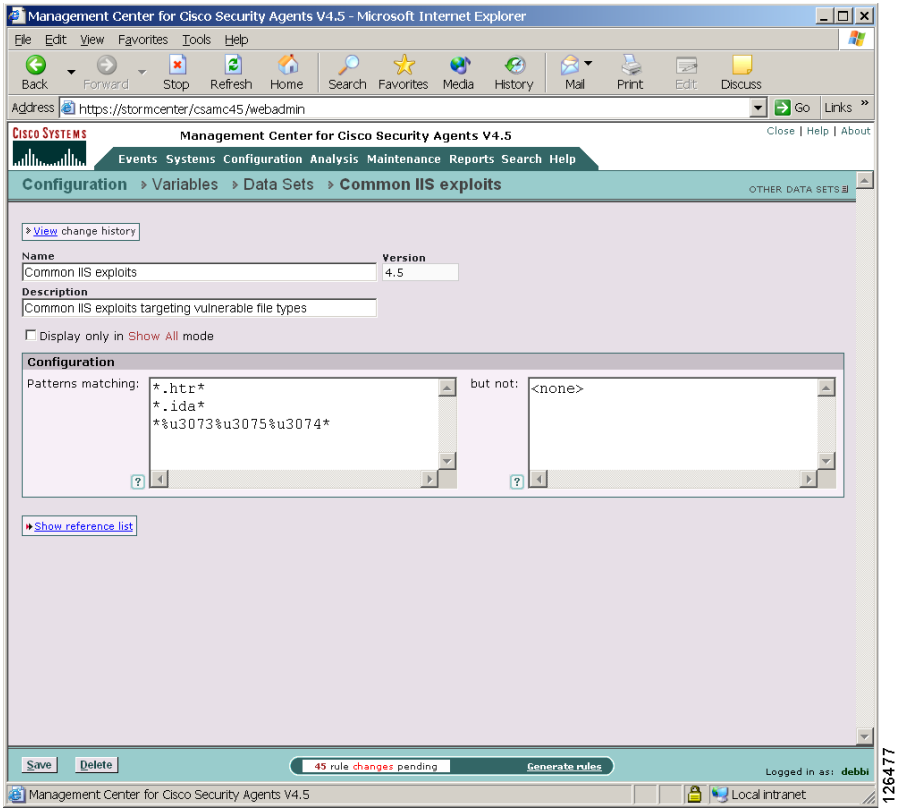
**Note** When entering data patterns, the "*" character is a generic wildcard specification.

**Step 6** **but not**—Make exceptions to the data strings you've entered in the directories matching field. By default, this field has a <none> entry indicating no exceptions. When you click inside this field, the <none> disappears so that you can enter your own exceptions.

**Step 7** When all required information is entered, click the **Save** button to save your data set in the CSA MC database.

You can now enter this data set name by clicking the **Insert Data Set** link in the data access control rule files field.

*Figure 7-3 Data Set Configuration View*



# File Sets

Configure file sets for use in file access control rules and application classes. File sets are groupings of individual files and directories under one common name. This name is then used in rules that control directory and file permissions and restrictions. All the parameters that exist under that name are then applied to the rule where the name is used.

CSA MC ships with several pre-configured File Sets you can use.

To configure a file set, do the following.

**Step 1** From the menu bar **Configuration** drop-down list, move the mouse over **Variables**. A cascading menu with further selections appears.

**Step 2** Select **File Sets [UNIX or Windows]** from the cascading menu. Any existing file set configurations are shown.

**Step 3** Click the **New** button to create a new file set. This takes you to the file set configuration view (see Figure 7-4).

**Step 4** In the available edit fields, enter the following information (See Using the Correct Syntax, page 2-28. You can also click the Quick Help question mark beside each field for syntax information.):

- **Name**—This is a unique name for this file set. Generally, it's a good idea to adopt a naming convention that lets you quickly enter file set names in a corresponding rule configuration field. When using configuration variables in file access rules, network access rules and application classes, you must enter the variable name preceded by a dollar sign:

  For example, if you have a file set variable named cgi_files, you must enter `$cgi_files` into any edit field where you are using this variable. The dollar sign tells CSA MC that this is a variable value.

- **Description**—This is a line of text that is displayed in the list view helping you to identify this particular file set configuration.

- **Display only in Show All mode**—If your lists of variables are growing too long in rule or application configuration pages, clicking the Display only in Show All mode checkbox on a variable page causes that variable to no longer appear in selection lists for that variable type. This feature works in

conjunction with Admin Preference settings. You must go the Admin Preferences page to make the item reappear. See Administrator Preferences, page 2-6.

**Step 5** **Operating System**—When you create a file set, you must select to either create a UNIX or a Windows file set. Your file set is then designated for all UNIX or all Windows platforms. Optionally, you select to target an operating system more narrowly by selecting a specific UNIX or Windows operating system from the **Target** pulldown menu.

**Step 6** **Directories matching**—Enter the directories and files here (one per line) to which you want to impose restrictions.

By default, this field has an <all> entry indicating all directories. When you click inside this field, the <all> disappears so that you can enter your own directory restrictions. When entering directory restrictions, use the following syntax (See Using the Correct Syntax, page 2-28):

Windows example:

```
c:\Program Files\**\*SQL*\bin\**
\Program Files\**\*SQL*\bin
```

UNIX example:

```
/apache/webroot/**
/usr/admn/sg
```

**Note** See Using the Correct Syntax, page 2-28 for details for information on protecting directory paths and files.

**Step 7** **but not**—Make exceptions to the files and directories you've entered in the directories matching field. For example:

Windows example:

```
c:\Program Files\**\*SQL*\bin\temp
```

**Caution** The exclusion entry above means that any temp files in the bin folder are ignored by the restrictions you apply using this file set. This also means that the path you're protecting in the Directories matching field is NOT protected when the excluded directory "temp" is being accessed.

UNIX example:

`/etc/passwd`

By default, this field has a <none> entry indicating no exceptions. When you click inside this field, the <none> disappears so that you can enter your own exceptions.

**Step 8** **Files Matching**—Enter the names of the files to which you are controlling access.

You can use wildcards here to indicate all of a specific file type. For example, `*.exe` to specify all executables.

By default, this field has an <all> entry indicating all files. When you click inside this field, the <all> disappears so that you can enter your own file restrictions.

**Step 9** **but not**—Make exceptions to the file names you enter in the Files Matching field. For example, all executables, but not regedit.exe.

By default, this field has a <none> entry indicating no exceptions. When you click inside this field, the <none> disappears so that you can enter your own exceptions.

**Note** Use **@dynamic** in the File set text field to indicate all files that have been quarantined by CSA MC. This list updates automatically (dynamically) as logged quarantined files are received.

To view the files that are added to the dynamically quarantined files list and to manually add files to be quarantined, click the **Manage dynamically quarantined files** link on the Global Event Correlation page. See Manage Dynamically Quarantined Files and IP Addresses, page 5-23 for more information.

**Step 10** (UNIX only instruction) File Sets created for UNIX have an additional configuration field. In the **Attributes Matching** edit fields, click the **Insert attribute** link and optionally select one or more file types to match against. Available file types are as follows:

- block device—A special file used for buffered or block I/O. For example, a disk device.
- character device—A special file used for unbuffered or character I/O. For example, a tty file.
- executable file—A file identified in /etc/magic as being executable.

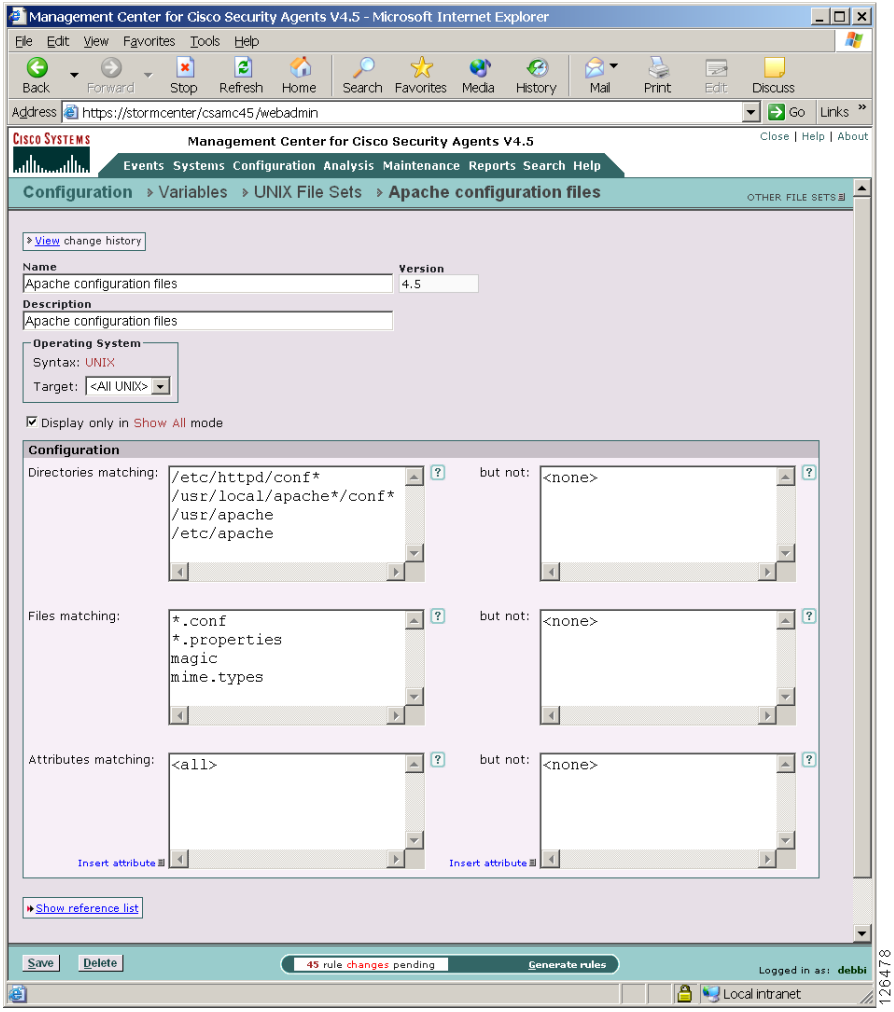
- interpreter file—A file which contains a script (shell, Perl, etc.) where the first line starts with "#! interpreter [arg]".
- java class file—A file identified in /etc/magic as being executable Java byte code.
- setgid file—A file with the "set group ID on execution" property set in the file mode.
- setuid file—A file with the "set user ID on execution" property set in the file mode.

**Step 11** When all required information is entered, click the **Save** button to save your file set in the CSA MC database.

You can now enter this file set name by clicking the **Insert File Set** link in the application class files field and in the file access control rule files field.

**Note** At the top of each variable page, there is a **View change history** link. Click this link to go to a page which lists all the changes that have been made to the item in question. This View change history link is also available for application classes, policies, and rules.

*Figure 7-4 File Set Configuration View*



# Network Address Sets

Configure network address sets for use in network access control rules to impose restrictions on specified IP addresses or a range of addresses. Once configured, you can simply enter the name of the address set in any network access control rules you create.

To configure network address sets, do the following.

**Step 1** From the menu bar **Configuration** drop-down list, move the mouse over **Variables**. A cascading menu with further selections appears.

**Step 2** Select **Network Address Sets** from the cascading menu. Any existing address set configurations are shown.

**Step 3** Click the **New** button to create a new network address set. This takes you to the configuration view (see Figure 7-5).

**Step 4** In the available edit fields, enter the following information (See Using the Correct Syntax, page 2-28. You can also click the Quick Help question mark beside each field for syntax information.):

- **Name**—This is a unique name for this address set. When using configuration variables in file access rules, network access rules and application classes, you must enter the variable name preceded by a dollar sign:

  For example, if you have a network address set variable named Finance systems, you must enter `$Finance systems` into any edit field where you are using this variable. The dollar sign tells CSA MC that this is a variable value.

- **Description**—This is a useful line of text that is displayed in the list view and helps you to identify this particular set of addresses.

- **Display only in Show All mode**—If your lists of variables are growing too long in rule or application configuration pages, clicking the Display only in Show All mode checkbox on a variable page causes that variable to no longer appear in selection lists for that variable type. This feature works in conjunction with Admin Preference settings. You must go the Admin Preferences page to make the item reappear. See Administrator Preferences, page 2-6.

**Step 5** **Enter address ranges**—In the available edit field, enter a single address or a range of addresses.

By default, this field has a <all> entry indicating no addresses. When you click inside this field, the <all> disappears so that you can enter your own addresses. When entering addresses, put each entry on its own line. Here are examples of address entries using proper syntax:

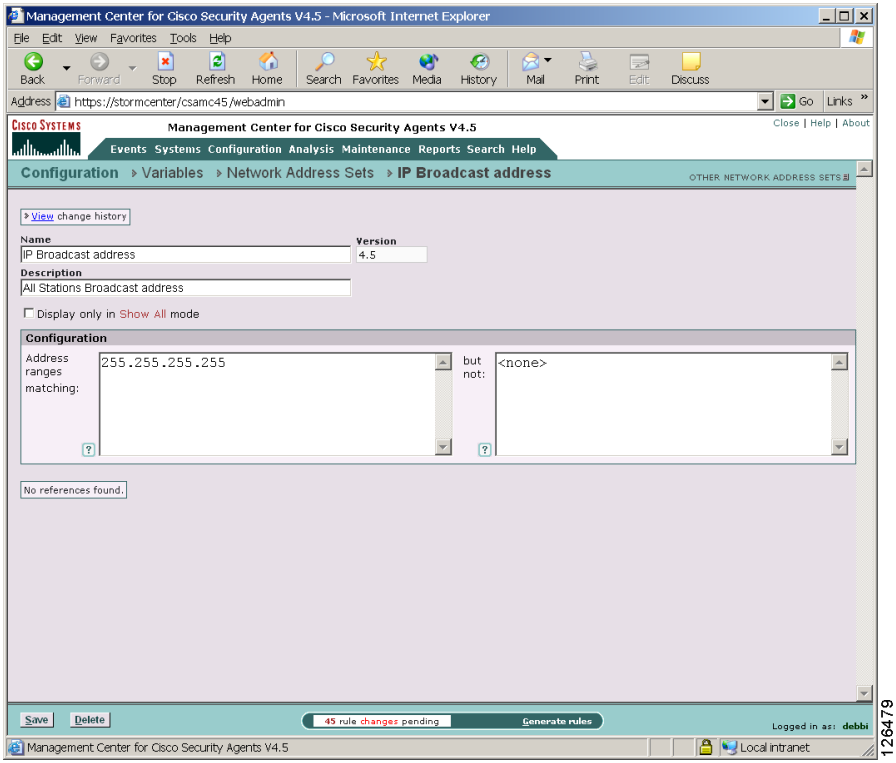
| | |
|---|---|
| 128.66.24.130 | Indicates one address |
| 128.67.2.10-20 | Indicates a range of addresses<br>128.67.2.**10** - 128.67.2.**20** |
| 128.67.3.0-4.255 | Indicates a range of addresses<br>128.67.**3.0** - 128.67.**4.255** |
| 128.67.0.0/16 | Indicates a range of addresses<br>128.67.**0.0** - 128.67.**255.255** |

Use **@local** to indicate all local addresses on the agent system. You would want to use this if you are allowing different applications on a single system to talk to each other without opening these applications up to network access.

**Note** Use **@dynamic** in the Addresses set field to indicate untrusted hosts that have been quarantined by CSA MC. Addresses are added to this list when they are seen as an untrusted host. (The built-in "Processes Communicating with Untrusted Hosts" is triggered in a rule.) This list updates automatically (dynamically) as logged quarantined addresses are received.

**Caution** On UNIX platforms, IPV6 addresses are not officially supported; however, an IPV6 connection will work as the applied rules dictate if the address in question is covered by the "all" addresses range (0.0.0.0-255.255.255.255 includes IPV6 addresses) or by @local. Local addresses on the agent system (indicated by @local) also include IPV6 addresses.

*Figure 7-5 Network Address Set Configuration View*




**Step 6** When all required information is entered, click the **Save** button to save your address set in the CSA MC database.

**Note** You can now enter this network address set name by clicking the **Insert Network Address Set** in the network access control rule host addresses field.

# Network Services

Configure network services for use in network access control rules to add preconfigured protocol and port number restrictions. You can restrict by initial connection ports, and when applicable, by subsequent client/server connection.

CSA MC ships with several pre-configured network services you can use.

To configure network services, do the following.

**Step 1** From the menu bar **Configuration** drop-down list, move the mouse over **Variables**. A cascading menu with further selections appears.

**Step 2** Select **Network Services** from the cascading menu. Any existing configurations are shown.

**Step 3** Click the **New** button to create a new network service variable. This takes you to the configuration view (Figure 7-6).

**Step 4** In the available edit fields, enter the following information (See Using the Correct Syntax, page 2-28. You can also click the Quick Help question mark beside each field for syntax information.):

- **Name**—This is a unique name for this network service configuration. This name is case insensitive. Generally, it's a good idea to adopt a naming convention that lets you quickly enter network service variables in network access control rule configuration fields. When using configuration Variables in file access rules, network access rules and application classes, you must enter the variable name preceded by a dollar sign.

  For example, if you have a network service variable named FTP Service, you must enter `$FTP Service` into any edit field where you are using this variable. The dollar sign tells CSA MC that this is a variable value.

- **Description**—This is a useful line of text that is displayed in the list view and helps you to identify this particular configuration.

- **Display only in Show All mode**—If your lists of variables are growing too long in rule or application configuration pages, clicking the Display only in Show All mode checkbox on a variable page causes that variable to no longer appear in selection lists for that variable type. This feature works in conjunction with Admin Preference settings. You must go the Admin Preferences page to make the item reappear. See Administrator Preferences, page 2-6.

**Step 5** **Protocol ports**—Enter a tcp or udp protocol and corresponding port or port range to indicate a restriction according to the system that is initiating the connection

By default, this field has a <none> entry indicating no ports. When you click inside the edit field, the <none> disappears so that you can enter your own port restrictions. For example:

Use the following syntax:

```
TCP/21
UDP/1025-65535
```

**Note** Some protocols, such as ftp, create additional connections as part of the same session started by the initial connection. The port numbers used for these additional connections must be defined as another Network Service and used appropriately in a rule module to consider callback connections. When a network service is used in an allow rule, once an initial connection is established, the subsequent connections will also be allowed, but only to the process that participated in the initial connection.

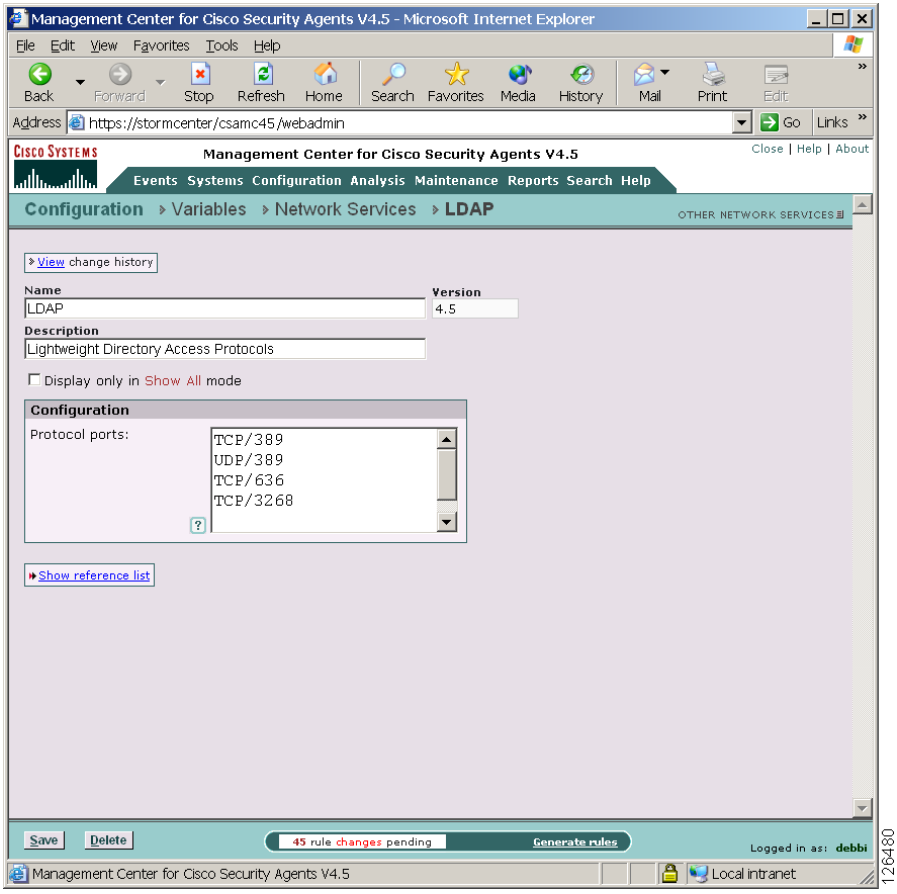
In some cases, an application may want to offer a temporary service port for callback data connections. An ephemeral port is a temporary system-assigned port for this purpose. You can specify an ephemeral port range for a Network service as follows (See Using the Correct Syntax, page 2-28 for more details):

```
TCP/ephemeral
UDP/ephemeral
```

**Step 6** When all required information is entered, click the **Save** button to save your event set in the CSA MC database.

You can now enter this network service name by clicking the **Insert Network Service** link in the network access control rule network services field.

*Figure 7-6 Network Services Configuration View*



# Registry Sets

A variety of viruses invoke themselves using registry settings. Use the preconfigured registry sets in registry access control rules to prevent viruses from writing to registry values popular with viruses.

This variable is not available for UNIX configurations.

**Caution** If you attempt to create your own registry sets to include in a rule, you should note that the ability to restrict registry access is an extremely powerful tool. Critical applications may not function as a result of a misconfigured registry restriction. Therefore, registry values should be as specific as possible. All rules restricting registry access should first be run in **Test Mode** to ensure that no unintended restrictions have been configured.

Registry sets are groupings of registry keys and settings under one common name. This name is then used in rules that allow or deny registry write operations. All the registry restriction parameters that exist under that name are then applied to the rule where the name is used.

To view preconfigured registry sets or to create a new registry set, do the following.

**Step 1** From the menu bar **Configuration** drop-down list, move the mouse over **Variables**. A cascading menu with further selections appears.

**Step 2** Select **Registry Sets** from the cascading menu. Any existing registry set configurations are shown.

**Step 3** To view an existing registry set, click the link for that item. Click the **New** button if you would like to create a new registry set variable. This takes you to the configuration view (see Figure 7-7).

**Step 4** Enter the following.

- **Name**—This is a unique name for this registry set.
- **Description**—This is a line of text that is displayed in the list view helping you to identify this particular registry set configuration.
- **Display only in Show All mode**—If your lists of variables are growing too long in rule or application configuration pages, clicking the Display only in Show All mode checkbox on a variable page causes that variable to no longer

appear in selection lists for that variable type. This feature works in conjunction with Admin Preference settings. You must go the Admin Preferences page to make the item reappear. See Administrator Preferences, page 2-6.

**Step 5** **Registry keys matching**—You *must* enter a value in this field if you are creating a registry set.
The registry key fields (matching and exclusions) must begin with a wildcard or specification of a registry hive. There must be at least one non-wildcarded component in a registry key.

Hives are one of the following strings:
HKLM—refers to the HKEY_LOCAL_MACHINE
HKCR—refers to HKEY_CLASSES_ROOT
HKCC—refers to HKEY_CURRENT_CONFIG
HKU—refers to HKEY_USERS (HKU* refers to all users)

***Table 7-1 Example valid and invalid registry key entries***

| | |
|---|---|
| `**\MSSQLSERVER\**` | This is a valid entry. |
| `**\M*\**` | This is invalid because there is no non-wildcard component. (M* is wildcarded.) |
| `HKLM\SOFTWARE\CSCOpx\**` | This is a valid entry. |
| `FOO\SOFTWARE\CSCOpx\**` | This is invalid (FOO is not a hive). |

**Note** Note that the wildcard syntax explained in Table 2-2 on page 2-30 also applies to registry sets. However, the asterisk is a valid single character in a registry key and should be represented with a single "?" wildcard.

**Step 6** **but not**—Make exceptions to registry keys.

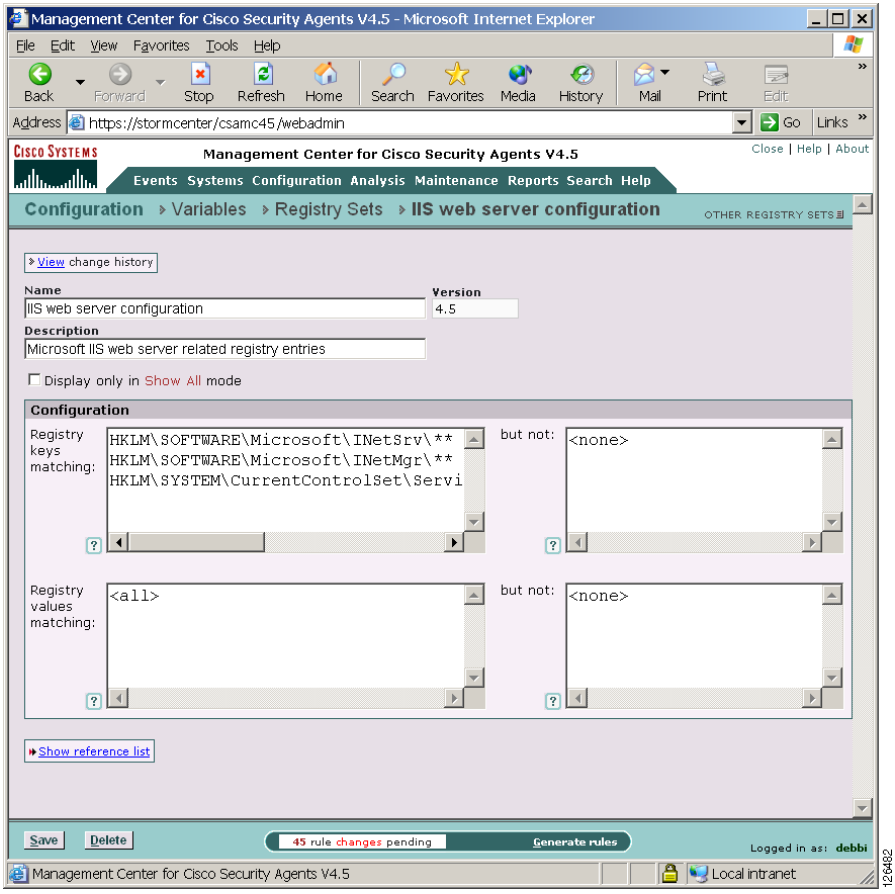
**Step 7** **Registry values matching**—Enter the registry values you are controlling access to.

**Step 8** **but not**—Make exceptions to registry values.

**Step 9** When all required information is entered, click the **Save** button to save your registry set in the CSA MC database.

You can enter this registry set name by clicking the **Insert Registry Set** link in the registry access control rule registry entries field.

***Figure 7-7 Registry Set Configuration View***




## Included Registry Sets

CSA MC ships with several pre-configured registry sets you can use in your registry access rules. Some are application specific, others are operating system specific. This section describes a sample of the included operating system specific registry keys.

- Run Keys are used to register programs so that the system will invoke them as a service. Viruses can make use of this key to become persistent.

  Protecting this registry value by creating a rule to prevent writing to run keys can prevent the type of virus described above from invoking and propagating itself.

**Note** It is important to note that if users have administrator privileges on their systems and are installing software, this type of rule may trigger and prevent that installation. In such cases, using a Query User rule would be most effective. This way, if users are installing software, they themselves can prevent the agent from stopping the installation by answering "Yes" to the query to allow the install. However, if users are not installing software, this type of Query User rule triggering on a system could be treated as a serious issue and the user should answer "No to all" to disallow the action.

- Shell commands are used to tell your system how to open a file based on the file format. This is how the system knows which application to use when opening a particular file.

  Viruses can exploit this by having the registry setting invoke the virus along with the application being opened. In this case, the application would open correctly and the virus could silently begin doing harm.

  BootExecute tells the system which executables should be run at system startup time.

- Reboot operations tell the system which operations should begin at system startup time. If programs have been uninstalled, the reboot operation also tells the system which files and services should be deleted on the next reboot and startup.

  Viruses can exploit this registry setting by marking particular files for copying, overwriting, or deleting on startup. For example, a virus may attempt to delete a system service that could possibly detect the virus itself. By deleting this service at startup, the virus can go undetected.

**Note** It is important to note that if users have administrator privileges on their systems and are uninstalling software, this type of rule may trigger and prevent the uninstall. In such cases, using a Query User rule would be most effective. This way, if users are uninstalling software, they themselves can prevent the agent

from stopping the uninstall by answering "Yes" to the query to allow the action. However, if users are not uninstalling software, this type of Query User rule triggering on a system could be treated as a serious issue and the user should answer "No to all" to disallow the action.

# Query Settings

From the Query Settings page, accessible from the **Configuration>Variables>Query Settings** menu, you configure the query text and the query buttons that appear in the pop-up box the end user will see when query rules are triggered.

**Note** For a Query setting, the response to the query is relevant to the question, not to the resource. For example, if a File access control rule queries the user for a response and that identical query is also configured for a Network access control rule, the user is not queried again when the Network access control rule triggers. The query response from the previous File access control rule is automatically taken.

To configure a query pop-up box for use with a query rule, do the following:

**Step 1** On the Query Settings list page, click the **New** button to create a new query. See Figure 7-8.

**Note** CSA MC ships with several preconfigured queries. You can use an existing one or create a new one.

**Step 2** Enter a unique **Name** for your query. Names are case insensitive, must start with an alphabetic character, can be up to 64 characters long and can include hyphens and underscores _ . Spaces are also allowed in names. Use a descriptive name that you can easily recognize in the rule selection box when you are selecting a specific query setting for a rule.

**Step 3** Enter a **Description** of your query.

**Step 4** **Display only in Show All mode**—If your lists of variables are growing too long in rule or application configuration pages, clicking the Display only in Show All mode checkbox on a variable page causes that variable to no longer appear in selection lists for that variable type. This feature works in conjunction with Admin Preference settings. You must go the Admin Preferences page to make the item reappear. See Administrator Preferences, page 2-6.

**Step 5** In the **Text used to query user** edit field, enter a description of the issue that likely triggered the query. This text field allows you to provide localized query text for agents using the corresponding language on their desktop. This is the same text that will appear in the query user pop-up box explaining what is occurring on the system to the user. Therefore, making this information descriptive of the system action that triggered the pop-up is important.

You can use specially designated tokens to represent the corresponding values presented to the end user who is responding to the query. See Using Query Tokens, page 7-28.

**Note** All Cisco Security Agent kits contain localized support for Spanish, French, German, Italian, Japanese, Korean, and Simplified Chinese language desktops. If you do not select a specific language, the default for query text is English. Click the **More languages** link to enter text to be displayed in a language other than English. This allows you to provide localized query text for agents using the corresponding language on their desktop. See Localized Language Version Support, page 7-29 for more details.

**Step 6** The Allowed query actions multi-select box lets you choose which radio buttons appear on the query pop-up box. For example, you may not want the user to have a “Terminate” option. Therefore, you would only select the Allow and Deny radio buttons to be displayed.

The user reads the information posted on the query and is given the choice to select one of the following possible choices and click Apply:

- **Allow** (Yes)—Allows the application access to the resource in question.
- **Deny** (No)—Denies the application access to the resource in question.
- **Terminate**—Denies the application access to the resource in question and also attempts to terminate the application process. (Some processes cannot be safely terminated, such as winlogon.)

**Step 7** Of the radio buttons you decided to display, you also choose one of those buttons to be the **Default action**. If the query is not answered by the user within 5 minutes or if the user is not logged in to the system, the default action is taken immediately.

**Step 8** You can also decide to display a **Don't ask again** checkbox so that the user's query response is remembered. If the user selects that checkbox when he/she responds to the query, and the same action is attempted on the same resource, the remembered response is automatically taken and the user is not queried again.

**Step 9** For added security, you can issue a **query challenge** on the query pop-up box. If the default answer is not selected by the user and the selected answer is weaker than the default, a challenge will appear. This ensures that the user sitting in front of the system is answering the query rather than a malicious remote user or program attempting to respond. To pass the challenge, the user enters the information displayed in a graphic on the pop-up box itself.

**Step 10** Click the **Save** button.

**Tip** When you phrase the question that will appear to users and select the radio button options to be displayed, make sure that the logic you use is in sync with the response the user should select. For example, you probably should not phrase a question in the following way: “Do you want to prevent this action from occurring?” In this case, if the response is “Yes”, this is counterintuitive to how queries should be used. The user is selecting Yes to indicate No. Instead, phrase the question as follows: “Select No to prevent this action from occurring.”

*Figure 7-8 Query Settings Configuration View*

## Using Query Tokens

When enter query text into the edit field, you can use the following tokens to represent the values presented to the end user who is responding to the query.

- @parent—The path of the parent process. Use in Application control rules only.
- @ActiveXname—The name of the ActiveX control being downloaded. Use in System API access control rules only.
- @appname—The path of the process triggering the action. Use in all access control rule types, except Application control rules.
- @child—The path of the process being invoked. Use in Application control rules only.

- @progid—The ProgID of the COM object. Use in COM component access control rules only.
- @clsid—The GUID of the COM object. Use in COM component access control rules only
- @dataname—The name of data being filtered. Use in Data access control rules only.
- @filename—The full file path of the file being accessed. Use in File access control rules only.
- @fileop—The type of file operation (file/directory, read/write). Use in File access control rules only.
- @funcname—The system API function being called. Use in System API access control rules only.
- @hostaddr—The remote address of a connection. Use in Network access control rules only.
- @localaddr—The local address of a connection. Use in Network access control rules only.
- @netop—The type of network operation (client/server). Use in Network access control rules only.
- @netservice—The service/destination port used by the remote connection end. Use in Network access control rules only.
- @regname—The registry entry being accessed. Use in Registry access control rules only.
- @targetapp—The path of the application being targeted for code injection or modification. Use in System API access control rules only.

# Localized Language Version Support

On systems running multiple locales, (for example, Multilingual User Interface installations or Terminal Services), queries are displayed in the supported language used for the Windows desktop on which the query is shown. Events appear in the Windows Event Log in the default systems language.

For example, on a Windows 2000 Multilingual User Interface (MUI) installation, if a user is running a Japanese language version desktop, queries will appear in Japanese. But the Windows Event Log on this system will store events formatted in US English because the system language on a Windows MUI system is English.

On a localized Japanese system, both the queries and the events appearing in the Windows Event Log appear in Japanese.

CHAPTER 8

# Event Logging and Alerts

## Overview

Events and messages logged by Cisco Security Agents can be viewed from CSA MC. You can also control the type of alert sent out based on the severity level of the logged event, the specific event, and the host that generated the alert. You can configure CSA MC to send email, issue SNMP traps, beep pagers, log to a text file, and execute custom programs.

**Note** Cisco Security Agent events are also stored in the NT event log on an agent system in a localized format.

This section contains the following topics.


- The Event Log, page 8-2
- Reading Event Details, page 8-6
- Reading Packet Details, page 8-6
- Event Monitor, page 8-7
- Event Log Management, page 8-8
- How Logging Works, page 8-12
- Verbose Logging, page 8-13
- Logging and Query User Rules, page 8-13
- About the Event Management Wizard, page 8-14

- Creating an Exception Rule, page 8-16
- Creating a Logging Exception Rule, page 8-22
- Perform a Behavior Analysis, page 8-25
- Event Sets, page 8-27
- Third Party Access to Events, page 8-32
- Configuring Alerts, page 8-34
- Generate an Alert Log File for Third Party Applications, page 8-41


# The Event Log

The Event Log view, available from the Events category in the menu bar, lets you view system events provided by registered agents according to designated time frames, event severity levels, and the system that generated the event.

The information displayed at the top of the Event Log page (controlled by the settings in the Change Filter window, see next section) tells you the following:

- Filter by eventset: This displays the name of the Event Set, if any, used to filter the event log view.

or Define a filter with the following parameters:

- Time range: This is the current time range set for the event log filter.
- Severity: This is the current minimum and maximum severity range set for the event log filter.
- Host: This displays which hosts have generated the events viewable in the event log (set as part of the filter).
- Rule Module: From the pulldown list, select a rule module to search for events generated by that module.
- Rule ID: Enter the ID number for a rule to search for events generated by that rule.
- Events per page: This is the current value set for the number of events displayed on each page of the event log (set as part of the filter).
- Filter text: Enter a text string here to either include or exclude in your event message search.

- Filter out duplicates: Use this radio button to pare down events and remove all duplicate events from the display.

## Start date and End date

To search events, click the **Change Filter** link to access a pop-up window from which you can enter search criteria such as Start and End Date time frames. You can refer to the following points for entering time frame information, but note that most reasonable time frames are recognized by CSA MC:

- You can select a preconfigured Event Set by which to filter the event log or
- You can specify a relative time using any of the following terms: tomorrow, yesterday, today, now, next, ago, year, month, week, day, hour, minute, and second.
- Enter a specific time using any of the follow time formats: hh:mm:ss. If no meridian (AM or PM) is specified, hh is interpreted on a 24 hour clock (0-23). Note that entering minutes and/or seconds is optional.
- Enter a specific month and day with optional year in the formats: mm/dd/yy, monthname dd , yy. Specifying the year is optional. The default year is the current year.

## Minimum and Maximum Severity Settings

From the Minimum and Maximum Severity pulldown list, select a severity level and click the View button to see all events within the designated severity levels that have been logged within the time frame you've specified. Select from the following.

- Informational
- Notice
- Warning
- Error
- Alert
- Critical
- Emergency

## Host

You can filter the Event Log by host systems. All is the default here. All events generated by systems registered with the server are displayed. You can enter a specific host name to search for that host. Click the **change** link beside the Host field for a host selection box.

## Events / page

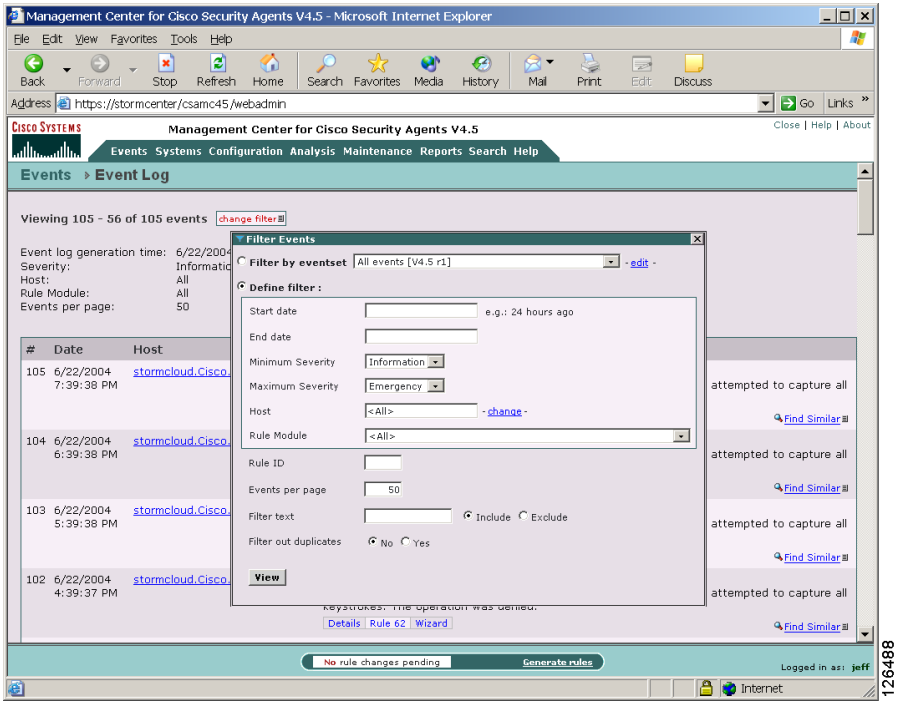
Enter the number of events per page you want to display up to a *maximum of 500 events* per page. The event log displays the most recent number of events based on the value you enter. You can page forward through links to view additional pages matching the query.

**Note** You can configure the CSA MC Event Log to display events from the agent system's NT Event Log. See NT Event Log, page 4-87.

## Filter out duplicates

You can select to filter out duplicate events. This will cause the event log to display only the most recent event for duplicated event entries.

*Figure 8-1 Event Log View*




The event log screen (see Figure 8-1) displays event messages within the time frame and severity level you specify and optionally by a specific host. These event messages explain the event that occurred and they provide a link to the rule that triggered the event. An event messages provides the time the event was recorded by the CSA MC, in its time zone and a link to the registered host view for the host that generated the event.

Some Event Log messages contain a **Details** link you can click to view more information about the event that generated the message. (The details contained here can be useful to customer support.) Read Reading Event Details, page 8-6, for more information. The Details link also provides packet information when appropriate. By installing Ethereal (http://www.ethereal.com) on the same server as the CSA MC is installed, you will be able to read the contents of a packet in a human-readable form rather than in hexadecimal notation. Read Reading Packet Details, page 8-6 for more information.

Log messages also contain a **Rule number** link. Clicking a Rule number link takes you to the rule that was triggered when the message in question logged.

Use the **Find Similar** link to locate messages similar to the one from which you accessed the Find Similar box. You can check parameters you wish to search by and select a time frame greater or less than the time the event in question was logged.

Use the **Wizard** link where available, to edit the rule that caused the event. See About the Event Management Wizard, page 8-14 for details.

# Reading Event Details

To view the details of an Event Log entry, follow this procedure:

**Step 1** Move the mouse over **Events** in the menu bar of CSA MC. Select **Event Log** from the drop-down list that appears. All events are displayed by default in the event log.

**Step 2** Click the Details link for the event about which you want more information. The details of the event are displayed in a separate page.

**Step 3** (Optional) If you want more information about an entry in the details, you can use the Google search engine to search the Internet. Do this in one of two ways:

- With your mouse, highlight the string of text, in the details page, about which you want more information. Then click the Google icon at the bottom of the details page. A new browser window opens with the results of the Google search.
- Drag the Google icon at the bottom of the details page over one of the fields in the details page. (Fields that are highlighted white can be searched by Google.) Let go of the mouse button. A new browser window opens with the results of the Google search.

# Reading Packet Details

CSA MC uses “Ethereal” software to translate packet information into a human-readable format. “Ethereal” is a third-party tool that analyzes protocols and works with WinPcap to analyze packets. Before you can view packet information in human-readable form, you must first install Ethereal on the same server that runs CSA MC.

To install Ethereal, follow the installation instructions at the http://www.ethereal.com site. Install the latest released version of Ethereal and the version of "WinPcap" recommended by Ethereal.

After you have installed Ethereal, you can read packet details by following this procedure:

**Step 1** Move the mouse over **Events** in the menu bar of CSA MC. Select **Event Log** from the drop-down list that appears. All events are displayed by default in the event log.

**Step 2** Click the **Details** link for the event about which you want more information. The details of the event are displayed in a separate page.

**Step 3** Scroll down to the **NetPacket** details row to read a description of the contents of the packet that triggered the event.

# Event Monitor

Similar to the Event Log, the Event Monitor, available from the Events category in the menu bar, lets you view system events provided by registered agents according to designated severity levels, and the host that generated the event. You can also enter the number of events to be displayed (default value is the last 50 events). Click the **Change** link to access a pop-up window from which you can edit these values and change the event filter. Refer back to The Event Log, page 8-2 for more information on these fields.

Unlike the Event Log page, the Event Monitor page automatically refreshes itself at set intervals. The event list is updated with the latest events each time the page refreshes.

The footer of this page provides a **Refresh** button and a **Pause** button. Use the Refresh button to refresh the page immediately without waiting for the set refresh interval to occur. Use the Pause button to immediately stop the page from refreshing. The set refresh interval will then stop at wherever it is in the countdown. This pause feature is useful when you are testing policies and you want to mark a certain place as a starting point for receiving new events. When you click it, the Pause button becomes a Resume button.

**Note** The administrator inactivity timeout value is still in effect when you leave the Event Monitor screen displayed on your system. The automatic page refresh does not constitute activity.

The Event Monitor will continue to refresh even after the timeout expires. However, you will not be able to navigate to any other page. This allows you to leave the Event Monitor on screen without worrying about anyone being able to access CSA MC after the session timeout.

# Event Log Management

The **Event Log Management** feature, available from the **Events** category in the menu bar, lets you create event database management tasks to manage the size of your event log. As your event log grows, specifying parameters for deleting events will help prevent this log from growing too large and from maintaining stale information.

**Note** You can configure global event insertion threshold parameters from the global **Event Insertion Tasks** page. This page already contains default settings for stopping the insertion of additional events for each event level when the specified threshold setting is reached. You can change these settings, if necessary. The thresholds on this page only trigger if the Event Log Management parameters you configure (described in the second section on this page) do not adequately keep events pruned below configured levels. For example, if there is a sudden flurry of events and configured pruning parameters do not trigger immediately, the global thresholds will kick in.

To access the global Event Insertion Tasks page:

**Step 1** Move the mouse over **Events** in the menu bar and select **Event Log Management** from the drop-down list that appears.

**Step 2** Click the top bracketed link **<Event Insertion Tasks>** to access the page. See Figure 8-3.

This page displays the total number of events in the Event Log. It also breaks events out to the number of events that exist for each severity level. Beneath this graphical event display are the default threshold settings for each event level. These thresholds represent the upper limit of events which must be reached for each severity level before no more events of this type will log. Event pruning must occur in order for these event types to once again be written to the Event Log.

To configure an event auto-pruning task, do the following. See Figure 8-2.

**Step 1** Move the mouse over **Events** in the menu bar and select **Event Log Management** from the drop-down list that appears.

**Step 2** Click the **New** button to create a new entry. This takes you to the auto-pruning configuration view.

**Step 3** Enter a **Name** for the auto-pruning task.

**Step 4** Enter a **Description**. This is a useful line of text that is displayed in the list view and helps you to identify this particular configuration.

**Step 5** Use the **Enabled** checkbox to enable this event auto-pruning configuration. (It is enabled by default.) By not selecting this checkbox, you can save this item, but it will not be active.

**Step 6** Enter a value in the **Delete Events - Older than** field. This is the value for which events, once having been in the log for this number of days, are deleted. Before these events are removed, they must also match the parameters of the event set selected on this page.

**Step 7** **And Matching the following Event Set**. Select the preconfigured event set for the event type you want to prune from the event log. Configuring event sets provides flexibility in selecting the events for auto-pruning.

**Step 8** Click the **Save** button.

**Note** This purging of events will occur periodically based upon the configured auto-pruning items. Generally, this pruning will take place at a time when the least activity is registered on the MC. When event auto-pruning occurs, a message appears in the event log notifying you of this action.

*Figure 8-2 Event Auto-Pruning*

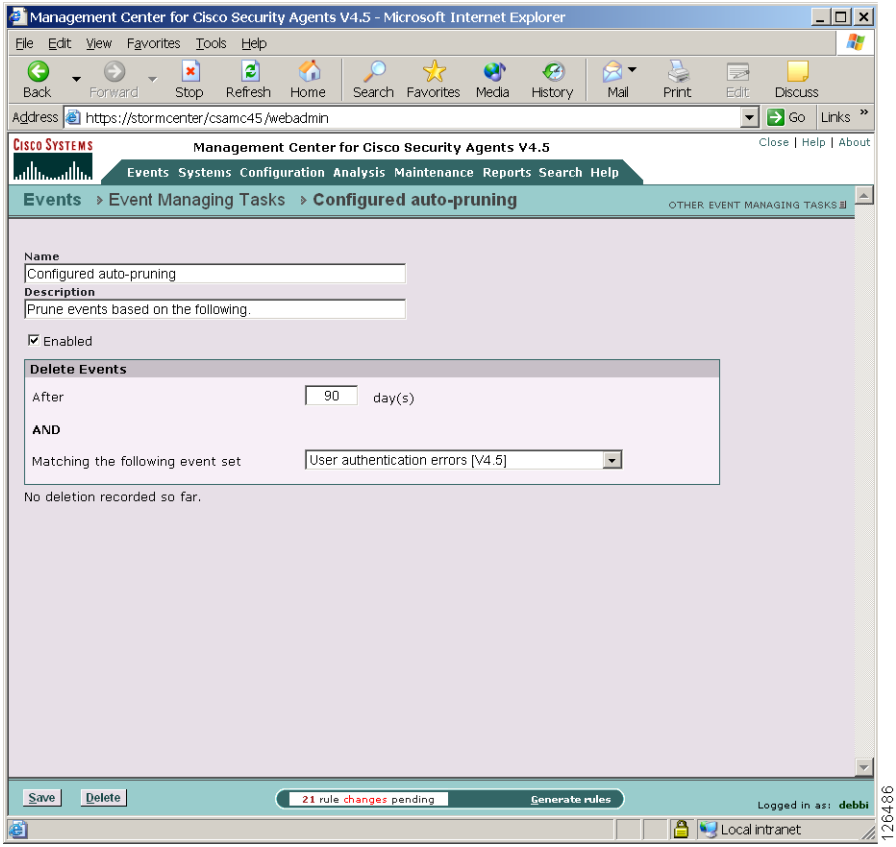
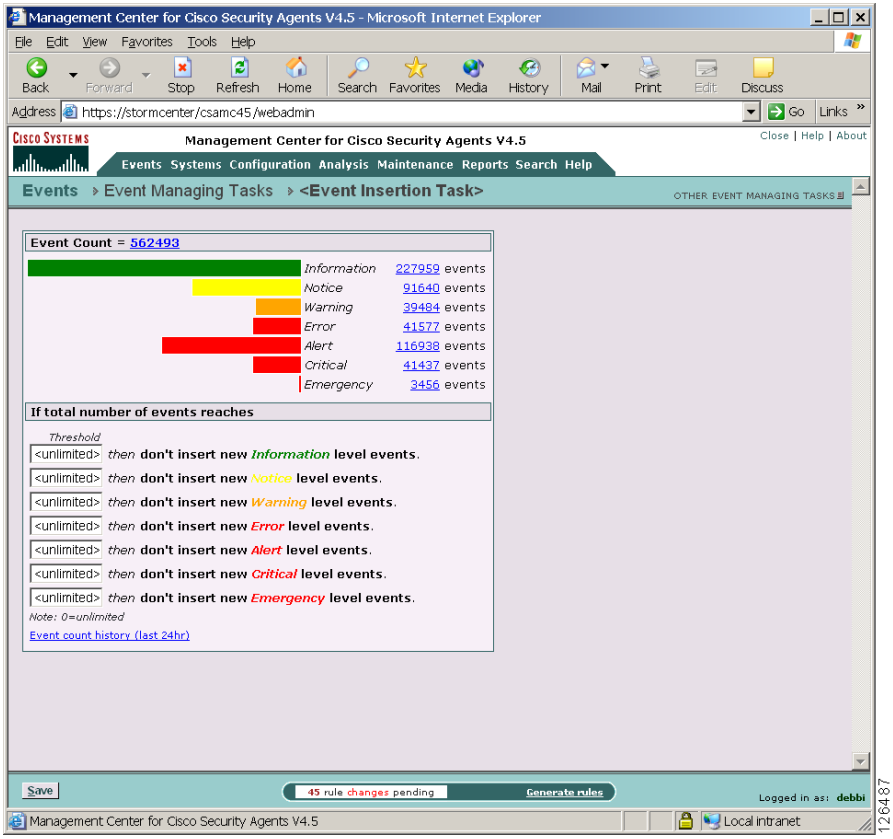


*Figure 8-3 Event Insertion Task*



# How Logging Works

The CSA MC Event Log does not contain every occurrence of an event from a system. Duplicate events are not logged for an hour after the first occurrence.

**Caution** In some cases, when an event is logging continuously, the agent will suppress this logging temporarily. Before it does this, a log message informing you of this suppression appears in the event log.

The following information is logged for each rule type.

- File access control logging—Process path and file names and file operation are logged.
- Network access control logging—Process path, network address, port and direction are logged.

**Note** No network access control rule denial events are logged for any TCP or UDP port resulting from multicast packet signals.

- Registry access control logging—Process path and registry key are logged.
- COM component access control logging—Process path and COM component PROGID/CLSID are logged.

A duplicate event is defined as follows:

- For file access controls, the name of the application and the file being accessed are the same.
- For network access controls, the name of the application, the remote address, and the network service port are the same.
- For registry access controls, the name of the application and the registry key name and value name are the same.
- For COM component access controls, the name of the application and the COM component PROGID or CLSID are the same.

# Verbose Logging

Enable Verbose Logging Mode in the Group configuration view to change the event log timer to log *all* recurring events rather than only logging recurring events once every hour. Verbose logging applies to all policies that are attached to the group that have logging turned on.

For normal operations, you would not want to enable Verbose logging. Verbose logging is useful for troubleshooting and for analyzing how applications work with rule sets, i.e. related processes and subprocesses. In the latter case, using Verbose logging with Test Mode can be very useful for monitoring how a rule set would work before deploying it.

**Note** Verbose logging is enabled on a host if any group in which the host is a member has Verbose logging turned on.

# Logging and Query User Rules

When a user responds to a Query User box (by pressing Yes, No, or Terminate), the agent remembers the response and caches it for an hour. This way, if the same rule is triggered again within that hour, the action is allowed or denied based on what the user answered previously, with no pop-up query box appearing again. When the user responds to a triggered Query User pop-up box, the system action that triggered the pop-up, as well as the user's response, are logged in the CSA MC event log. With Verbose logging turned on, all subsequent automatic allows or denies are logged as well. Otherwise, the one hour logging timer prevents agents from logging the automatic allowed or denied system action if it occurs again within the hour.

# About the Event Management Wizard

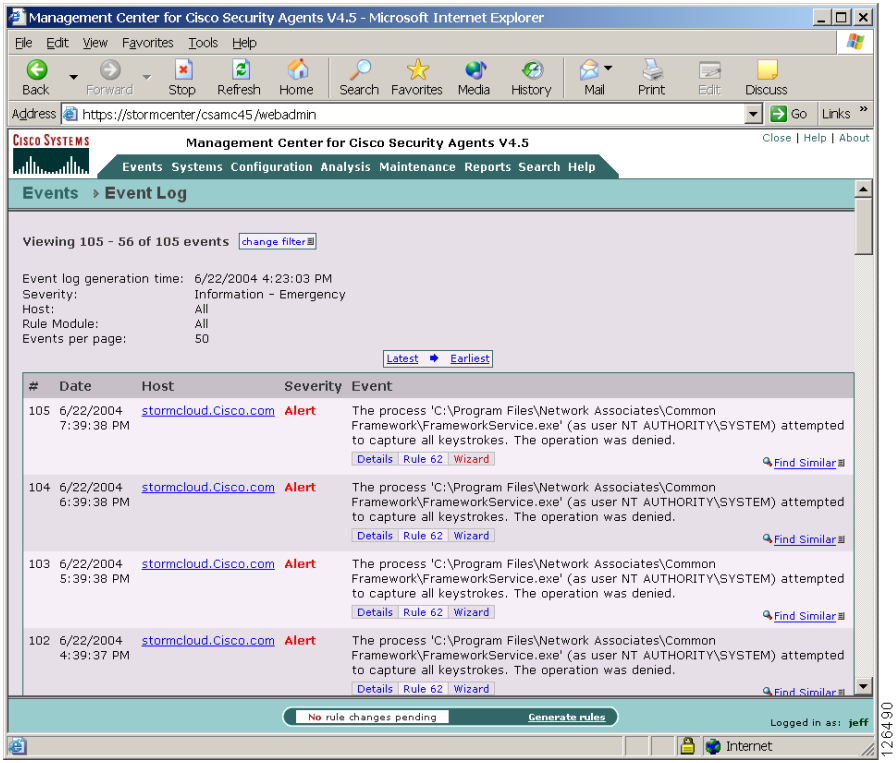
Use the Event Management Wizard to accomplish the following:

- To change the action of a rule that triggered a specific event. If an action is being denied on end user systems and you want to allow this action, you can automatically generate an "exception" allow rule which takes the application class and resource information in the event and creates an allow rule to counteract the rule that caused the deny.
- To create an exception rule that stops a specific event from logging. The Wizard makes use of the **Take precedence over other <action type> rules** feature to manipulate rule precedence and prevent logging of an event.
- To perform a Behavior Analysis Investigation for the application that caused the event. The Event Management Wizard is available for events triggered by Deny rules and Query User rules of the following types:

  (You launch the Wizard from a **Wizard** link which appears with certain event log messages of the following types.)

- Application control
- Buffer overflow
- COM component access control
- File access control
- Network access control
- Registry access control
- Rootkit/kernel protection
- System API control

*Figure 8-4 Event Management Wizard Link*



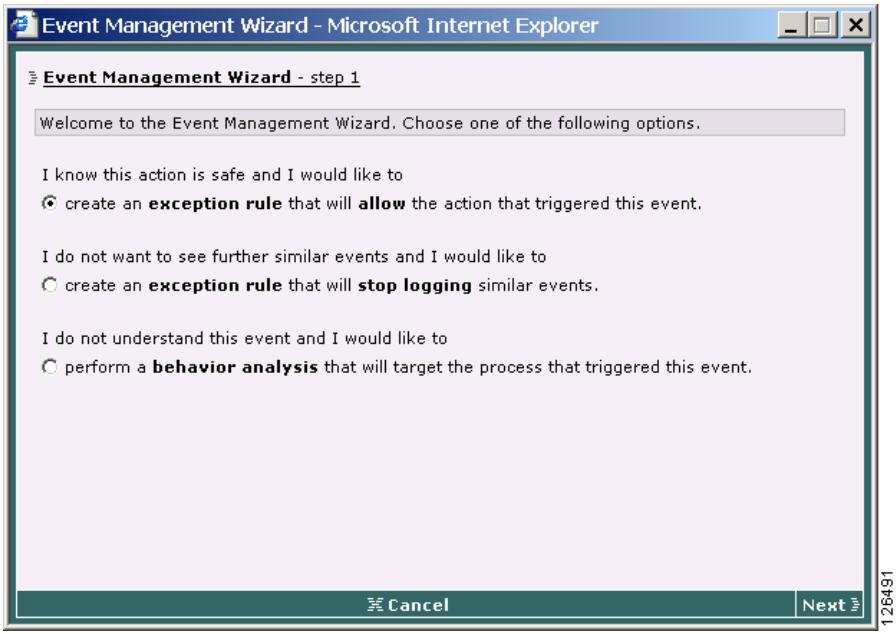
# Creating an Exception Rule

When you click the **Wizard** link from the Event Log page, you can choose to create an exception rule, an exception logging rule, or to configure a behavior analysis (see Figure 8-5). If you select to create an exception rule, when you click **Next** you are shown a summary of the rule that triggered the event. You click **Next** to continue to create the rule. The exception rule is an Allow rule that will be added to an existing rule module or to a new rule module and it will take precedence over the Deny or Query User rule that caused the event.

When the exception rule is added to a new rule module, the rule module is added to an exception policy for the group you specify. When the exception rule is added to an existing rule module, the existing rule module is already associated with one or more policies and those policies are already associated with certain groups.

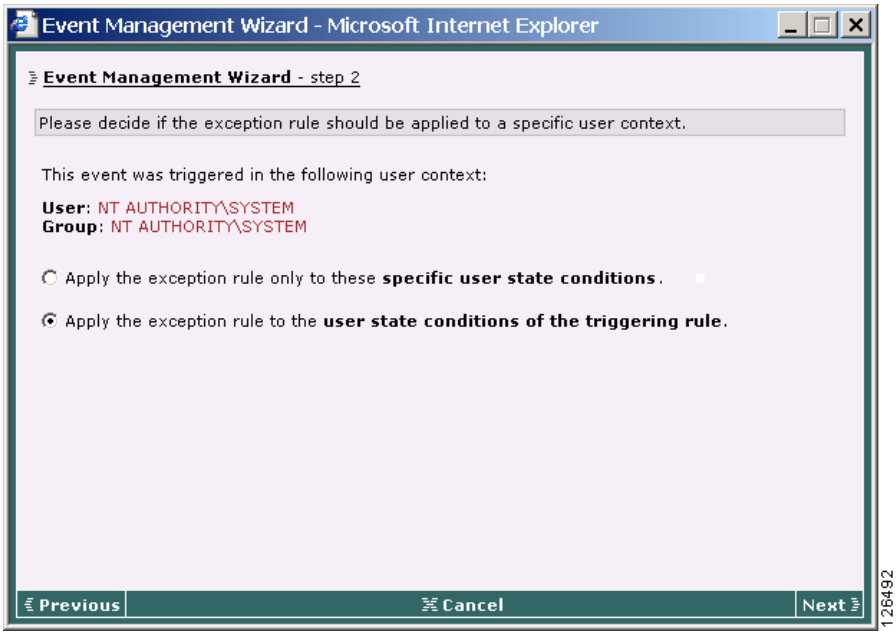
The wizard then takes you through a step by step procedure for affecting the changes you wish to make.

*Figure 8-5 Exception Wizard Step 1*



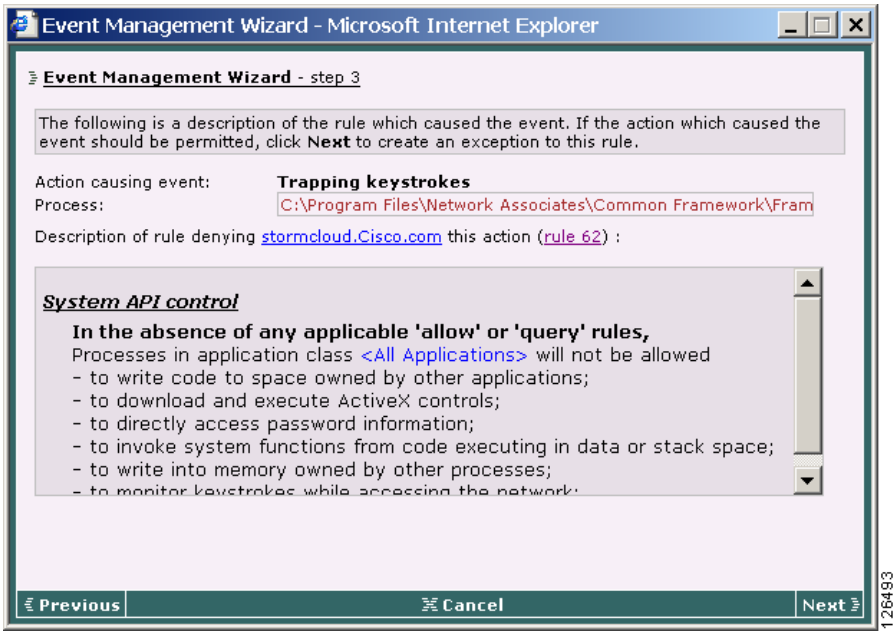

The next wizard page prompts you to optionally apply your changes to state conditions.

*Figure 8-6 Exception Wizard Step 2*




The third step provides a summary of the rule for which you are creating an exception.

*Figure 8-7 Exception Wizard Step 3*

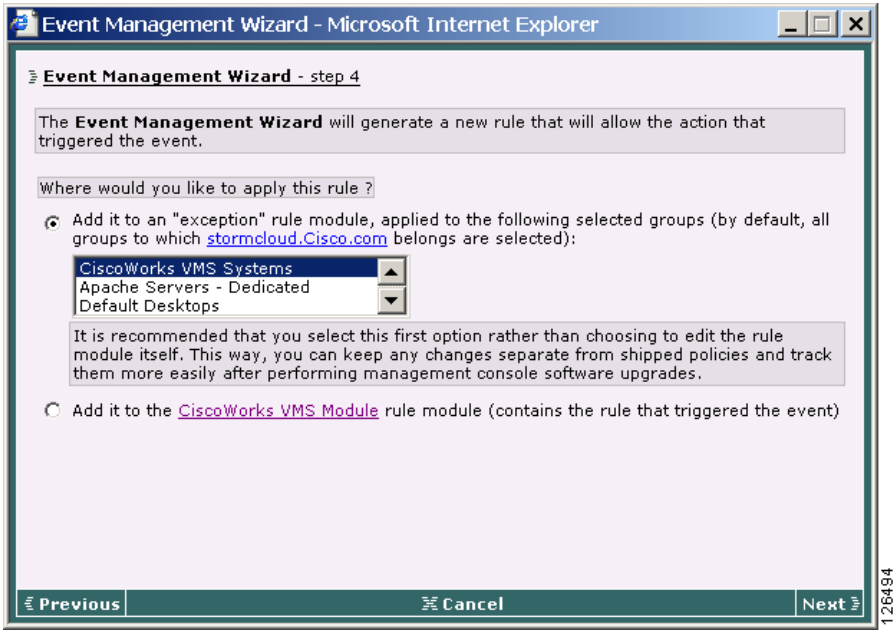


In the fourth step (see Figure 8-8), you are given two choices as to where you would like to apply this new rule. You can create a new rule module (an "exception rule module") which would contain the new exception rule. (This is the default and recommended choice.)

This new rule module would be attached to the exception policy for the group(s) containing the host from which the event was received. If you choose to create this exception policy, all subsequent exception rules you create through the wizard will be added to the same exception policy, if the group it is to be applied to is also the same. Therefore, a group could only have one exception policy, but contain any number of exception allow rules created through the wizard.

Your second choice is to add this new exception rule directly to the rule module which contains the rule that caused the event. This would be a change to the rule module itself. All policies that use this rule module and all groups that have this policy would receive the exception rule.

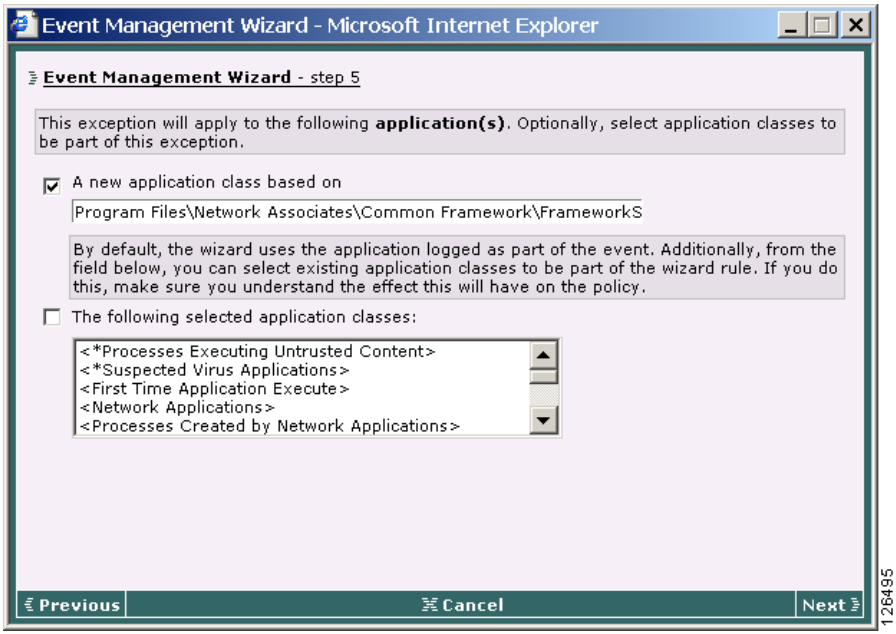
***Figure 8-8 Exception Wizard Step 4***



As you continue through the wizard, you can simply click **Next** and accept the defaults which create an allow rule for the exact application and resource named in the event. You can also select to include more groups to receive the exception and edit the process path of the application and/or include more application classes in the rule (see Figure 8-9).

When the wizard completes, it takes you to the new rule as it appears in CSA MC.

***Figure 8-9 Exception Wizard Step 5***



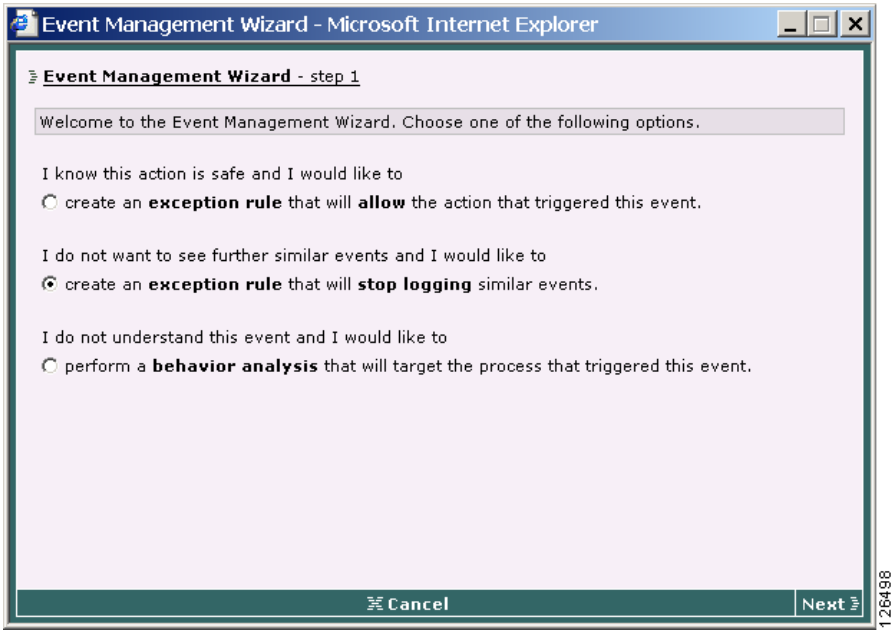
# Creating a Logging Exception Rule

The Wizard makes use of the **Take precedence over other <action type> rules** feature available in some rule types to manipulate rule precedence and prevent the logging of an event. The following rule types make use of precedence manipulation: File access control, Network access control, Registry access control, COM component access control, Application control, and System API control.

See Rules: Manipulating Precedence, page 4-13 for more information on the manipulating precedence feature.

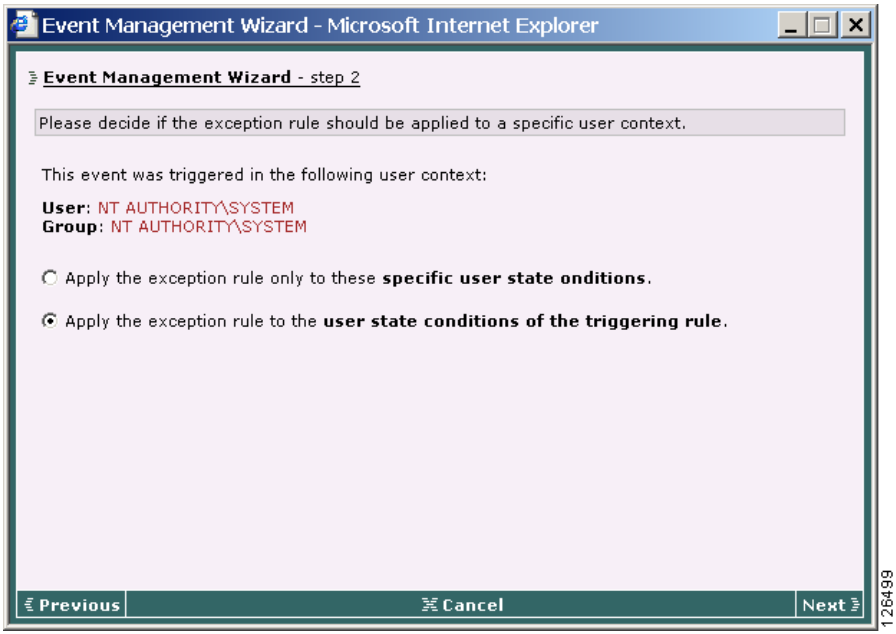
If you select to create an exception logging rule (see Figure 8-10), when you click **Next** you are shown a summary of the rule that triggered the event. You click **Next** to continue to create the exception logging rule.

***Figure 8-10 Exception Logging Wizard Step 1***



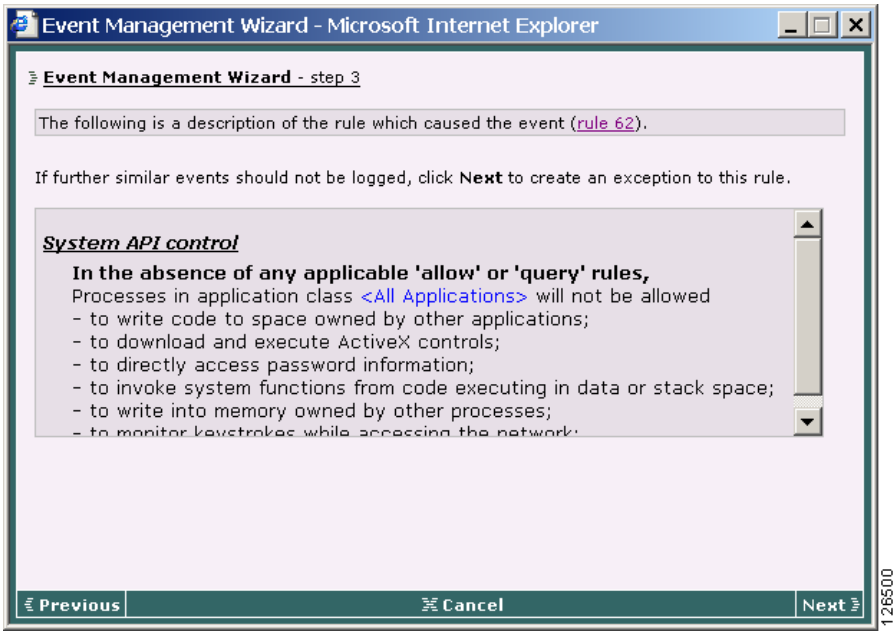

The next wizard page prompts you to optionally apply your changes to state conditions.

*Figure 8-11 Exception Logging Wizard Step 2*




The exception logging rule is a rule that is added to an existing policy or to a new policy. This rule is an exact copy of the rule that triggered the event. The one difference is that the rule created by the wizard has the **Take precedence over other <action type> rules** checkbox selected and the **Log** checkbox is unselected. This causes the rule created by the wizard to remain in effect, in the correct precedence within the policy, but not log an event when triggered.

*Figure 8-12 Exception Logging Wizard Step 3*



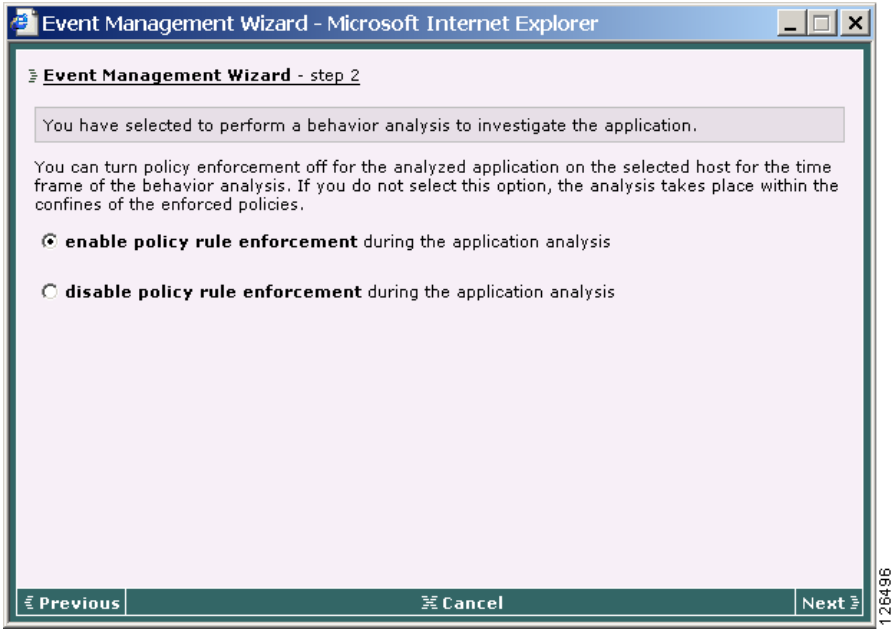
# Perform a Behavior Analysis

When you click the **Wizard** link from the Event Log page, you can choose to configure a behavior analysis to investigate the application that triggered the event (see Figure 8-5).

If you select to create a behavior analysis, optionally you can choose to **Disable policy rule enforcement** for the time frame of the analysis. Otherwise, the analysis takes place only within the confines of enforced policies. In that case, some events may be denied by rules during the analysis and therefore the analysis may not be complete.

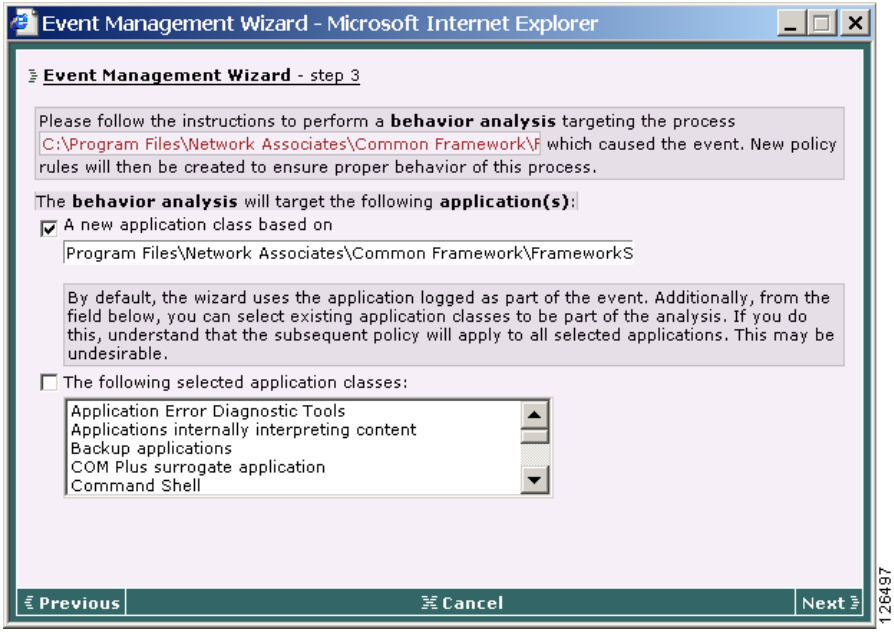
If you select the Disable policy rule enforcement radio button, when the logging agent receives an analysis, any policies relevant to the application being analyzed are disabled on the selected host until the behavior analysis is completed. You should understand that if the application being analyzed is untrusted or potentially a virus, you will allow it to run unimpeded during the analysis if you disable policy rule enforcement.

***Figure 8-13 Behavior Analysis Wizard Step 2***



If you decide that the application is not dangerous and it can run without any policy restrictions, you can begin to configure the behavior analysis.

***Figure 8-14 Behavior Analysis Wizard Step 3***




The next behavior analysis wizard page (see Figure 8-14) displays the application that triggered the event. This is the application the behavior analysis will investigate. Optionally, you can select other application classes to be analyzed. But in that case, the policy created would apply equally to all applications included in the analysis. For example, if the application class you are analyzing contains both Microsoft Word and Microsoft Outlook, the policy generated by the behavior analysis would be a combination of the resources required by both applications.

Continuing to click the **Next** button through the behavior analysis wizard configures the analysis with chosen defaults for analysis workstation and time frame. You can choose to edit these defaults or to accept them by making no changes.

When the wizard completes, it takes you to the new behavior analysis configuration page as it appears in CSA MC. You can edit it at this time or you can deploy the analysis by doing the following:

- **Generate rule programs** to distribute the behavior analysis to the host.
- Wait for the logging process to stop or click the **Stop logging** button to force the stop.
- Click the **Start analysis** button to start the analysis of the logged data.
- Optionally, use the **Import** button to import the policy, examine it and, if appropriate, deploy it to hosts.

# Event Sets

Configure event sets for use in alerts, reports, and event logs. When configuring alerts, event sets cause CSA MC to trigger alerts based on specified events. Once configured, these event set configurations become available in corresponding alert selection fields.

**Note** CSA MC ships with several preconfigured event sets you can use. If the included event sets do not suit your needs, use the instructions in the following pages to configure new event sets or to edit existing ones.

When creating your event sets, it's a good idea to adopt a naming convention that lets you quickly recognize event sets in your Alert configuration view.

**Note** To learn more about how event sets are used for generating reports, see Chapter 9, "Generating Reports".

To configure event sets, do the following.

**Step 1** Move the mouse over **Events** in the menu bar of CSA MC. Select **Event Sets** from the drop-down list that appears. All existing event set configurations are shown.

**Step 2** Click the **New** button to create a new event set. This takes you to the configuration view.

**Step 3** In the available edit fields, enter the following information (see Figure 8-15):

- **Name**—This is a unique name for this event set. Generally, it's a good idea to adopt a naming convention that lets you quickly recognize Event Sets in Alert configuration fields.
- **Description**—This is a line of text that is displayed in the list view and helps you to identify this particular Event Set configuration in the event set list view.

Under the **Event Specification** section, enter optional filtering parameters.

**Note** To select multiple items in a list box, hold down the Ctrl key as you select each item. To unselect a single item, hold down the Ctrl key when you click on the item in question. Press the Shift key to select multiple successive items.

**Step 4** Select **Filter by event** specifications.

Leave the Include all event types radio button selected to have events of all types included or select the Include only the following selected event types radio button. If you select the second radio button, then you must also select specific event log messages to filter by. These messages represent the spectrum of generated events that appear in the Event Log view.

**Step 5** Select **Filter by severity** specifications.

Leave the **Include all severity levels** radio button selected to have events of all severity levels included or select the **Include only the following selected severity levels** radio button. If you select the second radio button, then you must also select the severity level(s) that will trigger an alert for this event set. Available levels are: Information, Notice, Warning, Error, Alert, Critical, Emergency.

**Step 6** Select **Filter by group** specifications.

Leave the **Include all hosts** radio button selected to have events generated by all hosts included or select the **Include only hosts in the following selected groups** radio button. If you select the second radio button, then you must select the group(s) that trigger an alert for this event set. Any groups selected here that log the event in question will trigger an alert.

**Step 7** Select **Filter by rule module** specifications.

Leave the **Include all rule modules** radio button selected to have events generated by all rules modules included or select the **Include only rules in the following selected rule modules** radio button. If you select the second radio button, then you must select the rule module(s) that trigger an alert for this event set. Any rule modules selected here that log the event in question will trigger an alert.

**Step 8** Select **Filter by time** specifications.

**Note** If you do NOT have "Include all timestamps" selected, the Event Set is not available for use in Alerts.)

Leave the **Include all timestamps** radio button selected to have events generated at all times included or select the **Include only these timestamps** radio button. If you select the second radio button, then you can create a custom time here or select from available times, Today, Last 24 hours, Last 7 days, Last 30 days, and Events older than <you specify #> days to trigger an alert when an event occurs with the specified time range.

You can also enter **Custom start** and **Custom end** times in the following manner:

- Specify a relative time using any of the following terms: tomorrow, yesterday, today, now, last, this, next, ago, year, month, week, day, hour, minute, and second.
- Enter a specific time using any of the following time formats: hh:mm:ss. If no meridian (AM or PM) is specified, hh is interpreted on a 24 hour clock (0-23). Note that entering minutes and/or seconds is optional.
- Enter a specific month and day with optional year in the formats: mm/dd/yy, monthname dd, yy. The default year is the current year.

**Note** When you select multiple categories to filter by, all selections have to match.

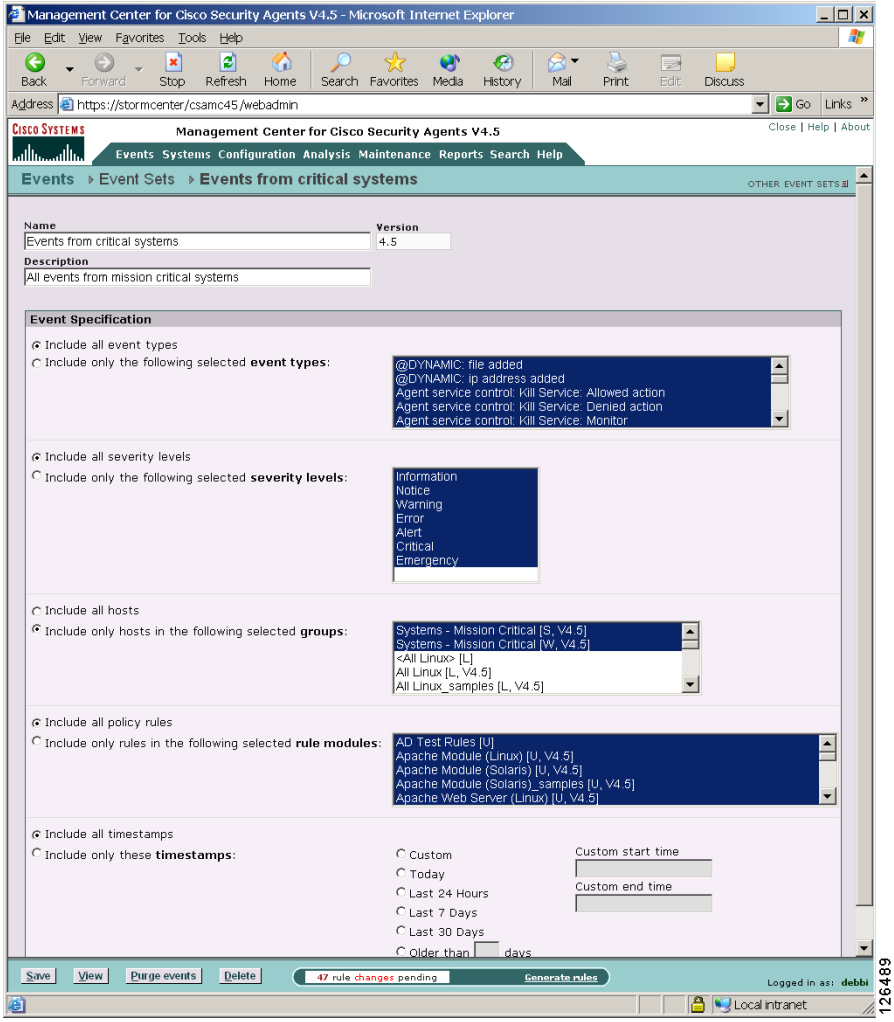
**Step 9** When all required information is entered, click the **Save** button to enter and save your event set in the CSA MC database.

In the Event Sets configuration page, the CSA MC frame at the bottom of the page provides a **View** button and a **Purge events** button.

- When you click the **View** button, all events that match the configured event set are displayed.

**Caution** When you click the **Purge events** button, all events that match the configured event set are deleted from the event log. If you make changes to an existing Event Set and click the Purge events button without saving those changes, all edits are saved and events are purged.

*Figure 8-15 Event Set Configuration View*



# Third Party Access to Events

To access events in the database for exporting to a different format (or for your own reports), connect to the database using ODBC DSN "csamc45dsn."

You can access events through the database view EventListView. (This is a SQL server view.) The columns defined in this view are as follows:

**Note** SNMP and Log file alert types can be used by third party event management applications. See page 8-37 for more details on those alert fields. (Note that the fields in the SNMP and Log file alerts are the same as those described in Table 8-1.)

***Table 8-1 EventList View Fields***

| Field | Description |
|---|---|
| EventId | An ID uniquely identifying the event. Increasing, in order of event arrival at CSA MC. |
| EventTime | The time at which the event occurred, using the clock of the host that generated the event. |
| HostId | An integer uniquely identifying the host that generated the event. This is NULL for events generated by CSA MC. |
| HostName | A non-unique string name for the host that generated the event. |
| HostOSType | The OS type for the host that generated the event, 'W' for Windows, 'U' for UNIX |
| CurrentHostIPAddress | The most recently recorded IP address for the host that generated the event. |
| SeverityCode | An integer, as follows in increasing severity -- Information (1), Notice (2), Warning (3), Error (4), Alert (5), Critical (6), Emergency (7) |
| SeverityName | The string representation of SeverityCode. |
| ProcessName | When applicable, the full path of the process that generated the event. |
| FileName | When applicable, the name (not path) of the relevant file from a file event. |
| SourceIPAddress | When applicable, the source IP address of a network event. |

| Field | Description |
|---|---|
| DestinationIPAddress | When applicable, the destination IP address of a network event. |
| RuleId | An integer uniquely identifying the rule that caused the event. |
| EventType | A string representing the type of the rule that caused the event, as discussed in Chapters 4 and 5. This field can be used as a broad-level categorization of CSA MC events. Possible values are as follows: File access control, Network access control, Network shield, Registry access control, System API control, Sniffer and protocol detection, File version control, COM component access control, Clipboard access control, Service restart, NT Event log, Application control, Agent service control, Agent UI control, Data access control, Connection rate limit, Analysis, Kernel protection, Network interface control, Rootkit / kernel protection, Buffer overflow, Syslog control, Resource access control, Downloaded content, Global virus scan, Global event log, Global network scan, Global email worm, Global IP address quarantine, Self-protection, Administrative. |
| RuleDescription | The user-specified string description for the rule that caused the event. |
| RuleModuleId | An integer uniquely identifying the rule module which contains the rule that caused the event. |
| RuleModuleName | The string name of the rule module which contains the rule that caused the event. |
| EventCode | An integer which uniquely defines the event code. |
| EventCodeTag | A short string representing the event code. |
| EventText | The complete formatted text of the event. (A Test Mode event is preceded by the string "TESTMODE".) |
| SourcePort | When applicable, the port used by the source of a network event. |
| DestinationPort | When applicable, the port used by the destination of a network event. |
| ButtonCode | The bottom 16 bits of this field represent the button that was pressed, with short integer values as follows, Yes (1), No (2), Terminate Process (3), OK (4). The upper 16 bits of this field represent whether the button was selected by default. A zero value indicates that the user actually pressed the button, while a non-zero value indicates that the default was chosen, e.g. because the query timed out. |

| Field | Description |
|---|---|
| Username | The name of the logged-in user at the time of the event. |
| RulePriority | The priority of the rule in question. |

# Configuring Alerts

You can configure CSA MC to send various types of alerts to specified recipients when a policy triggers an event. Available alert types include: Email, Pager, SNMP, Log to file, Named pipes and a Custom program that you provide.

Each alert type requires you to enter specific information. See Table 8-2 for details.

To configure CSA MC to issue alerts when specified system events occur, do the following.

**Step 1** Move the mouse over **Events** in the menu bar and select **Alerts** from the drop-down list that appears. The list of Alerts (if any) appears.

**Step 2** Click the **New** button to create a new alert. This takes you to the configuration view.

**Step 3** In the Alert configuration view (see Figure 8-16), enter a **Name** and a useful **Description**. This information is displayed in the list view and helps you to identify this particular alert.

**Step 4** From the **Send alerts for the following event set** list box, select the event set(s) you want to trigger the alert you're creating. Configuring Event Sets provides flexibility in selecting the events for which you want to be alerted.

**Note** The "time" filter in an event set is ignored for alerts. Alerts are generated as events are logged.

To select multiple items in a list box, hold down the **Ctrl** key as you select each item. To unselect a single item, hold down the Ctrl key when you click on the item in question. Press the **Shift** key to select multiple successive items.
If the available options here do not meet your needs, you can configure event set variables which become selectable in this field.

**Step 5** In the available alert configuration fields, enter data for *one or more* of the following alert types: Email, Pager, SNMP, Log, Named pipe, Custom (for alert configuration information, refer to Table 8-2).

For each alert type you want to send, select the corresponding **checkbox** and enter the required alert-specific information.

**Note** Although you can enter data into all available alert edit fields, if you do not check the corresponding checkbox, the alert in question is not enabled; however, the information you've entered is stored in the database. You can enable the alert type at a later time.

**Step 6** When your information is entered, click the **Save** button to save your new alert(s).

**Note** Use the **Clear Pending Alerts** button to clear all alerts that have been triggered by events but not yet sent. You might want to do this if several events are occurring simultaneously or continuously, you have already disabled the alert, and you have no further need for the continual notifications that are pending.

*Figure 8-16 Alert Configuration View*

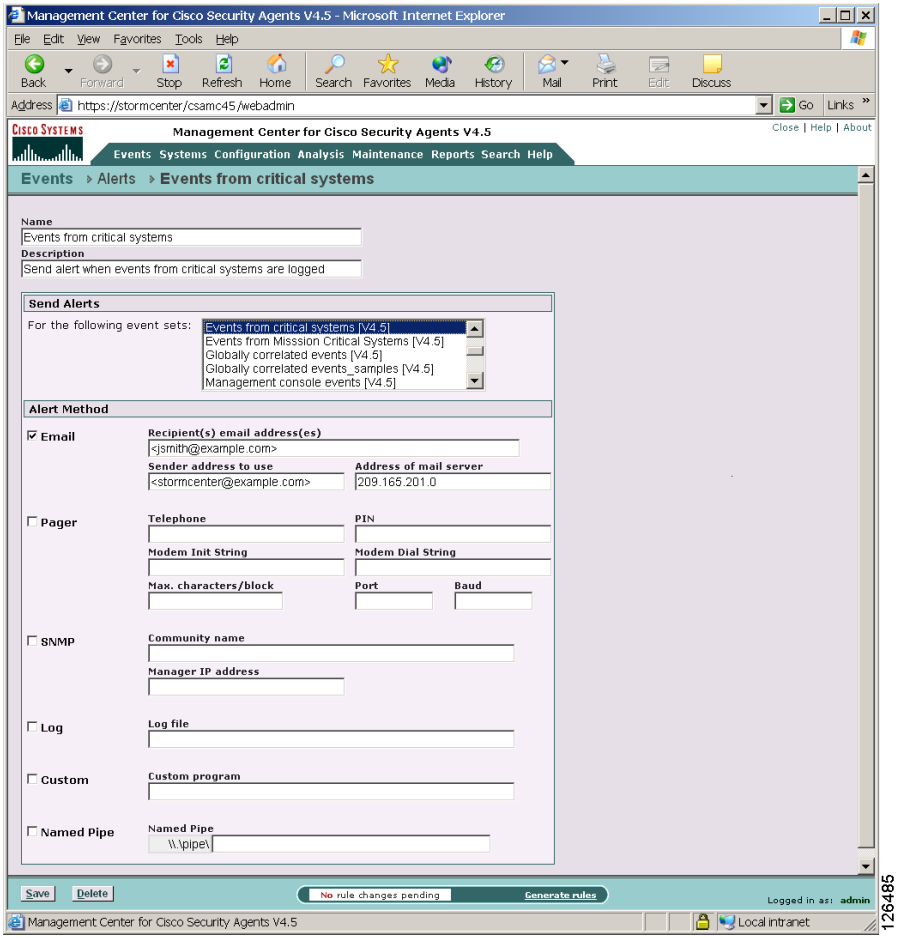


*Table 8-2 Alert Type Descriptions*

| Alert Type | Information | Description |
|---|---|---|
| Email | Recipient | Enter the email address of the mail recipient. Using brackets is optional. CSA MC will automatically enter them if you do not. You can enter multiple addresses separated by commas: `<dpaul@example.com>` |
| | Sender address to use | Enter the mail sender in brackets. Some mail servers require this to be specified: `<jsmith@example.com >` |
| | Address of SMTP server | Enter the IP address or DNS name of the SMTP server. |

| Alert Type | Information | Description |
|---|---|---|
| Pager | Telephone | Enter the recipient's pager number: `5550112`<br>Pager must support TAPI. Only alphanumeric pager services are supported. (Numeric pager services are not supported.) Refer to your paging service provider for further information.<br>(Note that if your company requires a number be dialed, such as 9, to access an outside line, you must enter that number here as part of the telephone number.) |
| | PIN number | PIN number: `10799`<br>(This is a string that identifies the pager. Obtain this from the service provider.) |
| | Modem Init String | Modem Init String: `ATQ0VI~`<br>(You must check your modem instruction manual to locate this value. In some cases, it can be left blank. Not all modems require this value or a modem dial string.) |
| | Max. characters/block | Max. characters/block: `80`<br>(Some paging services only allow a certain number of characters in a single message block. Check with your paging service. You can leave this field blank to use a default value of 80.) |
| | Modem Dial String | Modem Dial String: `TO=20,ATDT`<br>(See comment above.) |
| | Port | Port: `COM1`<br>(This is the serial port the modem is attached to.) |
| | Baud | Baud rate: `2400`<br>(This is the baud rate supported by the paging service. If you leave this field blank, CSA MC enters a default value of 2400 when you save the alert.) |

| Alert Type | Information | Description |
|---|---|---|
| SNMP | Community Name | Enter the community name. This is a text string agreed upon by the SNMP manager: `public` |
| | Manager IP Address | Enter IP address of the system where the SNMP trap should be sent. Optionally, you can put a colon and a port number (":<port number>) after the IP address if you are using a non-standard port. (Standard port is 162.)<br>Refer to the CSAMC-SNMPv2.mib document in the `CSCOpx\CSAMC45\doc` directory for SNMP-MIB definitions for Cisco specific objects.<br>Also see Third Party Access to Events, page 8-32 for third party event management details. |
| Log | Log file name (using full path) | Enter a name for the flat logging file that events will be written to.<br>c:\alerts\logfile.txt<br>This file can then be used by third party event management applications. See Third Party Access to Events, page 8-32 for details.<br>*In a distributed configuration, the path must correspond to the polling server system. |

| Alert Type | Information | Description |
|---|---|---|
| Custom | Custom Program | Enter a custom alert program name here.<br><br>The server calls the program as it appears in this field. You must enter the full pathname so that CSA MC can locate the program.<br><br>Your custom program must be an executable file. `c:\Program Files\CSCOpx\CSAMC45\program.exe`<br><br>The program passes the event message in a file whose name is passed to the program as its first parameter. Alternately, the program can also read the event message from its standard input. The file containing the event is automatically deleted when the program exits or closes its standard input.<br><br>FEATURE NOTES:<br><br>* The custom program must exist on the same system as CSA MC in the CSCOpx directory or subdirectory. If it is located elsewhere, the VMS policy will not allow it to run.<br><br>*Custom programs cannot require any user input.<br><br>*If a custom program is triggered and fails for some reason, it could take several minutes before the program closes itself and attempts to launch again. (If you are testing custom program alerts, one way to tell if the program has launched and is running, is to watch for it in the Task Manager.)<br><br>*In a distributed configuration, the path must correspond to the polling server system. |
| Named Pipe | Named Pipe | A named pipe is a form of internal communication. This alert type allows the integration of third party software for the purpose of receiving alerts over Windows named pipes. Consult your third party documentation for further configuration details.<br><br>Note that this feature is for use with third party vendors that support alerts over Windows named pipes. |

# Generate an Alert Log File for Third Party Applications

Using the **Log** checkbox and the **Log file** edit field in the Alerts configuration page (see Figure 8-16), you can have CSA MC generate a flat logging file to which events are written. Third party event management applications can then parse the information found in this file.

To generate this file, select the Log checkbox and enter the Log file name, using the full path that you want to write event data to. For example, enter `c:\alerts\logfile.txt`

Event data is written to this file as follows:

```
EventId,EventTime,HostId,HostName,
CurrentHostIPAddress,HostOSType,Severity,EventType,
EventText,EventCodeTag,FileName,ProcessName,
SourceIPAddress,DestinationIPAddress,SourcePort,
DestinationPort,RuleId,RuleDescription,RulePriority,
RuleModuleId,RuleModuleName,ButtonCode,UserName
```

Entry fields are separated by a delimiter of a comma. Event entries themselves are separated by a carriage return/line feed (ASCII Hex 0D 0A).

Once a log file exceeds 1 MB, it is closed and its name is suffixed with a time stamp. A new file, using the same file name entered in the CSA MC Alerts Log file field, is then created. Events continue to be written to this new file until it reaches 1 MB.

**Note** This file data is encoded in UTF-8 format.

CHAPTER 9

# Generating Reports

## Overview

You can configure the Cisco Security Agent to log an event each time a system action triggers a rule.

You can use the event logging data received from agents to generate reports that indicate overall network health. Using these reports, you can monitor how your current rule sets are working and adjust them, if necessary.

You can also generate reports related to configuration information.

This section contains the following topics.


- Types of Reports, page 9-2
- Viewing Reports, page 9-2
- Generating Reports, page 9-3
- Events by Severity, page 9-3
- Events by Group, page 9-5
- Host Detail, page 9-6
- Policy Detail, page 9-8
- Group Detail, page 9-9
- About the ActiveX Crystal Report Viewer, page 9-10

# Types of Reports

CSA MC lets you generate reports using various criteria. For example, you can create reports based on event severity level, on the group that generated the event, and on the individual host systems producing events. You can sort by other parameters such as time frame, host, and event code that you configure separately.

# Viewing Reports

When you generate your reports, you're given the option of selecting the type of viewer through which to display the report. From the Viewer type pulldown menu, you can select the following.

- ActiveX: The report viewer for ActiveX uses an ActiveX control that can be placed inside an HTML page and viewed through any browser that supports ActiveX. (Supported by Internet Explorer 3.02 and higher. Not supported by Netscape.) See About the ActiveX Crystal Report Viewer, page 9-10 for more information.
- HTML Frame: This view is selected by default if you do not select a viewer type. Using this viewer, you can display reports in HTML using frames to illustrate category data in a left frame. (Supported by Internet Explorer 3.02 and higher and Netscape Navigator 4.7 and higher.)

When you print reports, the formatting will vary depending on which view type you have selected and the printer settings on the printer you're using.

# Generating Reports

You generate reports by selecting various sorting options in the CSA MC report configuration views. When you are finished selecting sorting parameters, you can generate your report. The report opens in a new browser window.

## Events by Severity

You can generate reports using various selection and sorting criteria. In this case, you are creating a report based on event severity levels.

To generate an Events by Severity report, do the following.

**Step 1** Move the mouse over **Reports** in the menu bar of CSA MC. Select **Events by Severity** from the drop-down list that appears. Any existing reports are shown.

**Step 2** Click the **New** button to create a new report. This takes you to the configuration view.

**Step 3** In the Events by Severity report configuration view, enter a **Name** and a **Description** for the report.

**Step 4** From the pulldown list, select an **Event Filter**. This is an Event Set you create from the Events> Event Sets configuration view (see Event Sets, page 8-27).

**Step 5** From the **Sort by** pulldown list, select a parameter for sorting this report's contents (see Figure 9-1).

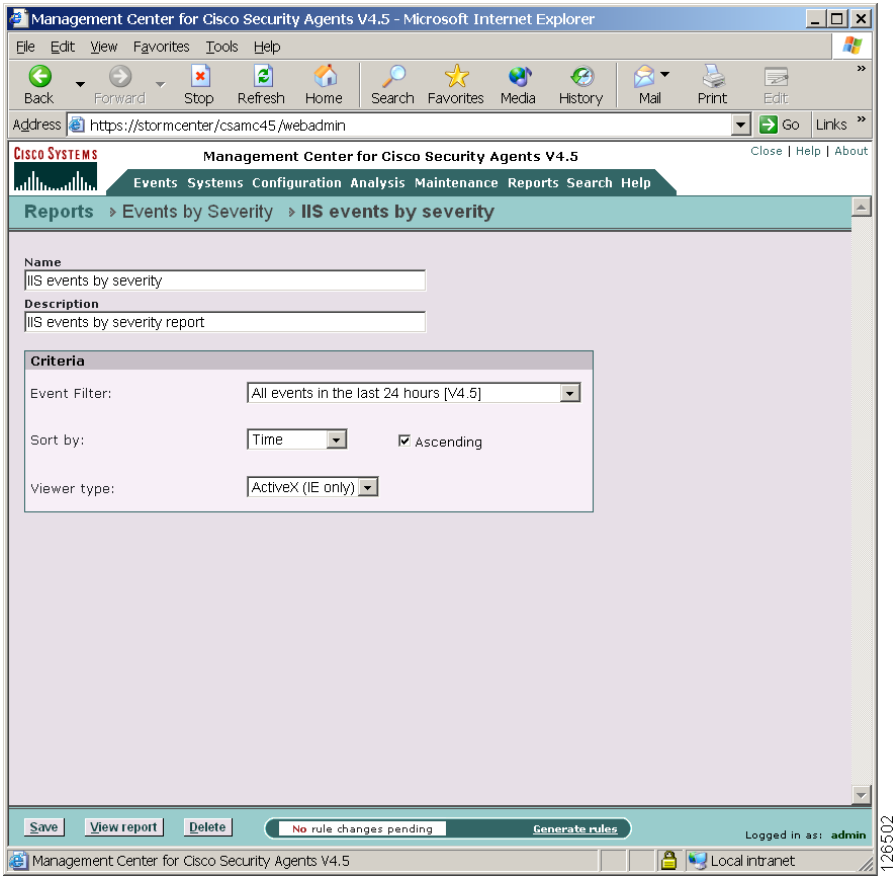
**Step 6** Enable or Disable the **Ascending** checkbox depending on the order in which you want to view your reports.

**Step 7** Select a **Viewer type**. By default, ActiveX is selected. This is the recommended viewer. For more information, see Viewing Reports, page 9-2.

**Step 8** Click the **Save** button to save the parameters you've just configured for generating this report.

**Step 9** Click the **View Report** button and the report is automatically displayed in a new browser window.

*Figure 9-1 Events by Severity Report Configuration*



# Events by Group

You can generate reports using various selection and sorting criteria. In this case, you are creating a report based on the groups that have generated the events.

To generate an Events by Group report, do the following.

**Step 1** Move the mouse over **Reports** in the menu bar of CSA MC. Select **Events by Group** from the drop-down list that appears. Any existing reports are shown.

**Step 2** Click the **New** button to create a new report. This takes you to the configuration view.

**Step 3** In the Events by Group report configuration view, enter a **Name** and a **Description** for the report.

**Step 4** From the pulldown list, select an **Event Filter**. This is an Event Set you create from the Events> Event Sets configuration view (see Event Sets, page 8-27).

**Step 5** From the **Sort by** pulldown list, select a parameter for sorting this report's contents.

**Step 6** Enable or Disable the **Ascending** checkbox depending on the order in which you want to view your reports.

**Step 7** Select a **Viewer type**. By default, ActiveX is selected. This is the recommended viewer. For more information, see Viewing Reports, page 9-2.

**Step 8** Click the **Save** button to save the parameters you've just configured for generating this report.

**Step 9** Click the **View Report** button and the report is automatically displayed in a new browser window.

# Host Detail

You can generate reports based on hosts in specific groups you select as part of the report. A host detail report provides in-depth information on the hosts in the groups you select for the report.

To generate a host detail report, do the following.

**Step 1** Move the mouse over **Reports** in the menu bar of CSA MC. Select **Host Detail** from the drop-down list that appears. Any existing reports are shown.

**Step 2** Click the **New** button to create a new report. This takes you to the configuration view.

**Step 3** In the Host Detail report configuration view (see Figure 9-2), enter a **Name** and a **Description** for the report.

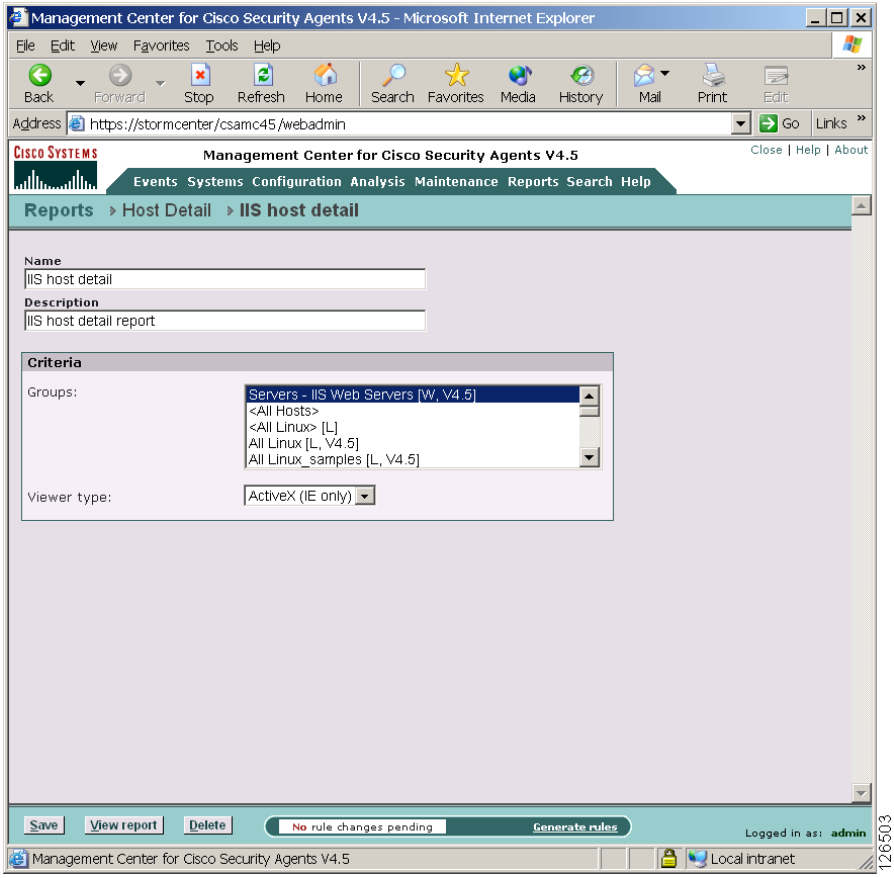
**Step 4** Select the **Groups** for which you want to generate a report. To select multiple items in a list box, hold down the **Ctrl** key as you select each item. To unselect a single item, hold down the Ctrl key when you click on the item in question. Press the **Shift** key to select multiple successive items. You can also select All Hosts here to generate a report for all registered hosts.

**Step 5** By default, ActiveX is selected as the **Viewer type**. This is the recommended viewer. For more information, see Viewing Reports, page 9-2.

**Step 6** Click the **Save** button to save the parameters you've just configured for generating this report.

**Step 7** Click the **View Report** button and the report is automatically displayed in a new browser window.

*Figure 9-2 Host Detail Report Configuration*



# Policy Detail

You can generate reports by selected policies. A policy report provides in-depth information on the policies you select for the report.

To generate a policy detail report, do the following.

**Step 1** Move the mouse over **Reports** in the menu bar and select **Policy Detail** from the drop-down list that appears.

**Step 2** Click the **New** button to create a new report. This takes you to the configuration view.

**Step 3** In the Policy Detail report configuration view, enter a **Name** and a **Description** for the report.

**Step 4** Select the **Policies** for which you want to generate a report. To select multiple items in a list box, hold down the **Ctrl** key as you select each item. To unselect a single item, hold down the Ctrl key when you click on the item in question. Press and hold the **Shift** key to select multiple successive items.

**Step 5** By default, ActiveX is selected as the **Viewer type**. This is the recommended viewer. For more information, see Viewing Reports, page 9-2.

**Step 6** Click the **Save** button to save the parameters you've just configured for generating this report.

**Step 7** Click the **View Report** button. Your report is created and is automatically displayed in a new browser window.

# Group Detail

You can generate reports by a selected group or groups. A group report provides in-depth information on the groups you select for the report.

To generate a group detail report, do the following.

**Step 1** Move the mouse over **Reports** in the menu bar and select **Group Detail** from the drop-down list that appears.

**Step 2** Click the **New** button to create a new report. This takes you to the configuration view.

**Step 3** In the Group Detail report configuration view, enter a **Name** and a **Description** for the report.

**Step 4** Select the **Groups** for which you want to generate a report. To select multiple items in a list box, hold down the **Ctrl** key as you select each item. To unselect a single item, hold down the Ctrl key when you click on the item in question. Press and hold the **Shift** key to select multiple successive items.

**Step 5** By default, ActiveX is selected as the **Viewer type**. This is the recommended viewer. For more information, see Viewing Reports, page 9-2.

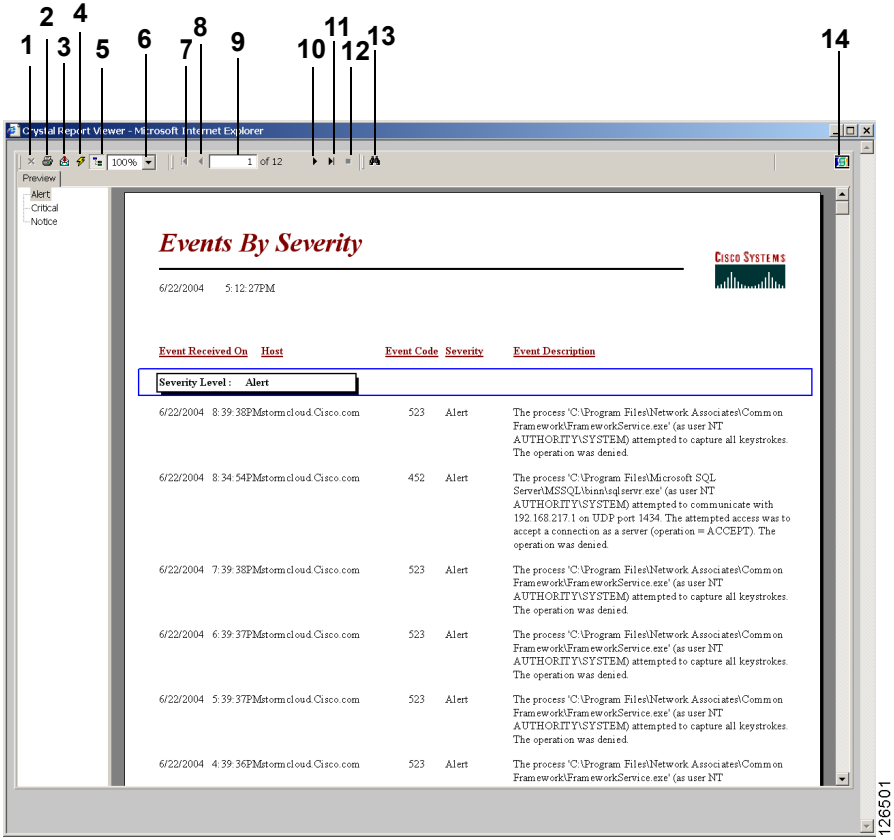
**Step 6** Click the **Save** button to save the parameters you've just configured for generating this report.

**Step 7** Click the **View Report** button. Your report is created and is automatically displayed in a new browser window.

# About the ActiveX Crystal Report Viewer

The report viewer for Active X reports contains elements that allow you to print, export, and search reports.

***Figure 9-3 Crystal Report Viewer***




Descriptions of the viewer button controls are as follows:

1. Close current view: This X button is generally grayed out unless a drill down item has been viewed. When active, this button allows you to close the drill down preview.

2. Print: This button allows you to print the report. When you click the button, a print setup window appears. From there, you can change the page setup of the report and select the print range.
3. Export report: The envelope button with the red arrow line allows you to export reports. This export utility lets you export reports to four file format choices (providing the applications for those formats are installed on the client system).

   To export a report, click the Export button and the "Crystal Smart Viewer Export" window appears. Select where you want to save the exported file to from the **Save in** field pulldown arrow. Then enter a name for the exported file in the **File name** field. From the **Save as type** pulldown field, select the format to save the report as. The choices are: Crystal Report, Rich Text Format, Word Document, and Excel Document.

   When you've made your format selection, click the **Save** button. A progress box lets you know the report is being exported.
4. Refresh: The refresh button is the one with the lightning bolt on it. When you click this button, a message is sent to the server to repopulate the report with fresh data.
5. Toggle group tree: The toggle group tree (navigation button) appears as a miniature directory tree. Clicking this button causes the left pane of the viewer to appear or disappear.
6. Zoom control: This control lets you set the magnification control of the viewer. You can select levels from the pulldown menu or you can enter your own numbers here.
7. Go to first page: Clicking the "Go to first page" control arrow takes you to the first page of the report. (When you are on the first page, this arrow is grayed out.)
8. Go to previous page: Clicking the "Go to previous page" control arrow takes you to the page of the report that is directly before the page you are currently viewing.
9. Current page out of total pages viewed: The number that appears in this field is the number of the page that is currently displayed. If your report has several pages, this number is followed by the word "of" and another number indicating the total number of pages in the report. This field can also function as a "go to" control. Entering a number in this field and pressing the Enter key takes you to that page in the report.

10. Go to next page: This right facing arrow button, when clicked, takes the viewer to the page immediately following the current page being viewed.
11. Go to last page: This right facing arrow button touching a vertical line, when clicked, takes the viewer to the last page of the report.
12. Stop loading: This button is generally grayed out. It contains a solid square in the middle and is only active when a report is loading. Clicking this button stops the report from loading in the window but it does not stop the report from continuing to be processed on the CSA MC system.
13. Search text: Clicking this button (with binoculars on it) allows you to search for any specific text, number, or character in the report. After entering the information you're searching for and clicking the "Find next" button, any matching items in the report are enclosed in a red-lined box.
14. Logo box: This box in the upper right corner of the viewer contains the viewer logo. This logo appears as a graphical rotating image when the viewer is busy loading.

CHAPTER 10

# Using Management Center for Cisco Security Agents Utilities

## Overview

The Management Center for Cisco Security Agents provides various utilities for advanced product maintenance tasks that extend beyond the administrator configuration and policy generation tasks done through the CSA MC user interface. Those utilities are documented here.

This section contains the following topics.


- Start and Stop Server Service, page 10-2
- Start and Stop Agent Service, page 10-2
- Backing Up Configurations, page 10-3
- Restoring Backup Configurations, page 10-6
- Database Maintenance (Free Up Disk Space on CSA MC ), page 10-8
- Using the COM Extract Utility, page 10-9
- Manual Agent Data Filter Installation, page 10-10
- Exporting and Importing Configurations, page 10-14
- View Import History, page 10-19
- Cisco Security Agent Posture Plug-in for CTA, page 10-20

# Start and Stop Server Service

As needed, you can start stop the Management Center for Cisco Security Agents service on a host by running the following commands from a command prompt window on the server host system:

```
net stop csamc45
net start csamc45
```

# Start and Stop Agent Service

As needed, you can start and stop the Cisco Security Agent service on a Windows host by running the following commands from a command prompt window on the agent host system:

```
net stop "Cisco Security Agent"
net start "Cisco Security Agent"
```

As needed, you can start and stop the Cisco Security Agent service on a UNIX host by running the following commands from a command prompt window on the agent host system:

```
/etc/init.d/ciscosec stop
/etc/init.d/ciscosec start
```

**Note** Running this stop command to stop the agent service on a system disables all rules on that system. Running a start csa command starts the agent service and reinstates all rules.

The shipped UNIX rule module, "Secure Management Module," allows secured management applications to stop the agent service. For example, after having logged in by selecting Command Line Login from the login screen in the options menu, you can issue the command `/etc/init.d/ciscosec stop`. Refer to the policy in CSA MC to see how these secured management applications are already defined and may be modified using application builder rules.

**Note** The UNIX agent has a utility (csactl) to provide capabilities that the Windows agent provides in its user interface. See Appendix A, "Cisco Security Agent Overview" for details.

If an agent has a policy containing an Agent service control rule that denies the stopping of the agent, administrators cannot stop the agent service on the system in question. See Agent Service Control, page 4-44.

# Backing Up Configurations

It is a good idea to back up your management server configurations at regular intervals. If your server system fails for any reason, and a copy of your configuration database is not stored elsewhere, you could lose your policy information.

**Caution** The CSA MC Backup Configuration feature is not available if you are using a remote database configuration.

The **Backup Configuration** feature, available from the **Maintenance** category in the menu bar, lets you backup your local database at regularly scheduled intervals or as needed.

To backup your CSA MC configuration, do the following.

**Step 1** Move the mouse over **Maintenance** in the menu bar and select **Backup Configuration** from the drop-down list that appears.

**Step 2** In the Backup Configuration window you can select the following radio buttons:

- **No database backup**—Select this option if you do not want backups to occur automatically at scheduled intervals but want to perform them manually. After selecting this radio button, enter the **directory path** (including drive letter) to which you want to save your backup configuration. Then click the **Backup now** button.

- **Scheduled database backup**—Select this option to schedule regular backups and then choose one of the scheduled backup options: Low frequency, Medium frequency, and High frequency. Enter the directory path (including drive letter) to which you want to save your backup configuration and click the Save button. Backups will now occur as scheduled.

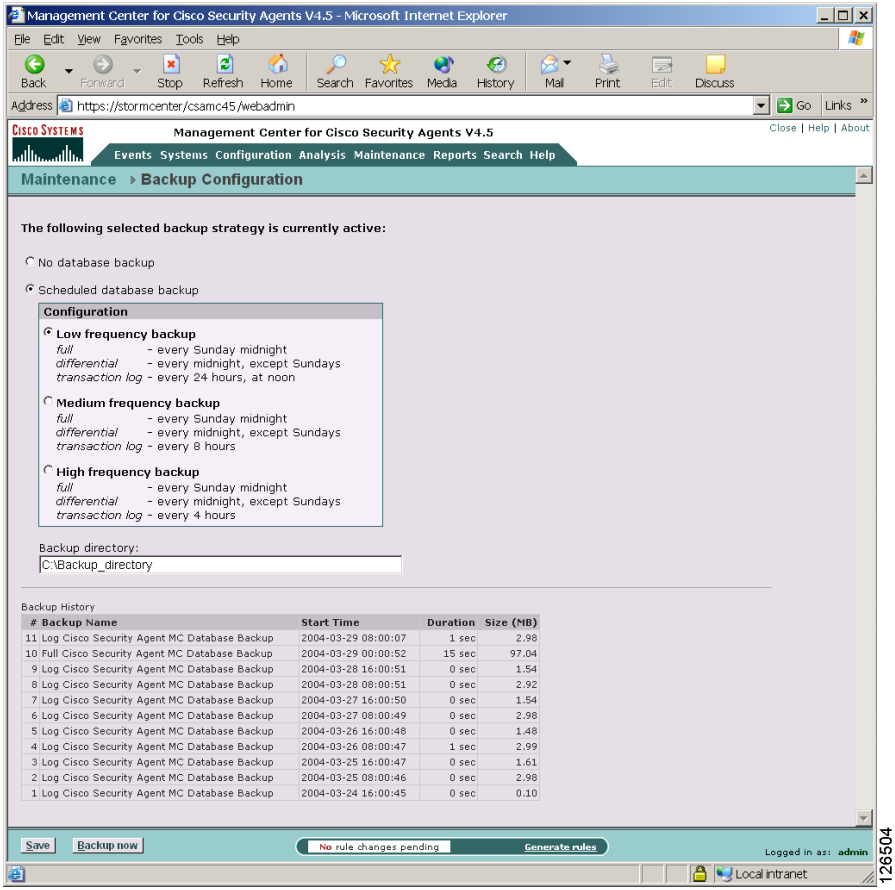
  Backup types are categorized as follows:

  **full**—A full backup occurs every Sunday night at midnight. This full backup includes the entire database with license information.

  **differential**—This type of backup occurs every night at midnight (except Sunday nights when a full backup occurs). A differential backup includes only data that has changed since the last backup (full or differential) occurred.

  **transaction log**—This backup occurs every 24 hours (low), 8 hours (medium), or 4 hours (high) depending on the frequency you select. The presence of this transaction log allows administrators to back out configuration changes to a certain point. Please refer to Microsoft documentation for details about the transaction log.

*Figure 10-1 Backup Configuration Window*




Backup Files appears as follows in the directory you select:

- full_backup_[db_name].bak—for full backups
- diff_backup_[db_name].bak—for differential backups
- log_backup_[db_name]_[x].bak—for log backups, where x is an integer from 1 to 23 (backup hour)
- crt_log_backup_[db_name].bak—for current transaction log backup

# Restoring Backup Configurations

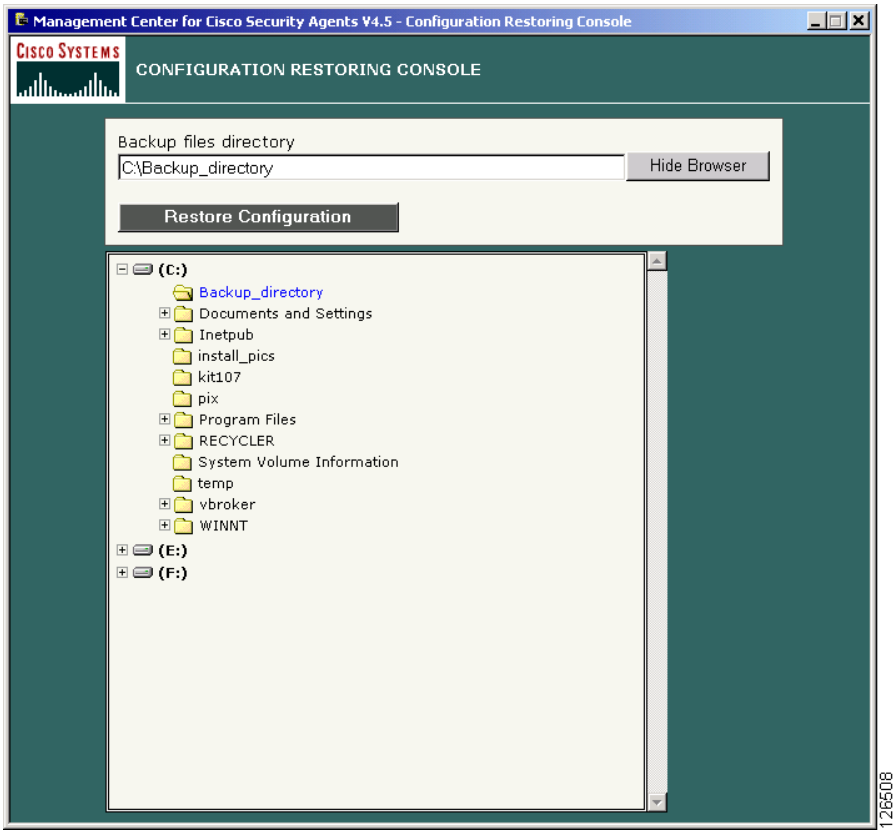
Restore backup CSA MC configurations, including database, license information, and transaction logs by running the Restore utility, called **Restore Configuration**, located in the default CSAMC45\bin directory:

**Note** If you are restoring a backup configuration due to a disk failure, after you re-install CSA MC and then restore the backup configuration, you may find that the final set of uncommitted transactions (no rule generation occurred) were lost.

**Step 1** Double-click the **Restore Configuration** file (located in the `CSCOpx\CSAMC45\bin` directory) to display the CSA MC restore user interface. See Figure 10-2.

**Step 2** Enter or browse to the directory path where the backup files are stored.

*Figure 10-2 Database Restoring Console*




**Step 3** Click the **Restore Configuration** button. When you click the Restore Configuration button, you are asked if you want to restore the backup configuration. Click **Yes** to do so.

The restore process now takes place. Once the restore is complete, a log file, the Database Restoring Log, is displayed.

**Note** When you restore backup configurations, you cannot select to restore only the transaction log, or only a differential backup. All files are automatically restored from the most recent backup that exists in the directory. It is recommended that you reboot the system after restoring from backup.

# Database Maintenance (Free Up Disk Space on CSA MC )

The **Database Maintenance** page is available from the **Maintenance** category in the menu bar. If you access this page and find that there are checkboxes available next to the database type(s), then the recommendation is for you to shrink your database files and log files to increase the amount of free disk space on your CSA MC system.

If the **Database Maintenance** category on the **Status Summary** page is issuing an alert about the database size or if your CSA MC event log contains an "insufficient disk space" message, this is an appropriate procedure for freeing up space.

**Note** If no checkboxes appear on this page, your database size is currently sufficient.

The following information points explain what you see on this Database Maintenance page:

**Database csamc45**

If you are using a database that is remote to the CSA MC system, you will see only this database category on this page. The database size is broken into two categories: **Event and configuration data** and **Application Deployment data**.

If the **Unallocated space** number listed on this page is more than 10% of the database size, a checkbox appears beside Database csamc45. If the checkbox is present, it is recommended that you select it and click the **Shrink database** button available from the bottom footer of this page.

**Database csaanalysis45 (behavior analysis data)**

If you are using a database that is local to the CSA MC system, you will see this database category in addition to the one above. You can shrink only this database or the csamc45 database, if necessary (if both checkboxes are available). If the **Unallocated space** number listed here is more than 10% of this database size, a checkbox appears beside Database csaanalysis45 (behavior analysis data). If the checkbox is present, it is recommended that you select it and click the **Shrink database** button available from the bottom footer of this page.

**Note** Even if both database categories are present, these are separate databases and their space allocations are independent.

**Note** Maintenance operations for remote databases must be done manually with the CSA MC service stopped (net stop csamc45).

# Using the COM Extract Utility

CSA MC provides a COM component extraction utility on agent systems, called `extract_com`, which installs in the `\Cisco Systems\CSAgent\bin` directory with each Cisco Security Agent. Running this utility extracts all COM component PROGID's and CLSID's for software running on the system in question and places this data into a text file. You can cut and paste these ID's from the text file into your COM component sets and access rules.

Run the extract_com utility on an agent system in the following manner:

**Step 1** Open a command prompt window.

**Step 2** From the `\Cisco Systems\CSAgent\bin` directory type in `extract_com filename`

"filename" is the name of the text file you want the utility to create. It is into this file that all COM PROGID and CLSID data is placed.

For example, enter:

```
\Cisco Systems\CSAgent\bin>extract_com foo.txt
```

The Cisco Security Agent creates the "foo.txt" file in the same \bin directory as the extract utility. You can access it from there.

**Caution** Both COM Component access control rule fields and Variable COM Component set fields require a very specific syntax for entering PROGID's and CLSID's. The COM component file created by the extract_com utility may display PROGID's

and CLSID's without the proper syntax in the output file. Despite this, when you enter these ID's into text fields for rules or variables you MUST use the correct syntax detailed on page 7-3.

# Manual Agent Data Filter Installation

On Windows platforms, if you install Web server software (IIS or Apache) after you install the Cisco Security Agent on the server system, or if you have installed the Web server in a directory other than the default, you must manually install the Cisco Security Agent data filter in order to use Data access control rules on the system in question.

**Note** If your Web server software is already installed (in its default directory) when you install the agent on Windows, the server software is detected by the agent and the data filter capability is automatically installed with the agent.

On Solaris and Linux, in order to use Data access control rules (on Apache or IPlanet servers for Solaris and on Apache servers for Linux) you must install the data filter manually after you install the Cisco Security Agent. Unlike Windows, the Solaris and Linux installations do not detect Web server software and do not install the data filter with the agent. You must always manually install it.

## Install Data Filter on Windows

If you have installed Web server software (IIS or Apache) after you install the Cisco Security Agent on the server system, or if you have installed the Web server in a directory other than the default, run the following command(s) to manually install the CSA data filter on the server system making use of Data access control.

For a Microsoft IIS Web server, run the following command:

```
csa_datafilter -i iis
```

For an Apache Web server, run one of the following Apache version appropriate commands:

```
csa_datafilter -i apache13 <.conf file with full path name>
<modules directory path>
csa_datafilter -i apache20 <.conf file with full path name>
<modules directory path>
```

For example, if Apache 2.0 was installed with its default settings after the agent is installed, you would run the following command to install the data filter:

```
csa_datafilter -i apache20 "c:\Program
Files\Apache\conf\httpd.conf" "c:\Program
Files\Apache\modules"
```

**Note** If there are spaces in the directory path, you must put quotations around the pathname.

**Caution** You must restart the web server service after the data filter is installed for data access control rules to take effect.

## Uninstall Data Filter on Windows

For a Microsoft IIS Web server, run the following command to uninstall the data filter:

```
csa_datafilter -u iis
```

For an Apache Web server, run one of the following Apache version appropriate commands to uninstall the data filter:

```
csa_datafilter -u apache13 <.conf file with full path name>
<modules directory path>
csa_datafilter -u apache20 <.conf file with full path name>
<modules directory path>
```

## Install Data Filter on Solaris or Linux

Run the following command to manually install the CSA data filter on the server system making use of Data access control.

```
webserver:root>./csa_datafilter -i
```

[output:]

```
CSA web server filter installation:
Should I install filters for IPlanet and/or Apache [No] y
Enter the path of the IPlanet config directory (null for
none): /usr/iplanet/servers/https-webserver/config
Enter the path of the Apache root (null for none):
webserver:root>
```

**Caution** You must restart the web server service after the data filter is installed for data access control rules to take effect.

**Note** On Linux, Data access control rules are only supported for Apache 2.0 servers.

## Uninstall Data Filter on Solaris or Linux

```
webserver:root>./csa_datafilter -u
```

[output:]

```
SA web server filter removal:
Should I uninstall filters for IPlanet and/or Apache [No] y
Enter the path of the IPlanet config directory (null for
none): /usr/iplanet/servers/https-webserver/config
magnus.conf saved as magnus.conf.sav
obj.conf saved as obj.conf.sav
The CSA agent filter for IPlanet 6.0 has been removed
Enter the path of the Apache root (null for none):
webserver:root>
```

# Exporting and Importing Configurations

Under the Maintenance category in the menu bar, use the Export utility to export your policies to other CSA MCs. If you have multiple CSA MCs, you might want to export some basic policies to those servers for deployment. Likewise, using the Import utility, you can download and import those policies as well as preconfigured policies that Cisco provides.

**Note** The Export utility exports entire rule modules and policies (not individual rules), including the accompanying application classes and configuration variables. Because of communication channels established in the original configuration, some site-specific imported configuration information (IP addresses) may not work on another server. Exporting an item will also export related data. In particular, exporting policies will export application classes and configuration variables referenced in rules within the policy. Exporting a group will export associated policies but not hosts.

**Caution** The Export/Import functions are not intended to be used as a backup/restore mechanism as they do not preserve system specific information such as group-host memberships.

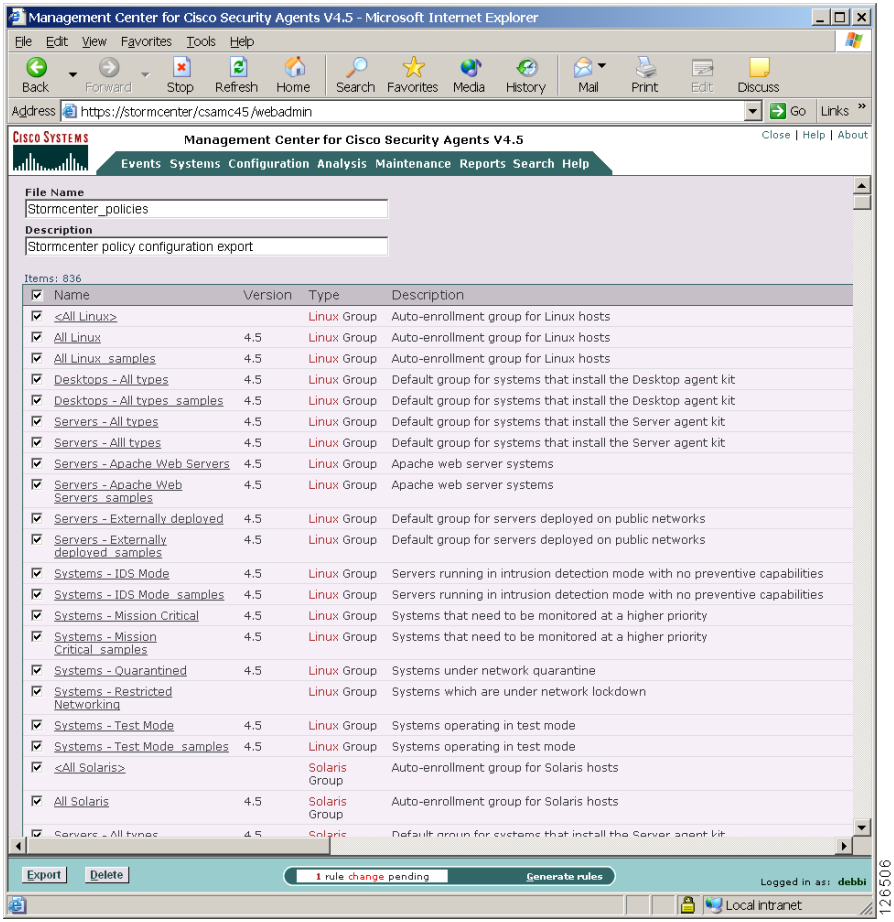
To Export configurations, do the following.

**Step 1** From the menu bar **Maintenance** drop-down list, move the mouse over **Export/Import**. A cascading menu with further selections appears. Select **Export** from the drop-down list that appears. Any previously exported files are shown.

**Step 2** Click the **New** button to create a new exported file. This takes you to a checkbox list of all configuration items.

**Step 3** **Check** the box beside the configurations you want to export. (See Figure 10-3). (You can also select the top checkbox beside the Name field to select all items.)

*Figure 10-3 Export Configurations*




**Step 4** At the top of the page, enter a **File Name** for the exported file you are creating. CSA MC will append an ".export" extension to the file name you enter.

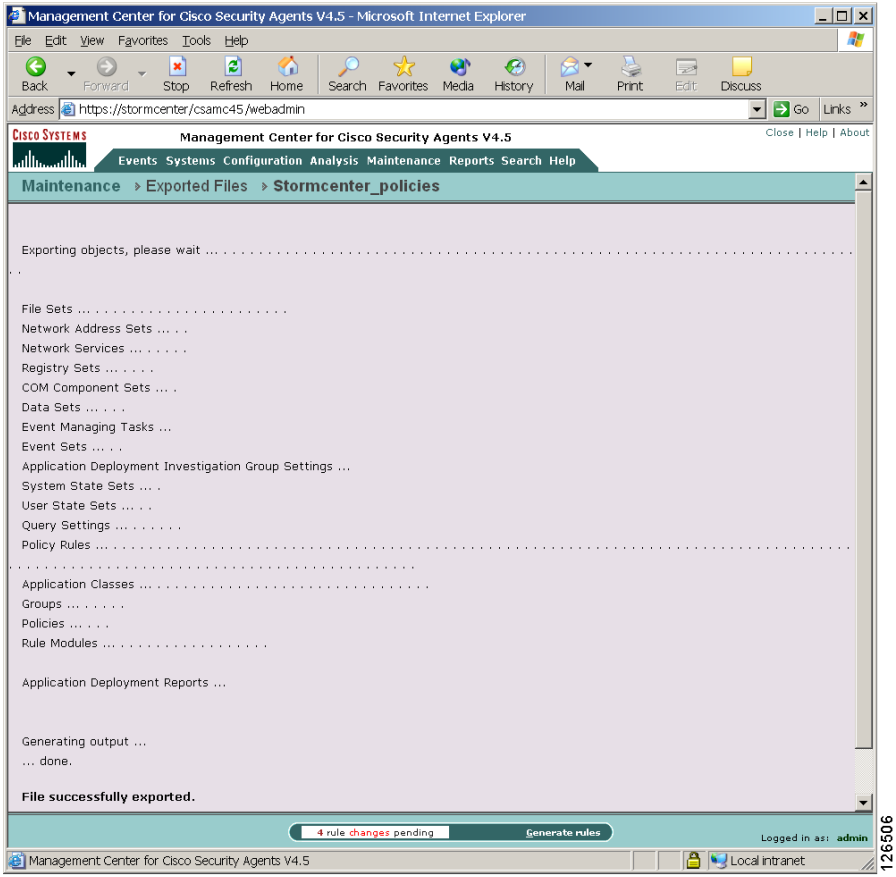
**Step 5** Click the **Export** button. The files are exported under the file name you create. Now you must save the file to the system.

**Step 6** Once the export has completed, a link is displayed that allows you to save the exported file. The link reads "Click here to download this file." **Click** on the "here" link to save the file to a directory you specify (see Figure 10-4).

Once you save the file, you can import it to any server.

**Note** When you export analysis reports, you are only exporting the report itself and the names of objects referenced in the report, such as a group or policy. The group and policy objects themselves are not automatically exported with the report. There is no cascading inheritance when you export either reports or event sets as occurs when other items are exported. You must select groups and policies separately if you want to export them for the purpose of the report.

***Figure 10-4 Export Download View***




To Import configurations, do the following.

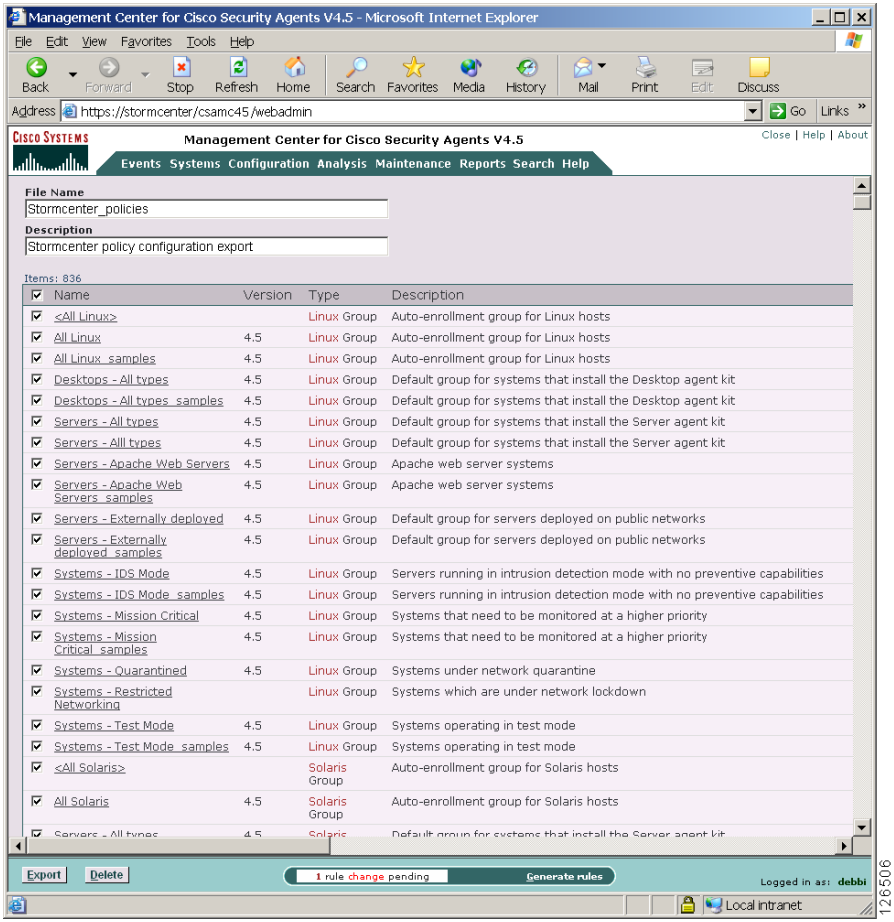
**Step 1** From the menu bar **Maintenance** drop-down list, move the mouse over **Export/Import**. A cascading menu with further selections appears. Select **Import** from the drop-down list that appears. Any previously imported files are shown.

**Step 2** Click the **New** button to create a new imported file. This takes you to the configuration Browse view (see Figure 10-5).

**Step 3** Click the **Browse** button to locate the exported file you want to import.

**Step 4** Enter a Description and then click the **Import** button to import the configuration.

*Figure 10-5 Import Configurations*




Imported files are automatically entered into the CSA MC database of the server you're importing them to. You don't have to do anything beyond the import function to unpack the exported file.

**Note** Configuration items shipped with CSA MC and provided by Cisco contain a version column with a version number. Administrator-created items have no version number.

When you import configuration items provided by Cisco, if it is found that there is already an existing exact match for an item, the new configuration data is not copied over. Instead, the existing item will be reused and the name will reflect the new versioning.

If the import process finds that there is an existing item with the same name and different configuration components (variables, etc.), the newly imported item is changed by adding a new version number. The new item is always the item that is re-versioned. Existing item are not renamed or reversioned if there is a collision.

Also note that CSA MC automatically appends the name of the export file to any non-Cisco item collision it finds during administrator imports. The imported item is given a different name and both new and old items can co-exist in the database.

# View Import History

Access this page from the CSA MC **Maintenence**>**Export/Import**>**Import History** menu path.

- The Import History List Page

The Import History page let you view lists of files that were imported to CSA MC from exported xml files. From this page, you can select the checkbox beside any file name and click the **Delete** button. This deletes the entire import, rolling your configuration back to its pre-import state.

- The Import History View Page

When you click on the name of a specific Import file, you can view another page listing all imported configuration items for that import file. You have the ability to purge specific imported items from CSA MC by selecting an item or items (via checkbox) and clicking the **Purge Objects** button. You can also use the **Delete** button to simply delete the history of the imported items, not the items themselves.

**Note** Items shipped with CSA MC are imported during the installation process. Therefore, the import done during the installation appears with any other imports shown on the Import History page.

# Cisco Security Agent Posture Plug-in for CTA

The Cisco Trust Agent(CTA) is a component of the Cisco NAC solution. The CTA client software may be installed separately or as part of the Cisco Security Agent installation. See Creating Agent Kits, page 3-8 for CTA installation information.

CTA communicates with all installed plug-ins on the system to extract various types of system information. The Cisco Security Agent sends posture state information (through its own posture plug-in) to CTA.

The Cisco Security Agent posture plug-in returns the following five attributes to CTA which then passes them on to NAC.

- CSAVersion—This is the software version of the installed Cisco Security Agent.
- CSAOperationState—This indicates whether the agent is up and running. A 1 value here indicates the Cisco Security Agent is enabled and running, providing security. A 0 value here indicates the agent is either not installed, not running, or security is turned off
- CSAMCName—This is the fully qualified domain name of the management center the Cisco Security Agent is registered with.
- CSAStatus—This may contain the following strings: global_testmode_on, rootkit_detected, or ipforwarding_on. (See other chapters in this manual for details on group test mode and rootkit detection.)
- DaysSinceLastSuccessfulPoll—This indicates the number of days that have passed since the Cisco Security Agent last polled in to the management center. If the agent has successfully polled within a period of time that is less than 1 day, the value represented here is 0.


# Using Cisco Security Agent Analysis

## What is Analysis

Cisco Security Agent Analysis functionality works with CSA MC and the agent, serving as a data collection and behavior analysis tool for administrators who are deploying policies across systems and networks.

This section contains the following topics.


- What is Analysis, page 11-1
- The Application Deployment Investigation Process, page 11-3
- Reporting Categories, page 11-3
- Turning Application Deployment Investigation On, page 11-4
- Configure Group Settings, page 11-4
- Configure Product Associations, page 11-7
- Associate Unknown Applications, page 11-12
- About Data Management, page 11-14
- Generating Application Deployment Reports, page 11-16
- AntiVirus Installations Report, page 11-17
- Installed Products Report, page 11-20

- Unprotected Hosts Report, page 11-23
- Unprotected Products Report, page 11-25
- Product Usage Report, page 11-27
- Network Data Flows Report, page 11-30
- Network Server Applications Report, page 11-34
- Viewing Reports, page 11-37
- Exporting Reports, page 11-38
- What is Application Behavior Investigation, page 11-38
- How Application Behavior Investigation Works, page 11-39
- The Application Behavior Investigation Process, page 11-39
- Behavior Analyses, page 11-40
- Creating, Saving, and Cancelling Analysis Data, page 11-40
- Configure a Behavior Analysis Investigation, page 11-42
- Start Behavior Analysis, page 11-47
- Importing the Rule Module, page 11-50
- Application Behavior Reports, page 11-52
- Report Components, page 11-53
- Working with Reports, page 11-57
- The Behavior Analysis Rule Module, page 11-58
- Behavior Analysis Methodology, page 11-59
- Reviewing the Rule Module, page 11-59


The rules that comprise policies are aimed at protecting your enterprise resources, knowing exactly what those resources are and how they are used is essential to deploying effective policies.

With Application Deployment Investigation:

- You can see what applications are running on systems and determine what their usage patterns are.
- You can see what applications are installed but remain largely unused on systems.
- You can see what applications are accessing critical network resources.

- Use collected data to accurately deploy policies or to generate new policies for unprotected applications using the Cisco Security Agent.

# The Application Deployment Investigation Process

Deployment Investigation is a part of the Management Center for Cisco Security Agents and requires no separate installation process and very little configuration. As previously mentioned, the analysis data collection process is controlled on a per group basis. Application Deployment Investigation is either turned on or off for a group. The investigation process does not affect any policies that are attached to the group in question.

**Note** All agent functionality, including enforced security policies, operate normally when tracking is taking place on an agent host.

## Reporting Categories

Application Deployment Investigation is mainly comprised of the reporting capabilities it provides once all the data is collected. You can organize the gathered data in various manners to provide information on how your enterprise operates, the resources that are accessed, resource and application usage time frames, and a great deal more. In turn, this data can inform the crafting of your policies while you create a more secure environment for all your users to operate within.

While you cannot configure what types of information you collect using deployment investigation (it gathers all usage information while it is enabled), you can organize the information that is gathered in various ways.

- You can generate reports to display the list of software products installed across your enterprise. Of those products, you can view which are being used and which are not. You can sort reports by application network usage. This could include usage time frames, client and/or server connections, and the applications that are accessing the network. Of the information types you gather, you can use reports to cross-reference this data to distill even more specific reports such as one which displays what applications are running unprotected (without a policy) on systems

# Turning Application Deployment Investigation On

**Note** Application Deployment Investigation is only supported on Windows platforms.

**Note** By default, Application Deployment Investigation is disabled for all Windows groups until you enable it.

## Configure Group Settings

Deployment Investigation is controlled on a per group basis and it is enabled or disabled using the **Analysis>Application Deployment Investigation>Group Settings** page.

**Caution** If deployment investigation is enabled for the group, it begins on all hosts in the group in question after you generate rules and the hosts next poll in to CSA MC.

**Note** If you want to enable Application Deployment Investigation for only one host, you must create a new group with Application Deployment Investigation enabled and add the host to that group. If a host belongs to multiple groups, having Application Deployment Investigation enabled, if present in any group for which the host is a member, takes precedence over not having it enabled. Once Application Deployment Investigation is enabled for a group, it continues to collect data until you disable it and generate rules.

To configure group settings for Application Deployment Investigation, do the following.

**Step 1** Move the mouse over **Analysis>Application Deployment Investigation** in the menu bar and select **Group Settings** from the drop-down list that appears.

**Step 2** Click the **New** button to create a new group setting. See Figure 11-2.

**Step 3** In the available group setting fields, enter the following information:

- **Name**—This is a unique name for this group setting. Names are case insensitive, must start with an alphabetic character, can be up to 64 characters long and can include alphanumeric characters, spaces, hyphens -, and underscores _ .
- **Description**—This is a useful line of text that is displayed in the list view and helps you to identify this particular group setting.

**Step 4** Configuration Analysis Application Deployment Investigation enable options.

Click the **Enable Application Deployment Investigation** checkbox and select one of the following radio button options:

- Product data collection - which would apply to the following reports:

  AntiVirus Installations, Installed Products, Unprotected Products, Product Usage

- Product and network data collection - which would apply to the following additional report:

  Network Server Applications

- Product and verbose network data collection - which would apply to the following additional reports:

  Unprotected Hosts, Network Data Flows

**Caution** For Deployment Investigation to function properly, you must not exceed the following limits: The total number of agents with Application Deployment Investigation enabled should not exceed 100,000; The total number of agents with Application Deployment Investigation enabled in non-verbose network mode should not exceed 10,000; The total number of agents with Application Deployment Investigation enabled in verbose network mode should not exceed 1,000.

The following diagram illustrates which radio buttons must be selected for which report types:

*Figure 11-1 Group Setting and Report Dependencies*

It is recommended that you choose lowest verbosity level available in reports whenever possible to keep the volume of network data collection manageable.

Also, enter an **Upload Interval** time for agent to send collected data to the MC. The default and minimum interval is 24 hours.

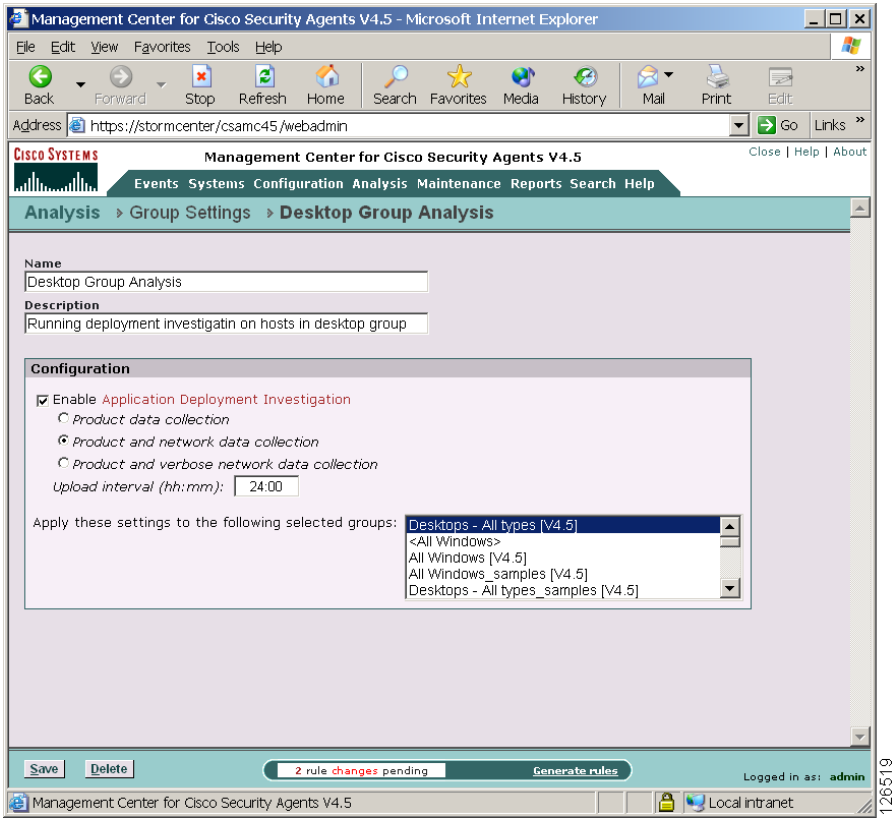
**Note** The uploading of data occurs at the end of the interval in question. Therefore, it may take more than one interval receive collected data. It depends upon when the hosts polls into the MC.

**Step 5** In the **Apply these settings to the following selected groups** list box, select one or more groups for data collection.

**Step 6** Click the **Save** button when your group setting configuration is finished.

Deployment investigation begins on all hosts in the group in question after you generate rules and the hosts next poll in to CSA MC.

***Figure 11-2 Deployment Investigation Group Settings***




# Configure Product Associations

You can use Application Deployment Investigation to generate reports that use installed software products as part of the report criteria. In order to do this, there is some prerequisite configuration. This is necessary because the deployment investigation process, in part, gathers data on systems according to the application name it finds. That is the application executable itself and not the product with

which the application is associated. Application Deployment Investigation does gather information on the products that are installed on systems, but it does not then map the applications back to the installed products. For example, Application Deployment Investigation may find that excel.exe is running on a system. It may also find that Microsoft Office is installed on that same system. But it will not know that excel.exe is part of Microsoft Office. You must tell it so.

Therefore, in order to generate certain reports types using installed product information, you must first associate the installed products found by Application Deployment Investigation with the application(s) that comprise the product. (This could entail creating new application classes for this purpose.)

You must make this application class/product association to use product criteria to generate the following report type:

- Product Usage

**Caution** Pre-configured application classes that ship with CSA MC are not available to Application Deployment Investigation functionality. It is recommended that you configure application classes that are separate and solely for the purpose of Analysis reports and investigation. This way, you are not compromising existing application classes that are used in CSA MC security policies.

To create application class/product associations, after Application Deployment Investigation has collected data, do the following.

**Step 1** Move the mouse over **Analysis** in the menu bar of CSA MC and select **Application Deployment Investigation>Product Associations**.

The deployment investigation Products page contains a list of all the installed products (not applications) found on systems that were investigated. See Figure 11-3. These are the products names that would be viewable through the Microsoft Add/Remove Programs window.

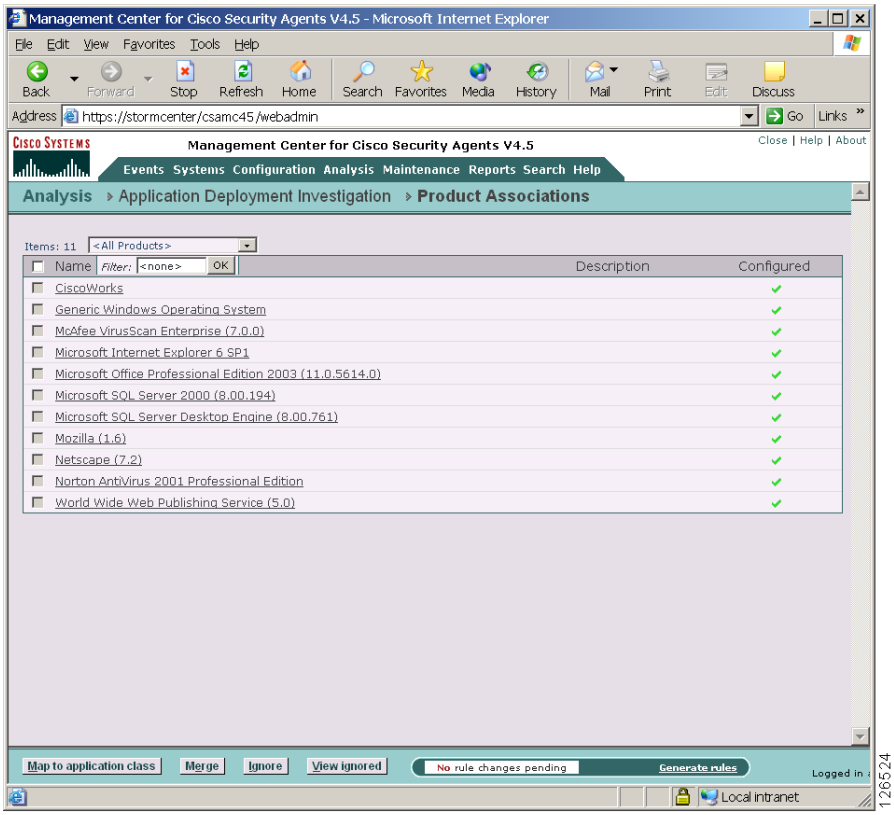
**Step 2** To associate a product with an application, click the product in the Product Associations window. This takes you to a window which allows you to select an application class or classes that will define the product.

You can also associate a product with an application by selecting the checkbox beside the product name link and clicking the **Map to application class** button. This opens a new window which allows you to select an application class that will define the product. You can map the product to an existing or new application class.

**Step 3** Click **Save** once you selected an application class(es).

**Step 4** Optionally, select a product and use the **Ignore** button to have that product be "ignored" and not appear in reports. You can undo an ignore setting by clicking the **View ignored** button to launch a new window which allows you to "restore" the product in question.

*Figure 11-3 Product Association List Window*




**Step 5** Optionally, you can use the **Merge** button to combine multiple unmapped products into one merged product. For example, you may have several "hotfix" items in your product list. You can put them all into one "Microsoft Hot Fixes" product category using the merge feature.

To merge products, select the checkboxes of the products you want to combine and click the **Merge** button. This takes you to a window which allows you to create a new name for the merged products. See Figure 11-4.

Once you merge products, they will no longer appear as separate items in your product list.

*Figure 11-4 Product Association Merge Window*

The Product Associations merge window allows you to enter a name for the new merged products. You can also use the **Add** and **Remove** buttons on this page to add more products to the merge or to remove one or more products from the merge.

**Note** You can also use the shortcut **Reports** link on the merge page to view the Installed Products and Product Usage reports for the product named on the page you're on.

# Associate Unknown Applications

This window displays a list of applications (processes) that have run on systems but have no product associated with them. (This is the inverse of the Application Deployment Investigation Product Associations page.)

You can use Application Deployment Investigation to generate reports that use installed software products as part of the report criteria. In order to do this, there is some prerequisite configuration.

This is necessary because the investigation process, in part, gathers data on systems according to the application name it finds. That is the application executable itself and not the product with which the application is associated. Application Deployment Investigation does gather information on the products that are installed on systems, but it does not then map the applications back to the installed products. For example, it may find that excel.exe is running on a system. It may also find that Microsoft Office is installed on that same system. But the analysis process will not know that excel.exe is part of Microsoft Office. You must tell it so.

Therefore, in order to generate certain reports types using installed product information, you must first associate the installed products found by the investigation process with the application(s) that comprise the product. (You can also associate a product with an existing application class from the Product Associations page.)

You must make this application/product association to use product criteria to generate the following reports type:

- Product Usage

To create application/product associations, after the data has been collected, do the following.

**Step 1** Move the mouse over **Analysis** in the menu bar of and select **Application Deployment Investigation>Unknown Applications**.

**Step 2** The Unknown Applications window contains a list of all the processes found on systems that were tracked which have no association with an installed product. See Figure 11-5. To associate an application with a process, select the checkbox beside the process name link and click the **Map to product** button. This opens a new window which allows you to select a product that will define the application

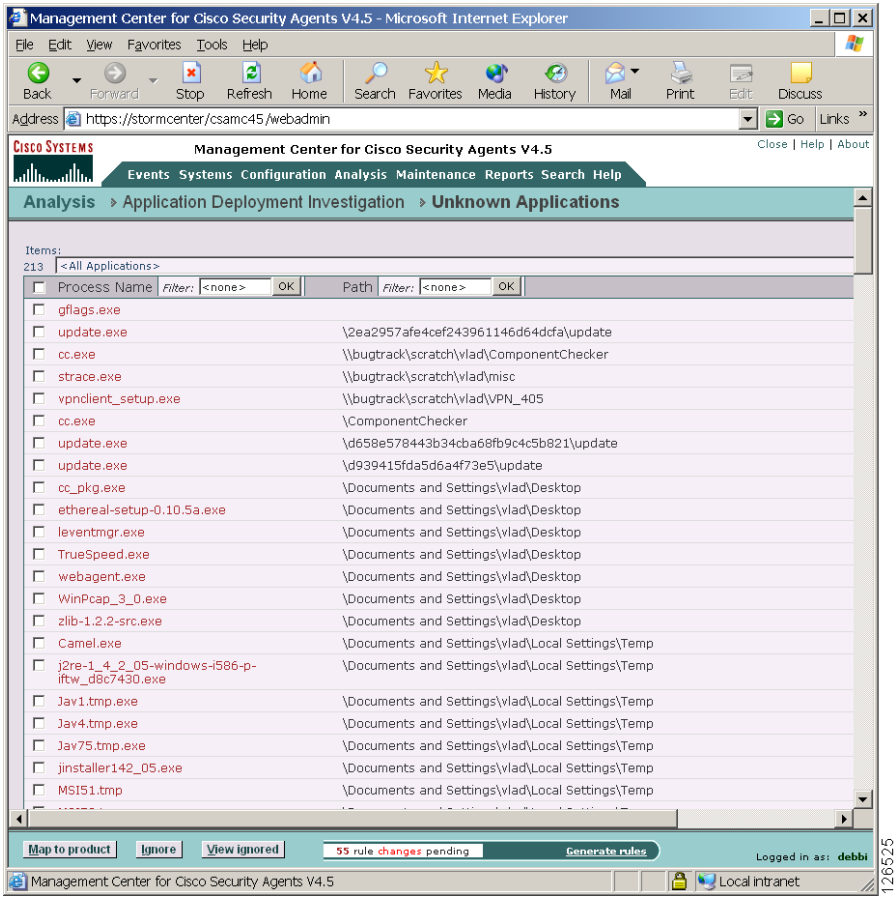
process. You can also map the application to an existing or new application class. (Note that you can only map and/or ignore products that have not yet been mapped.)

**Step 3** Click **Save** once you selected a product. The process will then disappear from the Unknown Applications list as it is no longer unknown.

Optionally, select a process and use the **Ignore** button to have that process be "ignored" and not appear in reports. You can undo an ignore setting by clicking the **View ignored** button to launch a new window which allows you to "un-ignore" the process in question.

**Note** You can enter text strings into the Filtering fields in this Window to search for particular items. You can also use the pulldown field at the top of the page to find particular paths for applications.

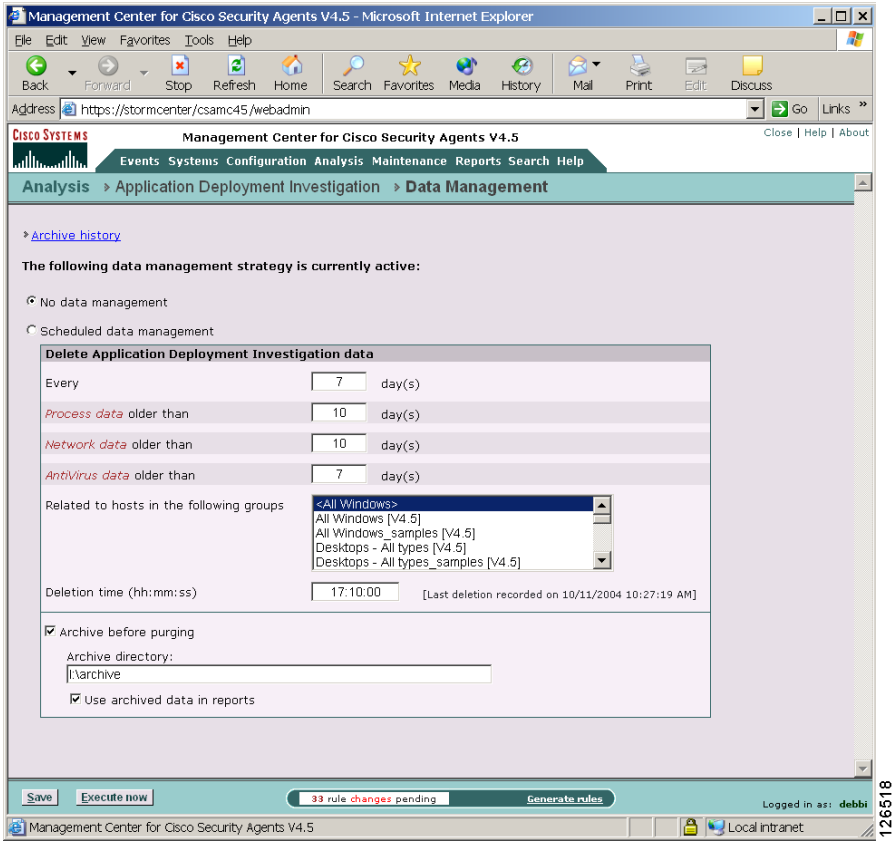
*Figure 11-5 Unknown Applications List Window*




# About Data Management

Accessible from the **Analysis>Application Deployment Investigation>Data Management** menu, the Data Management window allows you to archive and purge the data collected by the deployment investigation. See Figure 11-6.

*Figure 11-6 Data Management Window*




Use the Data Management page to purge deployment investigation data at scheduled intervals and to optionally archive the data you are deleting from the active database.

This page gives you the option having no scheduled data management (**No data management** radio button) or setting parameters for a scheduled purging of data (**Scheduled data managemen**t radio button).

You can configure your data management to purge certain types of data at different time intervals as you choose. Process data, Network data, and AntiVirus data can be purged according to the day and time interval you set. Note that AntiVirus data has been added as a separate category due to the large volume of this data type that can accumulate.

If you click the **Execute Now** button, you can trigger data management to occur immediately based on the current configuration, regardless of the data management type you have configured using the available radio buttons.

**Archive before purging**

**Note** The Archive feature is only available if the database is local to the CSA MC system.

Select the Archive before purging checkbox and enter a directory to store archived data in if you do not want to loose the report data you are purging. You can continue to use this archived data in your reports.

**Note** If you change the Archive directory after you've already archived data, that data is automatically moved to the new directory and new archived data will be stored in the newly specified directory as well.

**Note** You can click the **Archive history** link at the top of this page to view an informational list of data purges that have taken place on the system.

# Generating Application Deployment Reports

You can generate several different Application Deployment Report types using the data gathered during the tracking process. The following sections describe each of these reports.

You generate reports by selecting various sorting options in the CSA MC report configuration views. When you are finished selecting sorting parameters, you can generate your report. The report opens in a new browser window.

To generate an Application Deployment Report, do the following.

**Step 1** Move the mouse over **Analysis>Application Deployment Reports** in the menu bar.

**Step 2** A drop-down list and a cascading menu of report types appears. Select a report type from the cascading menu to enter parameters and generate that report.

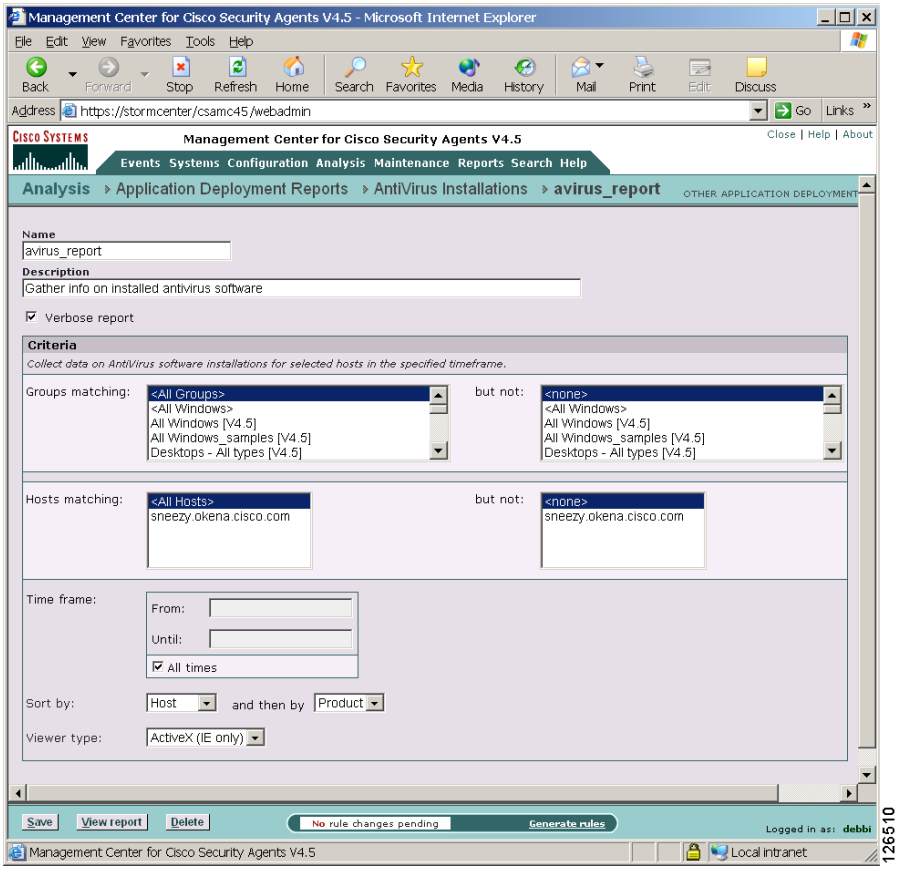
The follow section continues these instructions and describes each type of report.

# AntiVirus Installations Report

Use this report type to view software version and signature version information for detected Norton and McAfee AntiVirus installations. (Note that for McAfee AntiVirus software, you will also see the engine version in the report.) From the **Analysis>Application Deployments Reports** option, select a report type. In this case, click on **AntiVirus Installations** and do the following:

**Step 1** In the report window, click the **New** button to create a new report. This takes you to the report configuration view. See Figure 11-7.

*Figure 11-7 AntiVirus Installations Report Page*




**Step 2** Enter a **Name** and **Description** for the report.

**Step 3** Optionally, enable the **Verbose report** checkbox. If you do not enable this checkbox and you have selected to generate a report for <All Groups> and <All Hosts>, you will only see summary information (number of overall installation copies found) for installed antivirus products. If you enable Verbose, you will see a much longer report containing details for installed antivirus products on each host by host name.

AntiVirus Installations non-verbose reports contain the following data:

- AntiVirus product name, Product version, Engine and signature version, the number of Hosts running this combination.

AntiVirus Installations verbose reports contain the following data:

- Host name, Product version, Engine version, Signature version, Time this information was obtained.

**Step 4** From the **Groups matching** field, you can select a specific group for which to generate antivirus installation information. You can view information for <All Groups> or only for those you select. Optionally, use the **but not** field to exclude certain groups from those selected in the Groups matching field.

**Step 5** From the **Hosts matching** field, you can select hosts within the selected Group(s) for which to generate antivirus installation information. You can view information for <All Hosts> or only for those you select by using the **but not** field to exclude certain hosts from those selected in the Hosts matching field. Using exclusions, you can generate a report for a specific host within a selected group.

**Note** Individual hosts do not appear in the Hosts report field until they have uploaded data at least once.

**Step 6** Enter a **Time Frame** by which to view the collected data. This time indicates the last or most recent time the antivirus product was used on the system(s) in question.

You can enter **From** and **Until** time parameters using the syntax shown below or you can check the **All times** checkbox for all time frames.

Time syntax:

You can specify a relative time using any of the following terms: tomorrow, now, next, year, month, week, day, hour, minute, and second.

**Step 7** Select criteria by which to sort the report. You can first sort by host and then by product or vice-versa.

**Step 8** Select a **Viewer type**. By default, ActiveX is selected. This is the recommended viewer. Click the **Save** button to save the parameters you've just configured for generating this report.

**Step 9** Click the **View Report** button and the report is automatically displayed in a new window.

You can use the Delete button to delete/remove the report entirely.

# Installed Products Report

Use this report type to view a list of products that are installed or not installed on various selected host machines. The Products listed alphabetically in the report page are the software programs found to be installed (or not installed) on the systems that were analyzed. These are software programs that are visible in the Add/Remove Programs window.

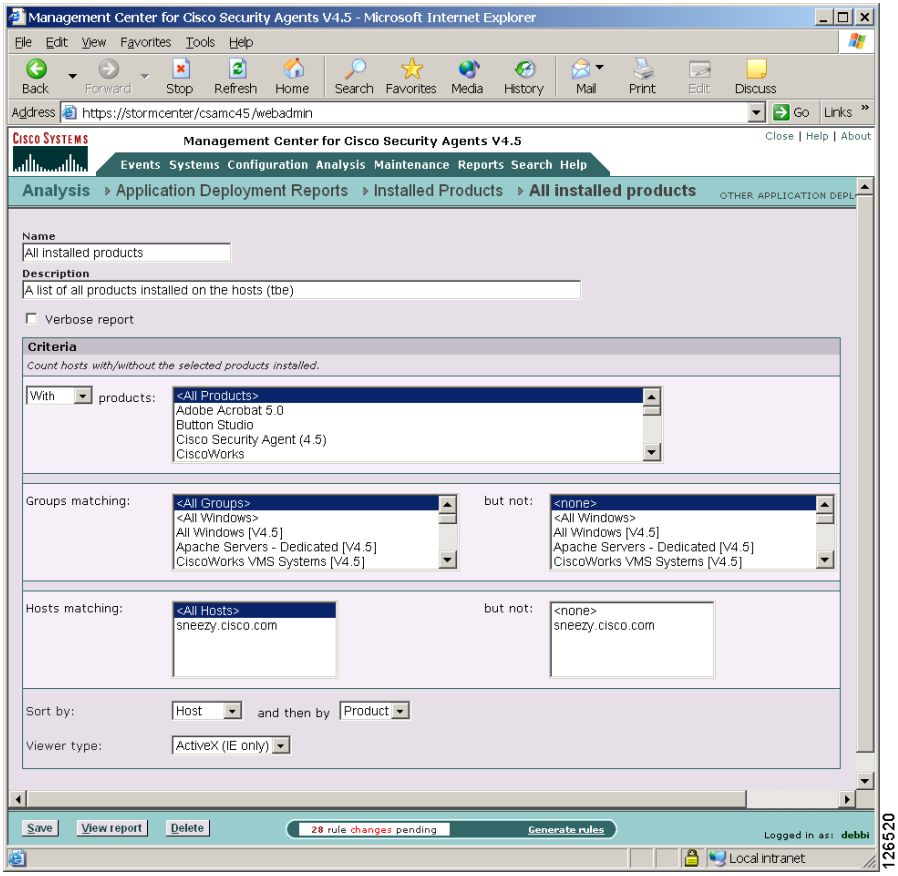
**Note** This report provides only the latest reported installed product information. It does not provide any historic data on installed products. Therefore, there is no time range available in this report.

You can choose to generate a report that provides the following information:

From the **Analysis>Application Deployments Reports** option, select a report type. In this case, click on **Installed Products** and do the following:

**Step 1** In the report window, click the **New** button to create a new report. This takes you to the report configuration view. See Figure 11-8.

*Figure 11-8 Installed Products Report Page*




**Step 2** Enter a **Name** and **Description** for the report.

**Step 3** Optionally, enable the **Verbose report** checkbox. If you do not enable this checkbox and you have selected to generate a report for <All Groups> and <All Hosts>, you will only see summary information (number of overall installation copies found) for installed products. If you enable Verbose, you will see a much longer report containing details for installed products on each host by host name.

Installed products non-verbose reports contain the following data:

- Distinct product name and the overall number of Hosts that have this product installed.

Installed products verbose reports contain the following data:

- Distinct product name and the individual Hosts that have this product installed.

**Step 4** If you are creating a report of products not installed on the system(s) in question, select "Count hosts **without** the selected product installed." If this is a report on products installed on selected hosts, leave the default choice of **with** in the pulldown view.

**Step 5** From the **Products** list field, you can select one or more products and view which hosts and or groups have that product installed (or not installed) on their system (verbose). You can also select <All Products> depending on the type of report you wish to generate.

**Note** You do not have to associate products with application classes to run this report type.

**Step 6** From the **Groups matching** field, you can select a specific group for which to generate product installation information. You can view information for <All Groups> or only for those you select. Optionally, use the **but not** field to exclude certain groups from those selected in the Groups matching field.

**Step 7** From the **Hosts matching** field, you can select hosts within the selected Group(s) for which to generate product installation information. You can view information for <All Hosts> or only for those you select by using the **but not** field to exclude certain hosts from those selected in the Hosts matching field. Using exclusions, you can generate a report for a specific host within a selected group.

**Step 8** Select criteria by which to sort the report. You can first sort by host and then by product or vice-versa.

**Step 9** Select a **Viewer type**. By default, ActiveX is selected. This is the recommended viewer. Click the **Save** button to save the parameters you've just configured for generating this report.

**Step 10** Click the **View Report** button and the report is automatically displayed in a new window.

You can use the Delete button to delete/remove the report entirely.

# Unprotected Hosts Report

Use this report type to view hosts which are being used in network connections, but are not protected by Cisco Security Agents.

**Note** This report type uses Network address sets and Network services for filtering criteria. It is recommended that you restrict the network address set to systems under your control. Otherwise, the report may describe external sites as not having the Cisco Security Agent installed. Likely, this is not the intention of the report.

**Note** Network data collection must be enabled to gather data relevant to this report.

From the **Analysis>Application Deployment Reports** option, select a report type. In this case, click on **Unprotected Hosts** and do the following:

**Step 1** In the report window, click the **New** button to create a new report. This takes you to the report configuration view.

**Step 2** Enter a **Name** and **Description** for the report.

**Step 3** From the **Network Address Sets** field, select a preconfigured Network Address Set. You can view information for <All Addresses> or only for those you select.

**Note** You can create a new Network Address Set or edit an existing one from this page by clicking the **New** link or by double-clicking an item in the selection field.

**Step 4** From the list field, select a preconfigured **Network Services**. You can view information for <All Ports> or only for those you select.

**Note** You can create a new Network Service or edit an existing one from this page by clicking the **New** link or by double-clicking an item in the selection field.

**Step 5** Enter a **Time Frame** by which to view the collected data.

You can enter **From** and **Until** time parameters using the syntax shown below or you can check the **All times** checkbox for all time frames.

Time syntax:

You can specify a relative time using any of the following terms: tomorrow, now, next, year, month, week, day, hour, minute, and second. Enter a specific time using any of the follow time formats: hh:mm:ss. If no meridian (AM or PM) is specified, hh is interpreted on a 24 hour clock (0-23). Note that entering minutes and/or seconds is optional.

**Step 6** Select the primary and secondary criteria by which to sort the report. You can sort by operation, host, unprotected address, or protocol.

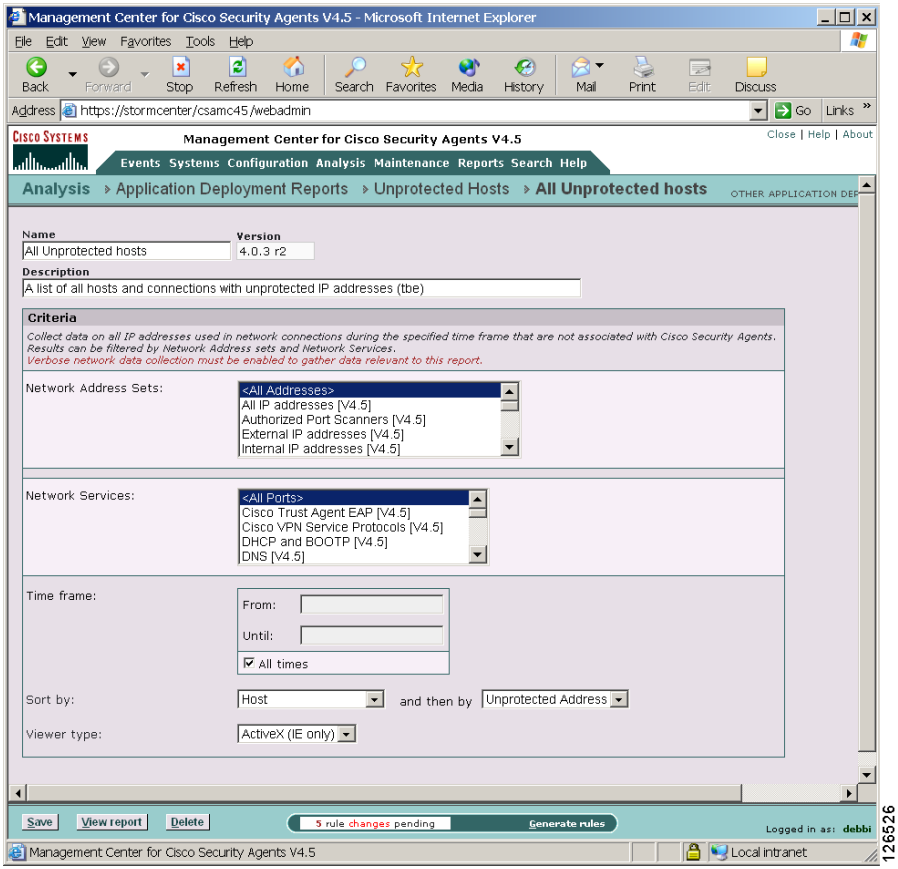
**Step 7** Select a **Viewer type**. By default, ActiveX is selected. This is the recommended viewer.

**Step 8** Click the **Save** button to save the parameters you've just configured for generating this report.

**Step 9** Click the **View Report** button and the report is automatically displayed in a new window.

You can use the Delete button to delete/remove the report entirely.

*Figure 11-9 Unprotected Hosts Page*




# Unprotected Products Report

Use this report type to view hosts that have products installed which have no associated Cisco Security Agent policies (i.e. Hosts running products for which there is no deployed policy.) Note that this report type is the most complex report to configure as it requires both product associations to be configured and network data to be collected.

From the **Analysis>Application Deployment Reports** option, select a report type. In this case, click on **Unprotected Products** and do the following:

**Step 1** In the report window, click the **New** button to create a new report. This takes you to the report configuration view. See Figure 11-10.

**Step 2** Enter a **Name** and **Description** for the report.

**Step 3** From the **Products** list field, you can select one or more products and view which hosts and or groups have used that product on their system (verbose) but have no policy for that product enforced. You can also select <All Products> depending on the type of report you wish to generate.

**Note** You must first associate products with application classes to run this report type.

**Note** Network data collection must be enabled to gather data relevant to this report.

**Step 4** From the **Groups matching** field, you can select a specific group for which to generate unprotected product information. You can view information for <All Groups> or only for those you select. Optionally, use the **but not** field to exclude certain groups from those selected in the Groups matching field.

**Step 5** From the **Hosts matching** field, you can select hosts within the selected Group(s) for which to generate report information. You can view information for <All Hosts> or only for those you select by using the **but not** field to exclude certain hosts from those selected in the Hosts matching field. Using exclusions, you can generate a report for a specific host within a selected group.

**Step 6** Select criteria by which to sort the report. You can first sort by host and then by product or vice-versa.

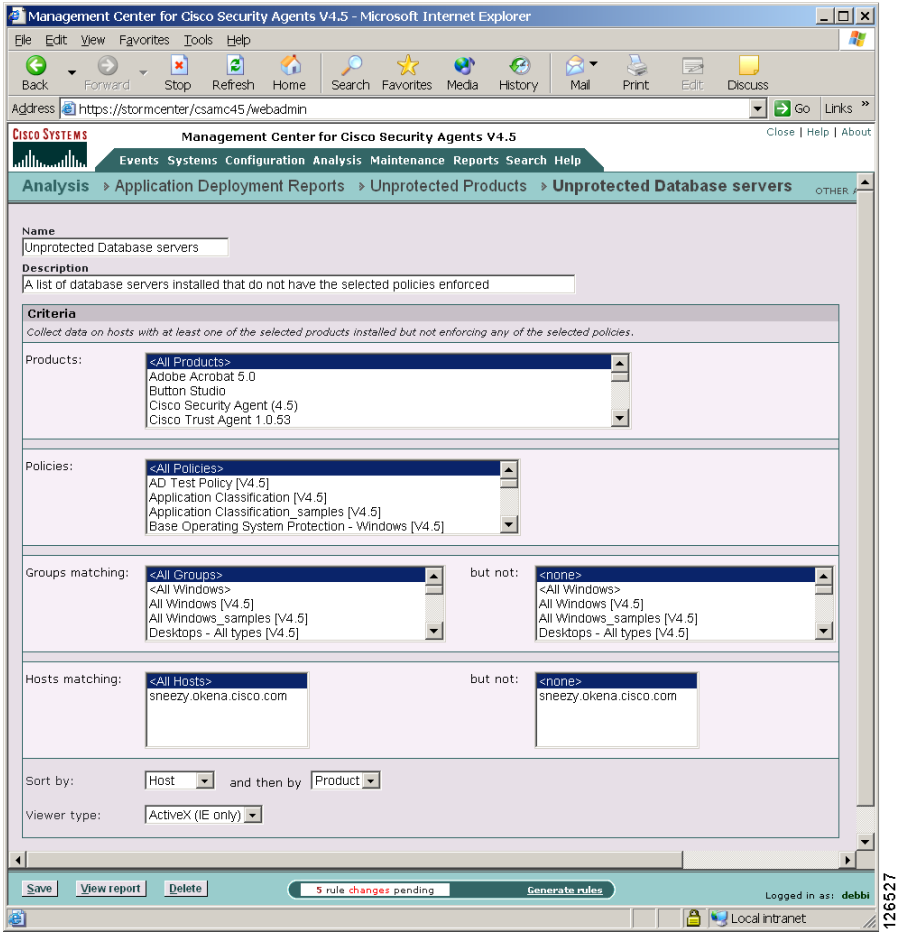
**Step 7** Select a **Viewer type**. By default, ActiveX is selected. This is the recommended viewer.

**Step 8** Click the **Save** button to save the parameters you've just configured for generating this report.

**Step 9** Click the **View Report** button and the report is automatically displayed in a new window.

You can use the Delete button to delete/remove the report entirely.

*Figure 11-10 Unprotected Products Report Page*




# Product Usage Report

Use this report type to view the number of systems on which installed products are used or not used.

**Note** In order to generate this report type, you must first associate products (all or just the particular ones you're interested in) with an application class or classes. See Configure Product Associations, page 11-7.

From the **Analysis>Application Deployments Reports** option, select a report type. In this case, click on **Product Usage** and do the following:

**Step 1** In the report window, click the **New** button to create a new report. This takes you to the report configuration view. See Figure 11-11.

**Step 2** Enter a **Name** and **Description** for the report.

**Step 3** Optionally, enable the **Verbose report** checkbox. If you do not enable this checkbox and you have selected to generate a report for <All Groups> and <All Hosts>, you will only see summary information displaying the overall number of systems each product is used on. If you enable Verbose report, you will see a much longer report containing details for product usage on each host by host name.

Product Usage non-verbose reports contain the following data:

- Product name and the overall number of hosts that have used the product.

Product Usage verbose reports contain the following data:

- Product name and the individual name of the host(s) that have used the product.

**Step 4** If you are running a report to determine which products are not used on systems, select "List hosts which have **not used** the selected products within the specified time" in the options pulldown list. Otherwise, leave the default choice of **used** selected.

**Step 5** From the **Products** list field, you can select one or more products and view which hosts and or groups have used that product on their system (verbose). You can also select <All Products> depending on the type of report you wish to generate.

**Step 6** From the **Groups matching** field, you can select a specific group for which to generate used product information. You can view information for <All Groups> or only for those you select. Optionally, use the **but not** field to exclude certain groups from those selected in the Groups matching field.

**Step 7** From the **Hosts matching** field, you can select hosts within the selected Group(s) for which to generate report information. You can view information for <All Hosts> or only for those you select by using the **but not** field to exclude certain hosts from those selected in the Hosts matching field. Using exclusions, you can generate a report for a specific host within a selected group.

**Step 8** Enter a **Time Frame** by which to view the collected data. This time indicates when the product was used on the system(s) in question.

You can enter **From** and **Until** time parameters using the syntax shown below or you can check the **All times** checkbox for all time frames.

Time syntax:

You can specify a relative time using any of the following terms: tomorrow, now, next, year, month, week, day, hour, minute, and second. Enter a specific time using any of the follow time formats: hh:mm:ss. If no meridian (AM or PM) is specified, hh is interpreted on a 24 hour clock (0-23). Note that entering minutes and/or seconds is optional.

**Step 9** Select criteria by which to sort the report. You can first sort by host and then by product or vice-versa.

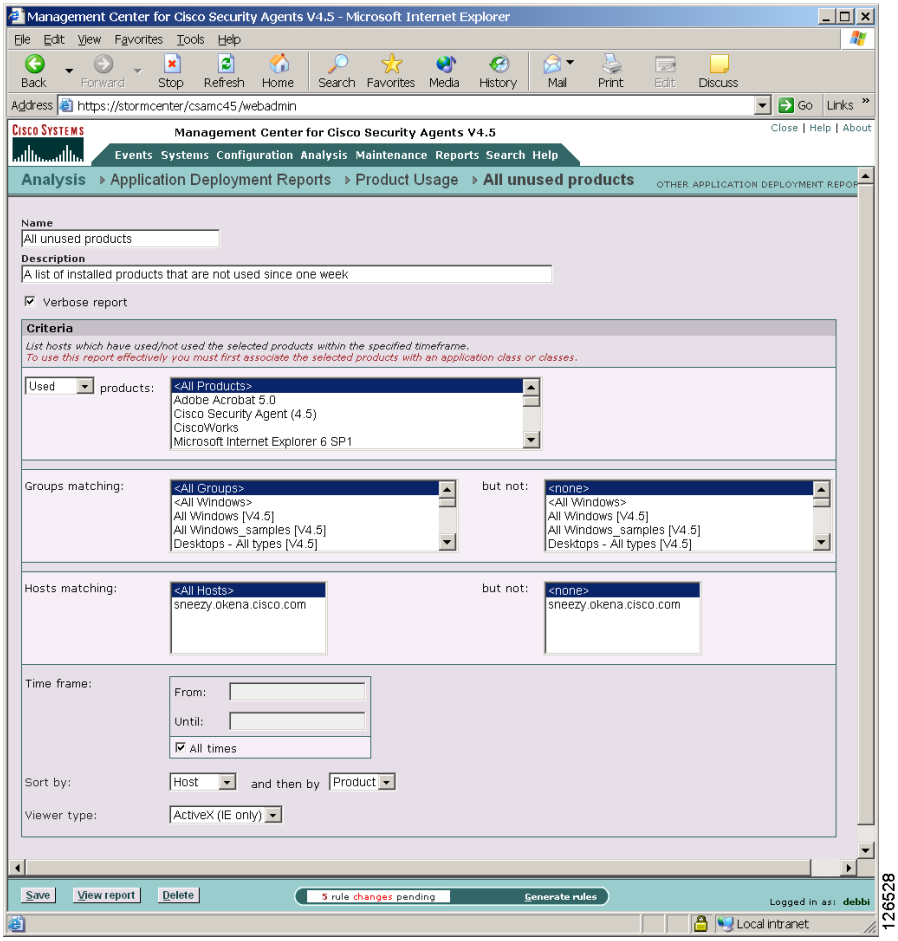
**Step 10** Select a **Viewer type**. By default, ActiveX is selected. This is the recommended viewer.

**Step 11** Click the **Save** button to save the parameters you've just configured for generating this report.

**Step 12** Click the **View Report** button and the report is automatically displayed in a new window.

You can use the Delete button to delete/remove the report entirely.

*Figure 11-11 Product Usage Report Page*




# Network Data Flows Report

Use this report type to view, by network service, the number of data flows (unique source/destination address combinations), the number of hosts acting as clients, and the number of hosts acting as servers. This data can be filtered by protocol,

source address set, and destination address set. You could use the results of this report to constrain a host's communication to only those hosts that it typically talks to.

**Note** Verbose network data collection must be enabled to gather data relevant to this report.

From the **Analysis>Application Deployment Investigation Reports** option, select a report type. In this case, click on **Network Data Flows** and do the following:

**Step 1** In the report window, click the **New** button to create a new report. This takes you to the report configuration view. See Figure 11-12.

**Step 2** Enter a **Name** and **Description** for the report.

**Step 3** Optionally, enable the **Verbose report** checkbox. If you do not enable this checkbox and you have selected to generate a report for <All Groups> and <All Hosts>, you will only see summary information displaying the overall number of data flows rather than data flows per host. If you enable Verbose report, you will see a much longer report containing details for hosts, source and destination addresses, protocols, and client/server connections.

Network Data Flows non-verbose reports contain the following data:

- Unique Protocol/port combinations, unique combination of Source IP address, Destination IP address (including address resolved to host name whenever possible), Number of incoming and outgoing connections between the source/destination combination in the specified time frame.

Network Data Flows verbose reports contain the following data:

- Local host, Local IP address, Local process name, Network operation, Peer host, Peer IP address, Number of network requests with the distinct combination of all items mentioned.

**Step 4** From the **Applications** list field, you can select one or more applications with which to filter this report. You can also select <All Applications> depending on the type of report you wish to generate.

**Step 5** From the **Local Groups matching** field, you can select a specific group for which to generate network data flow information. You can view information for <All Groups> or only for those you select. Optionally, use the **but not** field to exclude certain groups from those selected in the Groups matching field.

**Step 6** From the **Local Hosts matching** field, you can select hosts within the selected Group(s) for which to generate report information. You can view information for <All Hosts> or only for those you select by using the **but not** field to exclude certain hosts from those selected in the Hosts matching field. Using exclusions, you can generate a report for a specific host within a selected group.

**Step 7** From the list field, select a preconfigured **Peer Network Address Sets matching**. You can view information for <All Addresses> or only for those you select.

**Note** You can create a new Network Address Set or edit an existing one from this page by clicking the **New** link or by double-clicking an item in the selection field.

**Step 8** From the **Peer Groups matching** field, you can select a specific peer group for which to generate network data flow information. You can view information for <All Groups> or only for those you select.

**Step 9** From the **Peer Hosts matching** field, you can select a specific peer host for which to generate network data flow information. You can view information for <All Hosts> or only for those you select.

**Step 10** Optionally, enable the **Report also non-CSA host traffic (peer group/host filter is ignored)** checkbox. This will produce a much longer report and will ignore any peer settings you may have configured.

**Step 11** From the list field, select a preconfigured **Network Service**. You can view information for <All Ports> or only for those you select.

**Note** You can create a new Network Service or edit an existing one from this page by clicking the **New** link or by double-clicking an item in the selection field.

**Step 12** Enter a **Number of distinct peer hosts** by which to filter this report.

**Step 13** Enter a **Time Frame** by which to view the collected data.

You can enter **From** and **Until** time parameters using the syntax shown below or you can check the **All times** checkbox for all time frames.

Time syntax:

You can specify a relative time using any of the following terms: tomorrow, now, next, year, month, week, day, hour, minute, and second.

**Step 14** Select criteria by which to sort the report. You can sort by host, application, or peer address.

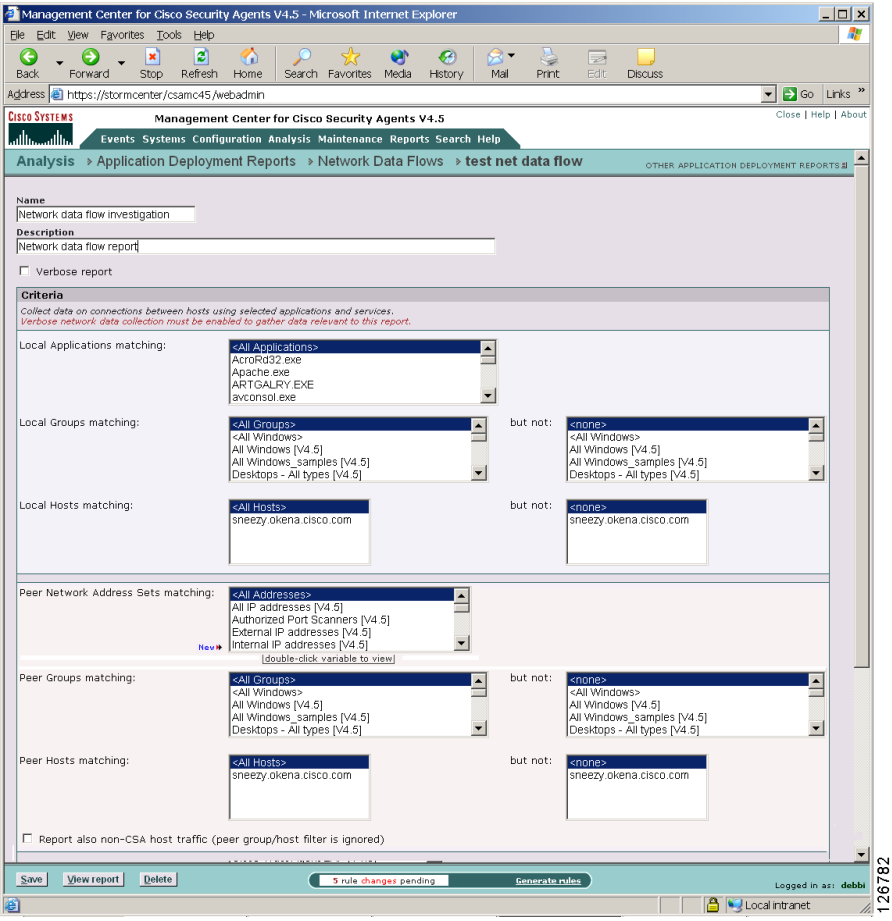
**Step 15** Select a **Viewer type**. By default, ActiveX is selected. This is the recommended viewer.

**Step 16** Click the **Save** button to save the parameters you've just configured for generating this report.

**Step 17** Click the **View Report** button and the report is automatically displayed in a new window.

You can use the Delete button to delete/remove the report entirely.

*Figure 11-12 Network Data Flow Report Page*




# Network Server Applications Report

This report is intended to break down network server application activity on a given set of hosts. You could use this report type to view which network server applications are listening on ports but not accepting any (or very few) connections. You could also use this to determine which are the most active web servers or database servers on your network.

From the **Analysis>Application Deployments Reports** option, select a report type. In this case, click on **Network Server Applications** and do the following:

**Step 1** In the report window, click the **New** button to create a new report. This takes you to the report configuration view. See Figure 11-13.

**Step 2** Enter a **Name** and **Description** for the report.

**Step 3** From the **Applications** list field, you can select one or more applications which hosts and or groups use to listen on the network. You can also select <All Applications> depending on the type of report you wish to generate.

**Step 4** From the **Groups matching** field, you can select a specific group for which to generate unused network application information. You can view information for <All Groups> or only for those you select. Optionally, use the **but not** field to exclude certain groups from those selected in the Groups matching field.

**Step 5** From the **Hosts matching** field, you can select hosts within the selected Group(s) for which to generate report information. You can view information for <All Hosts> or only for those you select by using the **but not** field to exclude certain hosts from those selected in the Hosts matching field. Using exclusions, you can generate a report for a specific host within a selected group.

**Step 6** Enter the **Maximum number of server ACCEPTs**. By default, this field has 10 entered. Use this number to find **more than** or **less than** the specified number of network listens with no or very few subsequent network connections.

**Step 7** Enter a **Time Frame** by which to view the collected data. This time indicates when the network listen/connection was seen on the system(s) in question.

You can enter **From** and **Until** time parameters using the syntax shown below or you can check the **All times** checkbox for all time frames.

Time syntax:

You can specify a relative time using any of the following terms: tomorrow, now, next, year, month, week, day, hour, minute, and second. Enter a specific time using any of the follow time formats: hh:mm:ss. If no meridian (AM or PM) is specified, hh is interpreted on a 24 hour clock (0-23). Note that entering minutes and/or seconds is optional.

**Step 8** Select criteria by which to sort the report. You can sort by port, host, or application.

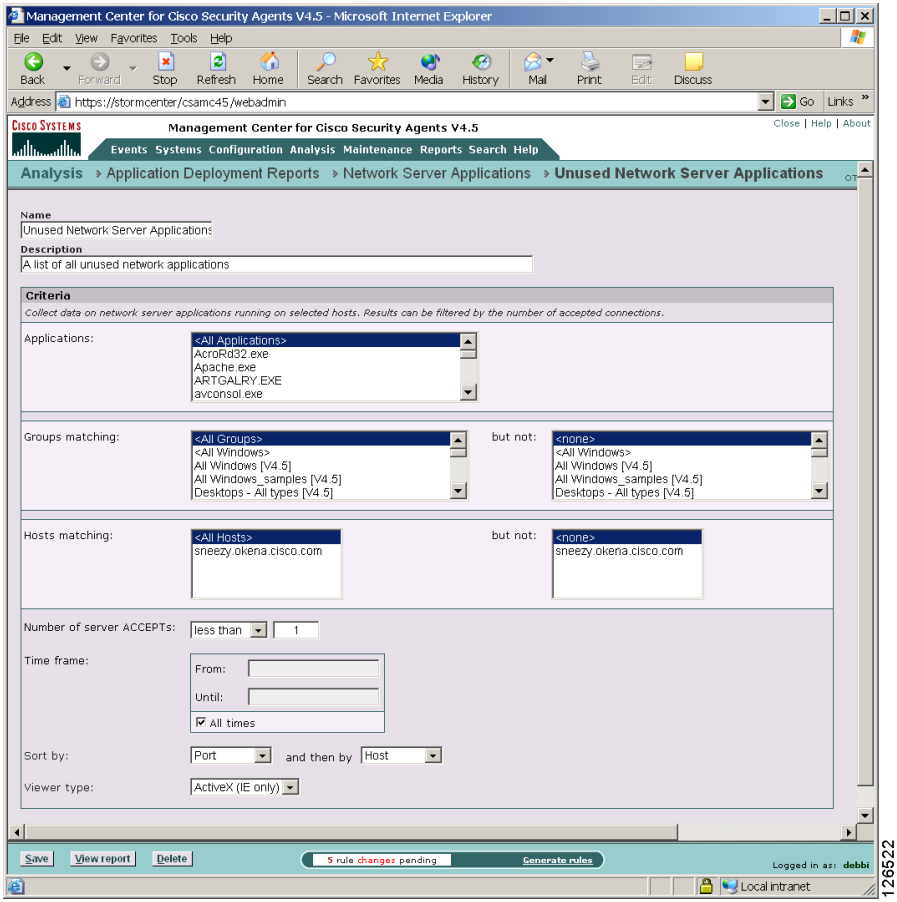
**Step 9** Select a **Viewer type**. By default, ActiveX is selected. This is the recommended viewer.

**Step 10** Click the **Save** button to save the parameters you've just configured for generating this report.

**Step 11** Click the **View Report** button and the report is automatically displayed in a new window.

You can use the Delete button to delete/remove the report entirely.

*Figure 11-13 Network Server Applications Report Page*




# Viewing Reports

When you generate your reports, you're given the option of selecting the type of viewer through which to display the report. From the Viewer type pulldown menu, you can select the following.

- ActiveX—The report viewer for ActiveX uses an ActiveX control that can be placed inside an HTML page and viewed through any browser that supports ActiveX. (Supported by Internet Explorer 3.02 and higher. Not supported by Netscape.)
- HTML Frame—Using this viewer, you can display reports in HTML using frames to illustrate category data in a left frame. (Supported by Internet Explorer 3.02 and higher and Netscape Navigator 4.7 and higher.) When you print reports, the formatting will vary depending on which view type you have selected and the printer settings on the printer you're using.

## Exporting Reports

When you export analysis reports, you are only exporting the report itself and the names of objects referenced in the report, such as a group or policy. The group, policy objects, and product mappings are not automatically exported with the report. There is no cascading inheritance when you export either reports or event sets as occurs when other items are exported. You must select groups, policies, and product mappings separately if you want to export them for the purpose of the report.

# What is Application Behavior Investigation

Cisco Security Agent Application Behavior Investigation works with CSA MC and the Cisco Security Agent, serving as a data analysis and policy creation tool for administrators who are deploying policies across systems and networks.

Because the rules that comprise CSA MC policies are application-centric, understanding the resources applications require for normal operations is integral to building effective policies. Behavior investigation does that by analyzing applications as they operate in a normal environment and generating useful reports and rule modules (rule module creation is a separately licensed feature) based on that analysis.

# How Application Behavior Investigation Works

When deployed on a system running a Cisco Security Agent, Application Behavior Investigation monitors the actions of designated applications on that system, logging all resource access attempts made by the application. It then analyzes the logging data it collects and develops detailed reports for the application in question. It also, optionally, generates a rule module. The generated rule module enforces what is determined to be normal application behavior while restricting all other behaviors. These other behaviors could now be construed as abnormal or suspicious based on the analysis.

**Note** If you are creating your own policies and not using Application Behavior Investigation, refer to Chapter 12, "Policy Definition Guidelines," for information.

# The Application Behavior Investigation Process

The application behavior investigation is performed by three different contributing components: CSA MC, the agent (logging agent), and the behavior investigation functionality.

- Through *CSA MC*, you designate which application you want to investigate. You also select an agent host on which the investigation is to take place and a time frame within which the investigation will be completed. This investigation configuration is then sent to the agent on the selected host in the same way policies are sent to agents.

  *Application Behavior Investigation* examines all the logged data it receives from the logging agent. When the analysis is complete, it creates a policy for the application and generates reports containing information on all resources accessed by the application. The policy enforces the normal operations seen in the log file and will deny any operation attempts by the application that do not align with this normal behavior.

- The *agent* receives the analysis configuration information when it next polls in to CSA MC. This agent now becomes the "logging agent" in this process. It logs all operations performed by the designated application. As this logging

takes place, it is assumed that the application is being thoroughly exercised in a normal operating environment. When the analysis is complete, the logged data is sent to the behavior investigation function for processing.

Optionally, CSA MC imports the rule module created by the behavior investigation.

# Behavior Analyses

By accessing the **Analysis>Application Behavior Investigation >Behavior Analyses(Windows or UNIX)** window, you can configure parameters for analyzing a particular application.

When you are ready to configure a behavior analysis for an application, you must have the following information:

- What application you want to analyze: You should have an appropriate application class configured for the analysis. (You can leverage existing application classes, but it is recommended that you analyze only one application at a time. See page 11-44 for more information.)
- Which host you want to select for application analysis: You should have an appropriate host chosen for the behavior analysis.

# Creating, Saving, and Cancelling Analysis Data

## Management Center Button Frame

Similar to most CSA MC windows, behavior analysis action items appear in a frame at the bottom of CSA MC.

**Note** The available buttons in the bottom frame change in accordance with the actions available for the page you're viewing. With a behavior analysis, several actions are performed from the same page as the behavior analysis progresses. You may have to refresh the behavior analysis page for the buttons to change appropriately.

Available buttons and links are as follows.

- New—Use the New button to create new a configuration item within the list view you have selected. Click the New button and a new item appears in the list view. Click the new item link to access the configuration view for that item.
- Delete—Use the Delete button in conjunction with the checkboxes beside each list view item. To delete a configuration, select its checkbox (you can select several at once) and click the Delete button. All checked items are deleted. To quickly select all checkboxes, click the very top checkbox in the list view heading bar. Clicking the Delete button then deletes all items.
- Clone—Use the Clone button in conjunction with the checkboxes beside each list view item. To clone a particular configuration, select its checkbox and click the Clone button. You can clone one item at a time. New links to the cloned configurations appear in the list view.

**Note** When you clone an item that contains variable items like application classes, the cloned item uses the same variables used in the original item. The variables themselves are not cloned.

- Save—When you enter configuration information, whether you are entering new data or editing existing data, you must click the Save button once you are finished to save your configuration in the CSA MC database. If you do not click Save before moving to another page in CSA MC, your data is lost.
- Stop Logging—If you want to stop the analysis early and send collected data to the workstation for analysis, click this Stop logging button.
- Start analysis—When the logging for the analysis is complete, a "Start analysis" button appears in the bottom frame of the behavior analysis page. Click this button to have the analysis workstation begin to analyze the logging data.
- Optional Import—When the analysis of the logging data is complete, the behavior analysis creates a rule module which you can import into CSA MC. The "Import" button appears when the rule module creation is complete if you have a license for Analysis rule module creation and import.

# Configure a Behavior Analysis Investigation

To configure a behavior analysis investigation, do the following:

**Note** In some cases, you can configure a behavior analysis investigation using the Event Management Wizard accessible from particular event log entries. See About the Event Management Wizard, page 8-14 for more information.

**Step 1** Move the mouse over **Analysis>Application Behavior Investigation** in the menu bar and select **Behavior Analyses (Windows or UNIX)** from the drop-down list that appears. The list of existing analyses (if any) is displayed.

**Step 2** Click the **New** button to create a new behavior analysis. This takes you the behavior analysis configuration page. (See Figure 11-14.)

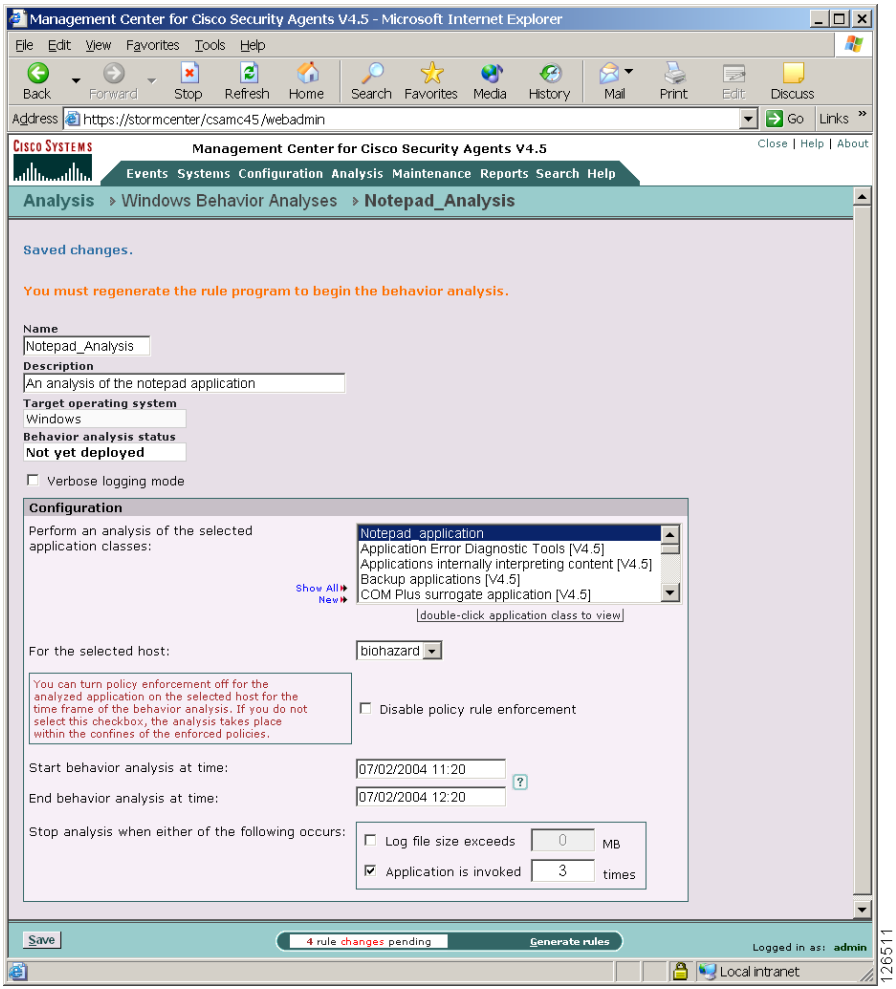
**Step 3** Enter a **Name** for the behavior analysis you are creating.

**Step 4** Enter a **Description** for your behavior analysis. This description becomes visible in the behavior analysis list view.

**Step 5** **Verbose logging mode**: By default, behavior analysis filters its logging process so that duplicate events are not logged. You can turn this feature off by selecting this checkbox. If you do turn this filtering off, your logs will be a great deal larger, but the advantage is that you will be able to see how often the same resource is accessed when you view the behavior analysis reports.

**Note** The **Target operating system** you selected is displayed in a read-only field. The **Behavior analysis status** field is also a read-only field. It displays text, informing you of each stage of the analysis. When you first configure your behavior analysis, it displays "Not yet deployed."

*Figure 11-14 Behavior Analysis Configuration Window*




**Step 6** In the **Perform an analysis of the selected application classes** list box, select the application class or classes you want to analyze. To select multiple items in a list box, hold down the **Ctrl** key as you select each item. To unselect a single item, hold down the Ctrl key when you click on the item in question. Press and hold the **Shift** key when you click on an item to select multiple successive items.

**Caution** You can select an application class that contains more than one application for the analysis. But in that case, the reports created would apply equally to all applications included in the analyzed application class. For example, if the application class you are analyzing contains both Microsoft Word and Microsoft Outlook, the reports created by the behavior analysis would be a combination of the resources required by both applications.

Next you must assign the behavior analysis to a specific host system.

**Step 7** Select the host you are assigning the behavior analysis to in the **For the selected host** list box. e.g. Note that you cannot have more than one behavior analysis running on a host at one time.

**Note** Once the behavior analysis begins, you can click the **Stop logging** button that appears in the bottom frame. The behavior analysis stops automatically according to the parameters you enter on this behavior analysis page. But if you want to stop the analysis early and send collected data to the workstation for analysis, click this Stop logging button.

**Step 8** Optionally, you can select to **Disable policy rule enforcement** for the time frame of the analysis. Otherwise, the analysis takes place only within the confines of enforced policies. Some events may be denied by rules and therefore the analysis may not be complete.

**Caution** If you select the Disable policy rule enforcement checkbox, when the logging agent receives a behavior analysis investigation, any policies relevant to the application being analyzed are disabled on the selected host until the analysis is completed. This may be undesired if the application in question is unknown or is in any way suspicious.

**Step 9** Next you must enter behavior analysis time frames.

- **Start behavior analysis at time**—From the pulldown options, select a time for the behavior analysis to start once the host polls in and receives the behavior analysis. If you specify no time here, "now" is automatically entered. This means the behavior analysis will start immediately when the host receives it.
- **End behavior analysis at time**—You must enter a time for the behavior analysis to end. The behavior analysis process will not allow you to save the analysis until you do. When you enter a *log size* parameter or an *application invocation number* in the fields below, they act as overrides of this end time.

  You can specify a relative time using any of the following terms: tomorrow, yesterday, today, now, last, this, next, ago, year, month, week, day, hour, minute. Enter a specific time using any of the following time formats: hh:mm:ss. If no meridian (AM or PM) is specified, hh is interpreted on a 24 hour clock (0-23). Note that entering minutes and/or seconds is optional. Enter a specific month and day with optional year in the formats: mm/dd?/yy, monthname dd, yy. The default year is the current year.

**Step 10** Stop behavior analysis when either of the following occurs:

- **Log file size exceeds __ MB**—You can enter a size restriction on the log file. When it reaches the size you indicate, the analysis is finished. (Note that the maximum log file size you can enter here is 256 MB. This is also the default value.)
- **Application is invoked __ times**:—You can specify an application invocation restriction. Once the application is invoked on the system the number of times you indicate, the analysis is finished.

**Caution** It is not always appropriate to use an invocation number limit. For example, for server applications, time frame parameters might be a more appropriate criteria for ending a behavior analysis.

**Note** If you enter analysis completion parameters in more than one field, the parameter that is reached first is the one that applies.

**Step 11** Click the **Save behavior analysis** button in the bottom frame of CSA MC to save it.

**Step 12** Once your behavior analysis is configured to your satisfaction, click the **Generate rules** link in the bottom frame and continue by clicking the subsequent **Generate** link to distribute the behavior analysis to the group hosts you've selected.

Depending on the behavior analysis parameters you've configured, the selected host will begin the behavior analysis after it polls in to CSA MC and receives the new rules.

**Note** Keep in mind that if you have configured your behavior analysis to begin immediately and your agents are configured to poll in to CSA MC once every hour, the behavior analysis will not begin until the agent next polls in. In this example case, that time frame could be up to one hour. Additionally, be careful not to designate the end time as a time frame that could occur before the agent polls in and receives the behavior analysis. In this case, the analysis will not run at all.

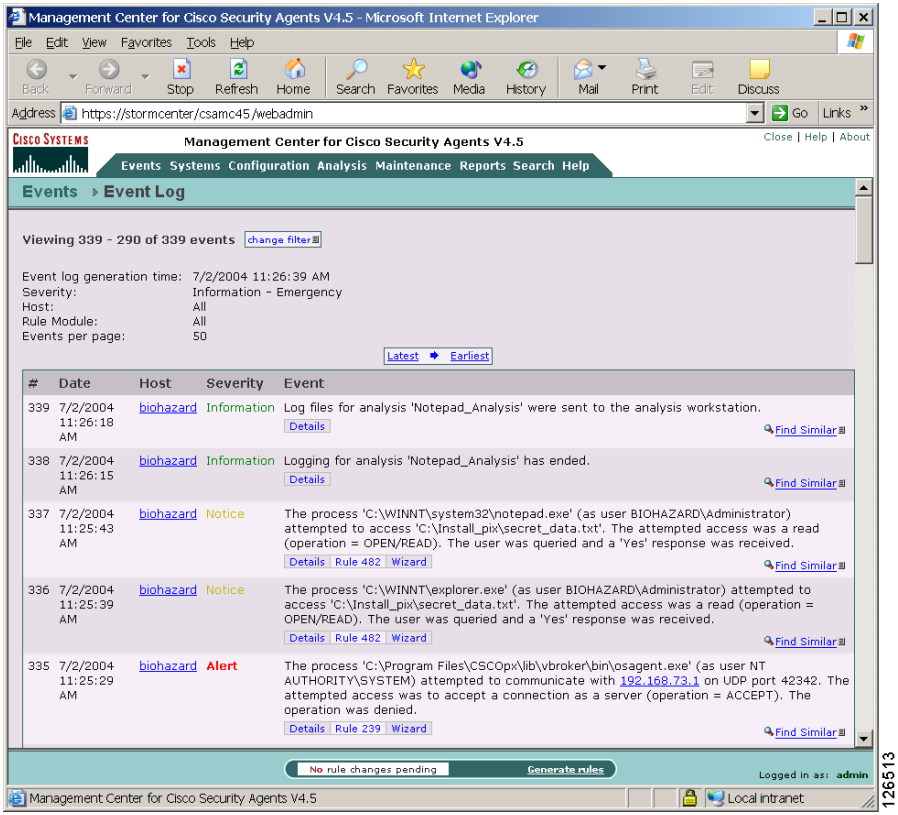
## Monitoring the Behavior Analysis

You can check your CSA MC **Event Log** to view the behavior analysis progression. An event is sent when the behavior analysis begins and again when it finishes.

You can also monitor **Progress Status** fields in the Behavior Analysis configuration page. These fields appear when the analysis is in progress. You can monitor the size of the log file and if you've set an application invocation limit, you can monitor the number of application innovations as well. These progress fields update each time the logging agent polls in to the MC.

When reports and the rule module are ready to be imported to CSA MC, an event log message appears indicating this.

*Figure 11-15 Behavior Event Log Messages*

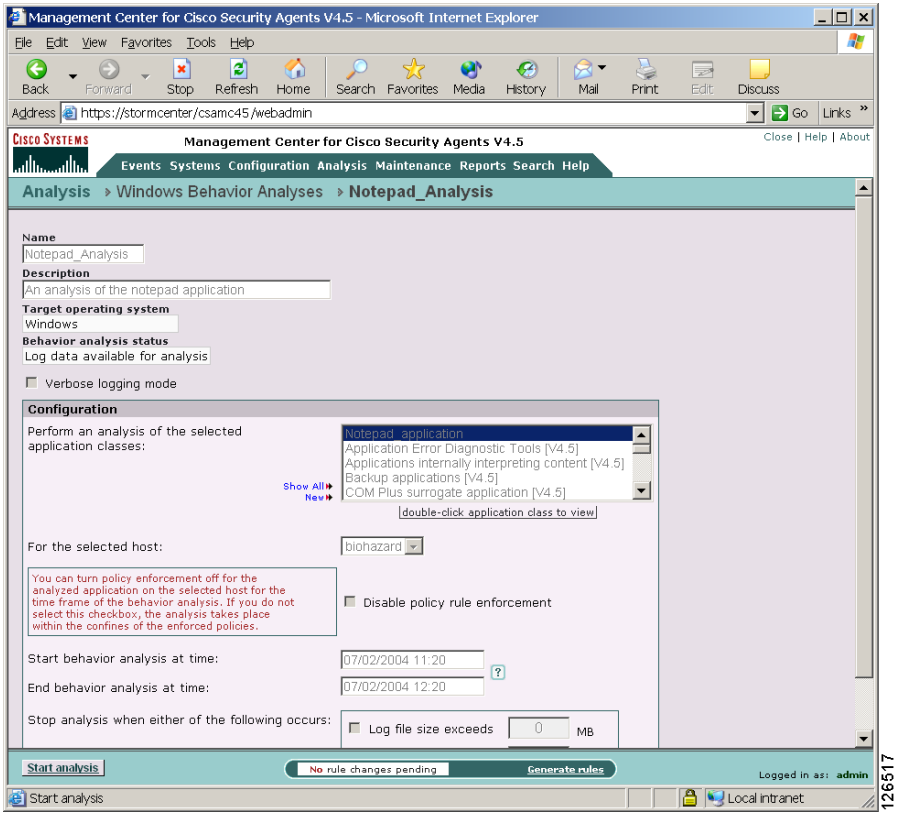



# Start Behavior Analysis

When the Event Log in CSA MC displays "Log files for behavior analysis were sent to the analysis workstation", you can begin the data analysis of the logging information.

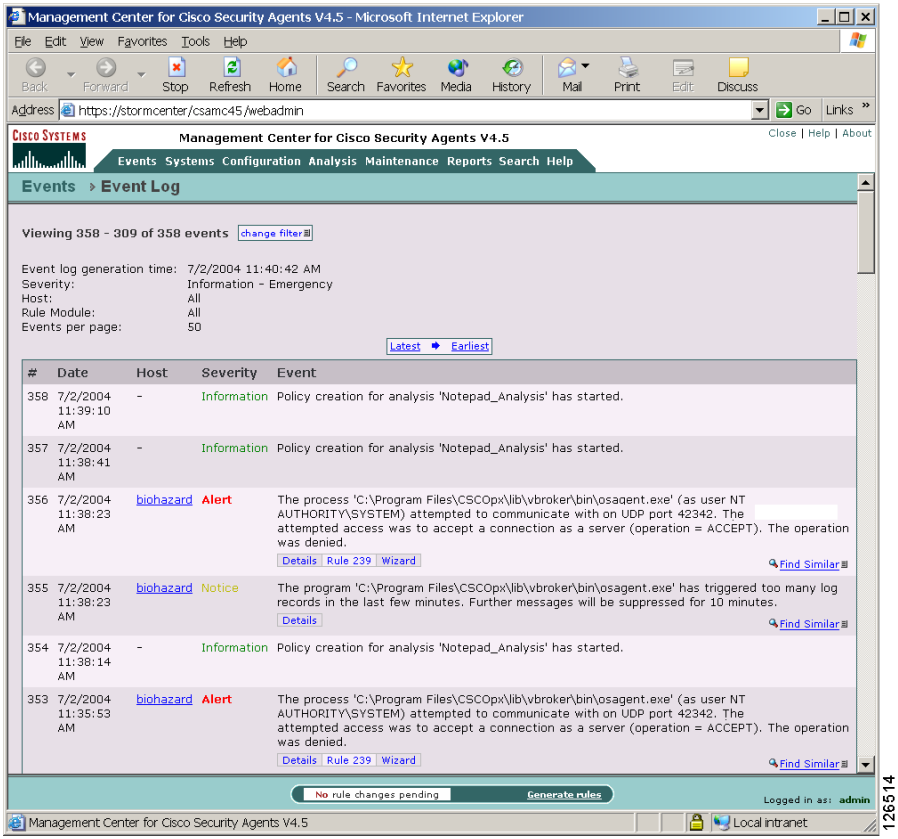
Begin this analysis by accessing the behavior analysis window for this particular analysis and clicking the **Start analysis** button in the bottom frame (see Figure 11-16). This begins the analysis. An Event Log message appears informing you that "Data analysis has started."

*Figure 11-16 Start Analysis of Logged Data*




- When the analysis is complete, you can “View reports”.
- If you have a license for rule module creation, when the analysis is complete, the Event Log file displays the message "Rule module creation for behavior analysis completed successfully". Once rule module creation is complete, you can import the module.

*Figure 11-17 Event Log Messages for Behavior Analysis Completion*



# Importing the Rule Module

**Note** If you do not have a separate license for importing behavior analysis rule modules, the behavior analysis results in report creation without the added step of creating a rule module.

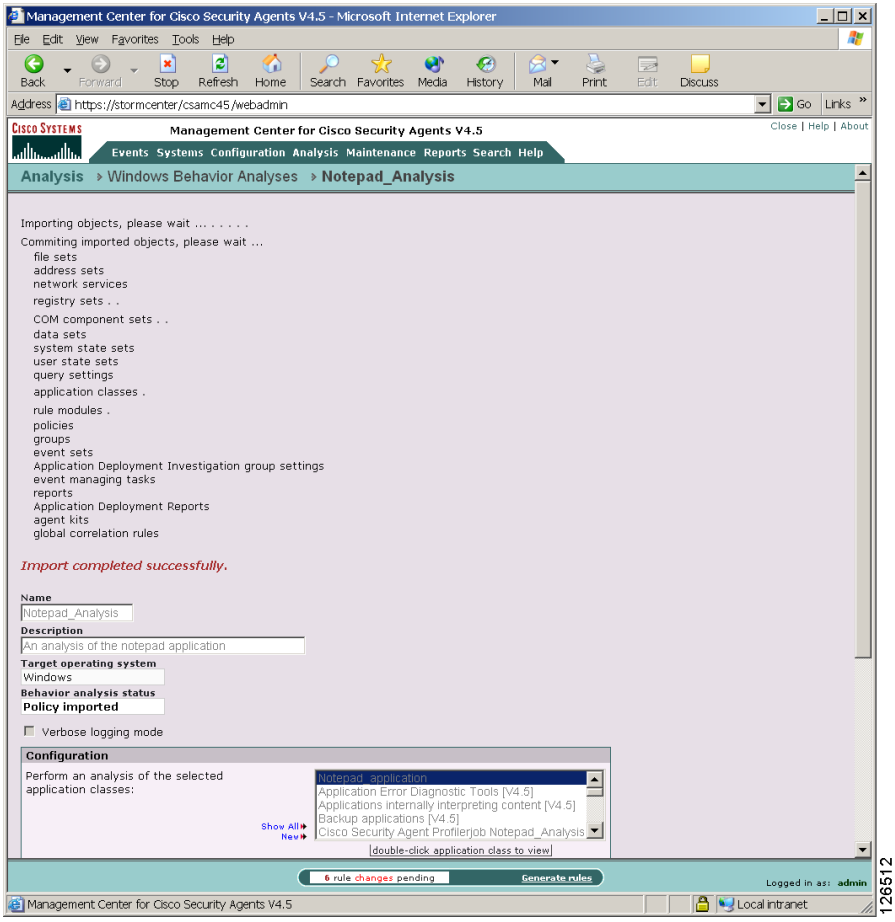
When the behavior analysis has completed its analysis of the logging data, the rule module it created is ready to be imported into CSA MC.

Import the rule module by once again accessing the behavior analysis window for this particular analysis. Click the **Import** button in the bottom frame. (This button only appears when the rule module is ready for importing.)

**Note** The rule module and its accompanying "variables" are imported into CSA MC. The behavior analysis creates its own variables for use in the rules it also creates. See Figure 11-18.

**Note** In order to deploy the rule module that the behavior analysis has created, you must associate it with an existing policy or with a new policy that you create. This policy must be attached to a group for the rules to be deployed to hosts.

*Figure 11-18 Import Process*

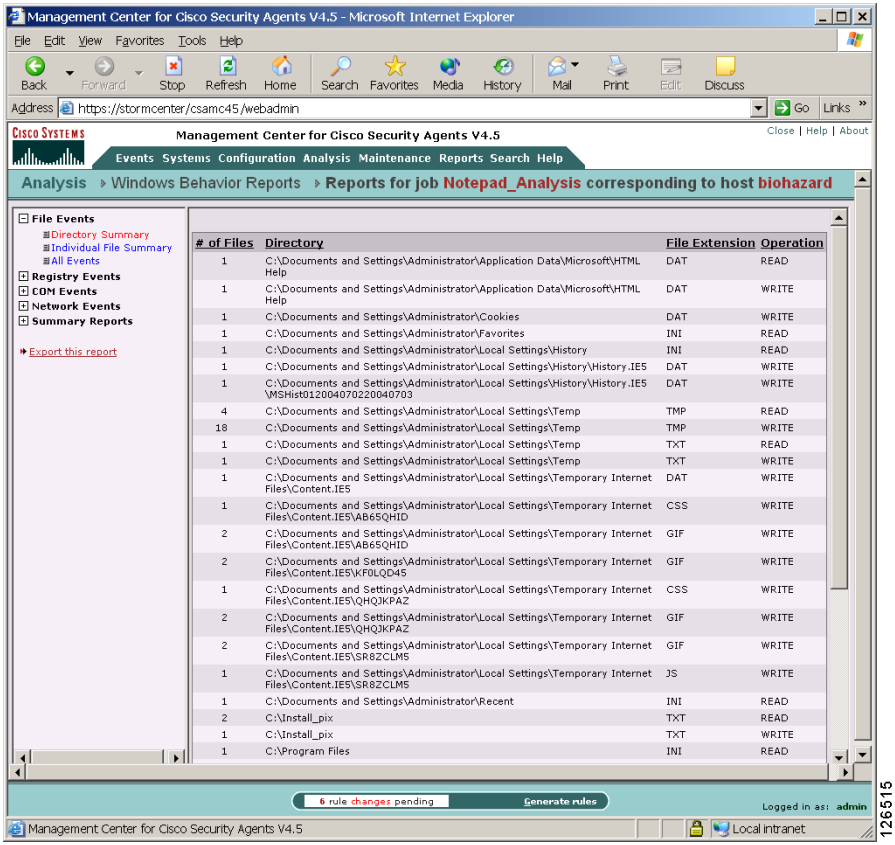


# Application Behavior Reports

During the analysis process, the behavior analysis sorts the logging data it receives from the logging agent into categorized reports. You can view these reports on the CSA MC system by accessing the **Analysis>Application Behavior Reports>Behavior Report(Windows or UNIX)**.

Reports on specific analyses only become available once the behavior analysis has successfully completed. The CSA MC Event Log displays a message to inform you that reports have been created.

***Figure 11-19 File Events Report***



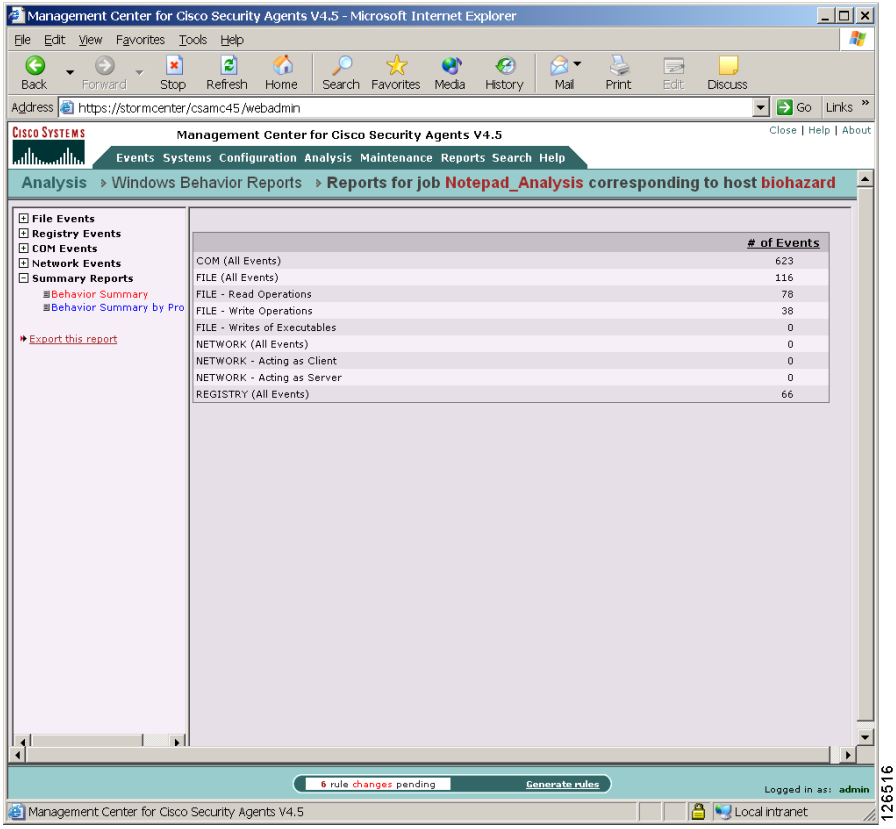
# Report Components

When you access the application behavior reports window, you can view individual reports for all completed analysis from the same window by selecting a particular behavior analysis from the **Reports for behavior investigation** pulldown list at the top of the window.

Reports are broken down into the system and network resource types that were accessed by the application during the behavior analysis logging session. Each report category has several sub-topics you can select from for organizing information.

Each category drop-down menu provides an overall summary view. This view displays all the data of that particular category which was accessed during the analysis time frame. If you select to view **Behavior Summary** for a report category (see Figure 11-20), additional views further sort the information the behavior analysis has collected by time frame, individual resource (e.g. single file or registry key), source and destination address in the case of network resources, and other criteria depending on the resource type in question.

*Figure 11-20 All Events Report Sorting*




Use the data from these reports to further refine your policies or to understand why particular rules were created for the policy.

You can view reports from the following categories:

## File Event Reports

File reports display information such as the name of the file accessed, the application accessing the file, and the operation performed on the file. More specifically, they provide:

- Time—Useful for determining the time frame between events.

- Directory—This is the directory location (local or network share) of the file resource accessed in the event.
- File type—This is the individual file accessed in the event.
- Operation—This is the operation (read, write) performed on the accessed file.
- Process name—This is the application that accessed the resource.
- Number of events—This is the number of times the event in question occurred during the logging period.

## Registry Event Reports (Windows only)

Registry reports provide details such as the name and value of the registry key that was accessed and the process that accessed it. More specifically, they provide:

- Time—Useful for determining the time frame between events.
- Key name—This is the name of the registry key accessed during the event.
- Value name—This is the registry value accessed during the event.
- PID—This is the process ID of the event. This is useful for distinguishing between different invocations of the same process.
- Process name—This is the application that accessed the resource.
- Number of events—This is the number of times the event in question occurred during the logging period.

## COM Event Reports (Windows only)

COM reports display information on the COM Class ID that was accessed and the process that made the request. More specifically, they provide:

- Time—Useful for determining the time frame between events.
- Object name—This is the unique identifier for the COM object accessed during the event.
- PID—This is the process ID of the event. This is useful for distinguishing between different invocations of the same process.
- Process name—This is the application that accessed the resource.
- Number of events—This is the number of times the event in question occurred during the logging period.

## Network Event Reports

Network reports display details such as the protocol accessing the network, the source and destination addresses of the connection, and the source and destination ports. More specifically, they provide:

- Time—Useful for determining the time frame between events.
- Role—This indicates whether the system in question was acting as a client or server during the network event.
- Protocol—This indicates whether this event was a TCP or UDP network connection.
- Source address—This is address where the connection originated from during the event.
- Source port—This is the port used during the event.
- Destination address—This is the destination address of the network connection for the event.
- Destination port—This is the destination port used for the connection. (Note that this port is used for the associated network rule that is generated as part of the policy.)
- PID—This is the process ID of the event. This is useful for distinguishing between different invocations of the same process.
- Process name—This is the application that accessed the resource.
- Number of events—This is the number of times the event in question occurred during the logging period.

## Summary Reports

Summary reports display the number of times each resource type was accessed during the logging time frame.

# Working with Reports

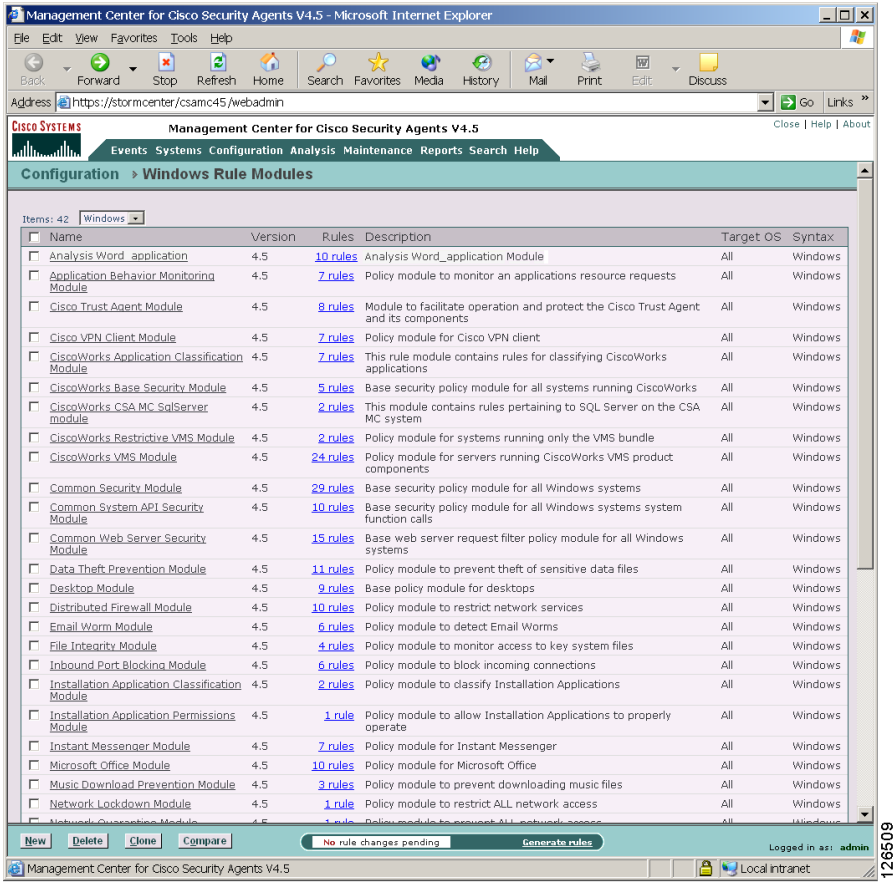
Behavior analysis reports contain a great deal of application information. You can search through this data using the browser window's own search capabilities. From the report page you want to search on, press and hold the **Ctrl** button and press the **F** key. The browser search window appears.

You can also highlight, copy and paste report text into an application such as Microsoft Excel. From Excel, you can then organize the data in any manner you choose.

# The Behavior Analysis Rule Module

Once imported, the behavior analysis rule module is added to your list of rule modules (Windows or UNIX) with the word "Analysis" appended to the original behavior analysis name. For example, if the analysis name is "Word_application", the name of the policy would be "Analysis Word_application Rule module."

***Figure 11-21 View the Rule Module***



# Reviewing the Rule Module

The rule modules created by the behavior analysis process enforce normal application behavior and maintain application and system integrity. To achieve this, the general strategy behind the creation of behavior analysis rule modules is to protect the application from the system and to protect the system from the application.

As with all new rule modules you create, you should review the rules generated by the behavior analysis and run the module in Test Mode for some period of time to ensure that it works as intended. You should also review the reports generated during the analysis as they are valuable resources for understanding the application as well as the rule module.

**Note** Behavior analysis does not add system hardening or global correlation "built-in" rules to the policy. For example, you can add System API control to the policy.

# Behavior Analysis Methodology

Protecting the application from the system

As part of the rule module, the behavior analysis creates file access control rules with the purpose of protecting the application data. These rules are left disabled by default as they restrict all other applications from accessing the analyzed application's data files. This is a fairly restrictive approach and, depending on the application itself, you may or may not want to enable these rules as part of the module.

Protecting the system from the application

Resources accessed by the application are broken down into file, network, registry, and COM categories and then rules for each category are created by the behavior analysis. Allow rules permit what was seen as normal application behavior while deny rules prevent access to all resources were not used by the application during the logging period.

Because security requirements may vary from site to site, the behavior analysis generates several rules that are disabled by default. The disabled rules are generally network and registry restrictions. The behavior analysis creates these rules but keeps them disabled, leaving it up to the administrator

to decide whether or not to impose these added restrictions. These rules are disabled by default because, generally, you should use the application-specific policies created by the behavior analysis in combination with the Sample Network (Permissive, Selective, and Restrictive) policies shipped with the CSA MC.

If you decide to edit behavior analysis rule modules based on your site's requirements, the reports generated during the logging analysis process contain information on all the resources accessed by the application during the logging period. The "summary" reports generated for each resource type are particularly useful in helping to pinpoint what resources my require more or less restrictive rules. (See Application Behavior Reports, page 11-52 for details.)

The general methodology behind the creation of rules for each resource type is as follows:

- File access control rules

  The behavior analysis creates file set variables that are combinations of file extension and directory pairs for accessed resources. These are used in allow file access control rules. It then creates a deny file access control rule that prevents access to all other files and directories.

  Use File Directory Summary and Individual File Summary reports to help refine these rules, if needed.

- COM component access control rules (Windows only)

  The behavior analysis creates COM component set variables which it then uses in a COM component access control rule to allow access to the required COM components. It then creates a COM component deny rule to deny all applications access to the COM components not used during the logging period.

  Use COM Object Summary reports to help refine these rules as needed.

- Registry access control rules (Windows only)

  The behavior analysis creates these rule types but disables them by default. Registry access control rules are very powerful system control tools. Restricting access to a required registry key could produce undesired results.

  The behavior analysis creates Registry Set variables based on the registry resources accessed during the logging period. These registry variables are broken into those that should be allowed and those that can be denied. Those allowed are registry keys accessed during the logging period. All others fall

in the deny range. This deny applies only to write access. All registry keys are still allowed read access. You can enable these rules, but you should understand the restrictions you are imposing.

Use Registry Key Summary reports to help refine these rules, if needed.

- Network access control rules

  The behavior analysis creates network access control rules but disables network deny rules by default. Network allow rules are created to allow network services for all addresses, both client and server, that were accessed during the logging period. The disabled deny rules then deny all services, client and server, on all ports for the analyzed application. These are fairly restrictive rules. If you intend to enable them or refine them (change port number restrictions or address information), you should refer to the Network Summary reports for information on network services used by the application.

## Variable and Application Class Creation

When the behavior analysis creates the rules for the rule module, it also creates all the registry and COM component variables required by the rules. All Windows files are entered as literals. (Note that UNIX files are grouped into sets.)

Additionally, the behavior analysis creates a new application class for the analyzed application and uses this new application class in all rules that make up the rule module. You should note that if you select more than one application class for the analysis, the application class created for the rule module is an aggregate of all the analyzed applications.

If you decide that the application is not dangerous and it can run without any rule module restrictions, you can begin to configure the behavior analysis.

CHAPTER 12

# Policy Definition Guidelines

## Overview

The policies you create on the Management Center for Cisco Security Agents should reflect a well-planned, enterprise-wide security policy. If your corporate enterprise already has security guidelines in place, the rules that form your policies should reflect those guidelines.

When you begin to configure policies, there is a common methodology you can use to successfully form the rules that will provide the security and the flexibility you require. This appendix provides a general approach you should take when creating your CSAMC policies.

This section contains the following topics.


- Analyzing Applications, page 12-2
- Configuring Policies—The Methodology, page 12-3
- General Server Policy, page 12-5
- Sample Web Server Policy, page 12-6
- Combined General Server and Sample Web Server Policies, page 12-8

# Analyzing Applications

The rule modules you create as part of your policies are application-centric. The application classes, those shipped with CSAMC and the ones you configure yourself, are the key to the rules you build as part of your security policies. Understanding how those applications work is necessary for configuring rules that adequately address the needs of a secure yet unobtrusive policy for that application.

There are three specific areas to consider when determining the type of security required by the application in question. There are overall *generic types of protection* that stop malicious code such as System API protection, Buffer overflow protection, and Port scan detection (Network shield rule). There are *application-specific types of protection* you can put in place to allow the application to operate normally while insulating it from any undesired access. Then there are *environment-specific types of protection* that control access to the application in question and its data over various network channels. It is the latter two, application-specific and environment-specific protection requirements, that this chapter concentrates on.

When analyzing an application for the purpose of writing a policy, consider the following questions.

- What resources does the application own (file, network, and registry resources)?
- Can the application access other resources?
- Can other applications access this application's resources?
- How is the application administered? (e.g. configuration tools used, accessed locally or remotely)
- Does the application interact with other applications as part of its normal operation?
- Does the application spawn processes and if so, what resources do those processes access?
- What application-based rules vs. environmental rules are necessary?

Determining the answers to these types of questions will help you target the resources you want to control as part of your policy for protecting the application.

For example, asking the questions above when analyzing how a Web server application operates would first lead you to determine which files are installed and used by the Web server application itself. What network resources are accessed and what registry keys are owned by the application? How is the Web server administered? Are html files FTP'ed to the server or is Front Page used locally on the system? These are questions targeted at producing application specific rules for a policy.

You would also note how the Web server is used and who can access it. Is it an intranet or Internet server? Does it act as a standalone server or does it access other resources? If there are forms users fill out on the Web server, does it use a backend SQL Server to store data? If so, which applications must be able to communicate with each other and what services, other than HTTP, are required for this communication? These are questions targeted at producing environment specific rules for a policy.

Ultimately, you want your policy to secure both the application and the environment it operates within.

# Configuring Policies—The Methodology

Once you understand how an application works, you can begin forming a policy to protect it. There are three general areas you want to address for each resource you are protecting. By addressing the security needs of these three areas, you can configure a well-formed policy to protect the resources you are targeting.

When building a policy to protect a designated resource, refer to the following steps to help you address each resource area.

**Step 1** Protect the application and its resources (binary files, directories, registry keys, etc.).

You must prevent writing to the application executables themselves. This maintains the integrity of the executable. The only time the executable should change is if you're upgrading the application.

This type of rule would prevent a Trojan from naming itself "Netscape.exe" to disguise itself as the real Netscape executable.

Restrict access to specified data by other applications. For server policies, you'll want to protect information in certain directories on the server in question, allowing restricted access to specific files and blocking all outside access to other files.

In order to correctly formulate this rule, you must examine what other applications (if any) need to access the application data. This type of rule would protect another application from retrieving sensitive data from a server, such as credit card information or a password file.

Restrict access to sensitive application-specific registry keys. You want to allow the specific application to write to its own registry keys, but prevent all other applications from writing to those registry keys.

**Step 2** Restrict the application processes. Understand what resources the application needs and write restrictions to lockdown the application and not compromise the system.

Dictate what the applications in question can and cannot do. Likely, you'll want specific applications to write only to their own file types. To restrict an application, you must look at the files the application needs to read from and write to and then restrict it to only those files. This type of rule would prevent a buffer overrun from compromising a running application, and damaging other components on the system.

When applications are invoked, they often spawn other processes as part of the action they are performing. It may be desirable to place different restrictions on spawned processes. Therefore, when you analyze an application in preparation for writing rules, CSA MC gives you the option of including or excluding child processes created by the original application. You can also restrict the child processes of an application and create a rule to address only those processes.

**Step 3** Provide permissions, as required, to allow the application to function.

For example, if an application requires network connectivity, you should specify what required network services must be enabled. Components that are "network visible" are especially vulnerable to attacks. It is important to control what these network-accessible applications (and their spawned processes) can do.

# General Server Policy

The General Server policy described here uses the applicable steps mentioned previously to secure common server resources. This is a generic server policy that can be applied to any server. Depending on the type of server you're protecting, you'll want to apply this General Server policy and then create an additional policy, which more specifically targets the resources you want protected, to augment this general one. Here is an overview of a General Server policy.

***Table 12-1 General Server Policy***

| Rule Type | Description |
|---|---|
| File access control | Allow, all applications read system dll's |
| Network access control | Deny, lockdown network access client |
| Network access control | Deny, lockdown network access server |
| File access control | Deny, protect system executables |
| Network shield | Detect network port scans, detect and protect against network SYN flood attacks |
| System API control | Detect and terminate potential application Trojans and viruses. |

Note that the rules in these tables are ordered (top to bottom) according to their priority. High priority deny rules take precedence over all others. Allow rules take precedence over deny rules. This General Server policy now locks down the server machine protecting the system directory and protecting network access.

# Sample Web Server Policy

Once you have a general server policy to protect basic server resources, you can write a policy that actually targets the resources used by the particular server application you want to protect. For the purposes of this example, the application is a Web server. The executable is "WEB.EXE."

This targeted server policy builds on the General-Server policy restrictions, allowing the services required for WEB.EXE to operate securely. Once we explain the components of this policy, we will combine both the General-Server and Sample Web Server policies and implement them together to provide the overall protection the Web server application requires.

*Table 12-2 Sample Web Server Policy*

| Rule Type | Description |
|---|---|
| File access control | High Priority Deny, protect Web server data |
| File access control | Allow, let WEB.EXE write to temp files and log files |
| Network access control | Allow, let WEB.EXE talk to network |
| File access control | Query user, protect Web server directories from others |
| Registry access control | Deny, protect sensitive Web server keys |
| File access control | Deny, prevent WEB.EXE all file write access |

Here is how the methodology detailed in the first section of this document was applied to the creation of this policy. The Description, appearing in italics below, given for each rule in the Web server policy table is listed here with the "methodology" step that applies to it.

**Step 1** Protect the application executables and data.

*Protect Web server directories from others*: Here we have denied all applications from writing to the directories that contain the Web server application executables. *Protect Web server data*: This rule prevents anyone from writing to html files and defacing web pages. *Protect sensitive Web server keys*: This would protect, for example, keys controlling user authentication settings.

**Step 2** Restrict the application processes.

For a general purpose policy, you want to protect the system from the application in question. Therefore, you can allow the application (ex. WEB.EXE) to read all system files, but restrict writes to system files. (If you are concerned about the application reading certain system files, you can restrict reads to those files specifically, if necessary.)

*Prevent WEB.EXE all file write access*: This rule denies the Web server application access to all files on the system.

*Let WEB.EXE write to temp files and log files*: This rule allows the Web server application to write to temp and log files used by the application.

Note that restricting access to a resource should always be done in the policy that owns that resource.

**Step 3** Provide permissions as required.

*Let the WEB.EXE talk to network*: This allows WEB.EXE to act as a server for the http service.

# Combined General Server and Sample Web Server Policies

To fully protect the Web server, we apply our base General-Server policy and our targeted Sample Web Server policy to the agent running on the Web server system. When applied to the Web server, the combined policies work as displayed in the table below (in order of rule precedence).

*Table 12-3 Combined Policies*

| Rule Type | Description |
|---|---|
| File access control | High Priority Deny, protect Web server data |
| File access control | Allow, let WEB.EXE write to temp files and log files |
| File access control | Allow, all applications read system dll's |
| Network access control | Allow, let WEB.EXE talk to network |
| File access control | Query user, protect Web server directories from others |
| Network access control | Deny, lockdown network access client |
| Network access control | Deny, lockdown network access server |
| Registry access control | Deny, protect sensitive Web server keys |
| File access control | Deny, prevent WEB.EXE all file write access |
| File access control | Deny, protect system executables |
| Network shield | Detect network port scans, detect and protect against network SYN flood attacks |
| System API control | Detect and terminate potential application Trojans viruses. |

## Reference

"Vulnerable applications" defined in various rules are network-aware applications. These application types are much more vulnerable than others. They are as follows:

- TCP and UDP servers and processes created by them are vulnerable because they are susceptible to buffer overflow attacks.

- Processes that read downloaded content are vulnerable because they may be interpreting and taking action based on downloaded data.
- Remote clients are applications running on another machine and are therefore vulnerable because CSA does not know what these applications are when they attempt to access resources.
- Removable media, in some cases, is categorized as vulnerable. This includes media accessed from CD-ROM, floppy, USB drives, or any other peripheral device.

CHAPTER 13

# Third Party Product Integration

## Overview

The Management Center for Cisco Security Agents provides integration with other third party products. This section provides information on supported third party integration applications.

In most cases, you are referred to the third party documentation for configuration information.

This section contains the following topics.


- Cisco VPN Client Support, page 13-2
- Cisco Security Monitor Integration Support, page 13-2
- netForensics Integration Support, page 13-2
- Check Point™ OPSEC™ Integration, page 13-3
- Configuration Prerequisites, page 13-3
- Integration Configuration, page 13-4

# Cisco VPN Client Support

The Cisco Security Agent is a supported configuration for the "Are You There?" feature of the Cisco VPN Client, Release 4.0. For configuration details, please refer to Chapter 1 of the Cisco VPN Client Administrator Guide, in the section entitled "Configuring VPN Client Firewall Policy -- Windows Only."

# Cisco Security Monitor Integration Support

Cisco Security Monitor is a Security Information Management application that can receive security events from multiple devices. Security Monitor presents the information in a real-time, web-based console so that these events can be managed across the network. Security Monitor also provides event notification, event reporting, and event correlation.

To integrate events generated by the Cisco Security Agent with the Security Monitor application, refer to Chapter 3 of your Security Monitor documentation, “Configuring Devices to Monitor.”

# netForensics Integration Support

netForensics is a Security Information Management application that can receive security events from multiple devices. This gives the administrator the convenience of having a single point from which to manage events from heterogeneous sources. netForensics presents the information in a real-time, web-based console so that these events can be managed across the network.

To integrate events generated by the Cisco Security Agent with the netForensics application, refer to your netForensics documentation.

# Check Point™ OPSEC™ Integration

The Check Point™ OPSEC™ (Open Platform for Security) provides a set of API's (Application Programming Interfaces) which allow integration of various network security components. The SCV (Secure Configuration Verification) API provides a mechanism by which the configuration of a machine running the VPN-1® SecureClient™ can be verified.

With its Cisco Security Agent product, Cisco provides an "SCV Check" which can be used to verify that the agent is running on machines connecting via the VPN-1 SecureClient. With such a configuration, machines which fail the "SCV Check" are not allowed to establish connections through the Firewall.

## Configuration Prerequisites

The following components are required to integrate the Cisco Security Agent as an SCV check within the OPSEC framework:

- On Machine A, an installation of Management Center for Cisco Security Agents, version 4.0 or greater.
- On Machine B, an installation of the Check Point VPN-1& Firewall-1®, along with the Management Client and Policy Server, all of which are components of Check Point NG FP1 (Next Generation Feature Pack 1). The Firewall should be configured for VPN-1 SecureClient use.
- On Machine C, an installation of the Check Point VPN-1 SecureClient which points to the Firewall on Machine B. Also on Machine C, an installation of the Cisco Security Agent, installed from the Management Center for Cisco Security Agents on Machine A. (See the *Caution* below.)

**Caution** On Machine C, it is important that you install the SecureClient software before you install the Cisco Security Agent.

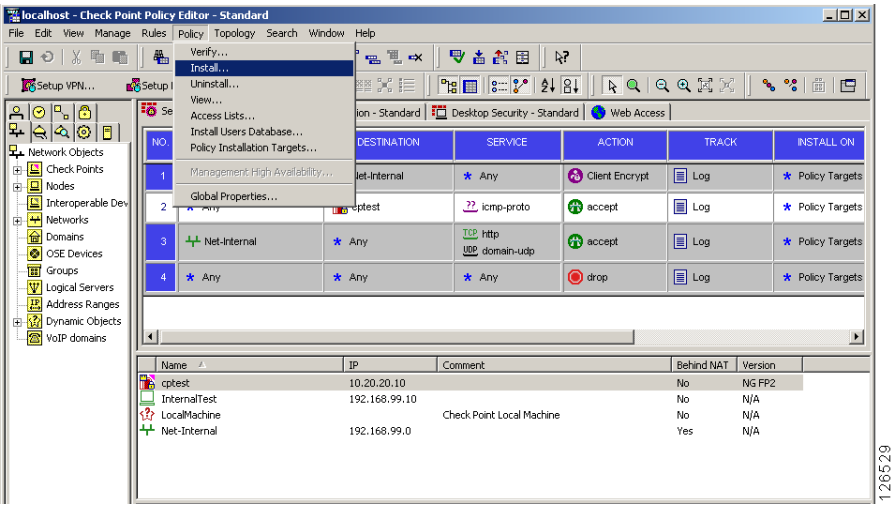
# Integration Configuration

This section provides the procedure for deploying the SCV check. The following instructions assume the existence of (and refer to) the prerequisites described in the previous section. These instructions also refer to a file called `LOCAL.SCV`, which is accessible from the self-extracting executable located `ThirdParty\OpSec\SCV.exe` on the CSA MC product CD.

**Step 1** On Machine B, copy the `LOCAL.SCV` file from the CD to the `\winnt\fw1\ng\conf` directory. Note that any pre-existing versions of LOCAL.SCV should be renamed so that they are not overwritten.

**Step 2** Using the Check Point™ Policy Editor, perform a Policy->Install onto Machine C and on to any other SecureClient machines for which the SCV check "CSAgent" is to be enforced. (Configuration for enforcing SCV checks varies across Check Point™ Feature Packs. Please refer to the "Desktop Security Guide" for VPN-1 and SecureClient configuration details.)

***Figure 13-1 Check Point Policy Editor***




**Step 3** On Machine C (and other relevant SecureClient machines), the new policy will automatically be downloaded.
With the SCV check now enforced, only machines with an installed (and running)

Cisco Security Agents are allowed to establish connections through the Firewall. Otherwise, the user receives a message box stating “Cisco Security Agent SCV Check Failed.”

**Note** No configuration is required on the client side. The Cisco Security Agent installation automatically installs and registers the relevant files.


# Cisco Security Agent Overview

## Overview

This chapter describes the agent and provides information on the agent user interface. 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 provide end users with an advanced UI that allows them to control their security settings and to use other added features.

If you have configured Query User rules, users should know how to respond to query pop-up boxes. This information and additional advanced UI configuration information is included in the Help provided with the agent user interface. You may want to refer end users to this agent help.

This section contains the following topics.


- Downloading and Installing, page A-2
- Network Shim Optional, page A-7
- The Agent User Interface, page A-10
- Turn Agent Security Off, page A-22
- Installing Software Updates on Agents, page A-23
- Installing the Solaris Agent, page A-24
- UNIX Agent csactl Utility, page A-27

- Installing the Linux Agent, page A-29

# Downloading and Installing

Once you build an agent kit on CSA MC, you deliver the generated URL, via email for example, to end users so that they can download and install the Cisco Security Agent. They access the URL to download and then install the kit. This is the recommended method of agent kit distribution.

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

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

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

End users must have administrator privileges on their systems to install the agent. Systems to which agents are installed must meet the following requirements:

*Table A-1 Agent Requirements (Windows)*

| System Component | Requirement |
|---|---|
| Processor | Intel Pentium 200 MHz or higher<br>**Note** Uni-processor, dual processor, and quad processor systems are supported. |
| Operating Systems | • Windows Server 2003 (Standard, Enterprise, Web, or Small Business Editions)<br>• Windows XP (Professional or Home Edition) with Service Pack 0, 1, or 2<br>• Windows 2000 (Professional, Server or Advanced Server) with Service Pack 0, 1, 2, 3, or 4<br>• Windows NT (Workstation, Server or Enterprise Server) with Service Pack 6a<br>• All Windows, Internet Explorer 4.0 or higher required.<br>**Note** Citrix Metaframe and Citrix XP are supported. Terminal Services are supported on Windows XP and Windows 2000 (Terminal Services are not supported on Windows NT.)<br>Supported language versions are as follows:<br>• For Windows 2003, XP, and 2000, all language versions, except Arabic and Hebrew, are supported.<br>• For Windows NT, US English is the only supported language version. |
| Memory | 128 minimum—all supported Windows platforms |

| System Component | Requirement |
|---|---|
| Hard Drive Space | 15 MB or higher<br>**Note** This included program and data. |
| Network | Ethernet or Dial up<br>**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 and UNIX platforms.

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

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

*Table A-2 Agent Requirements (Solaris)*

| System Component | Requirement |
|---|---|
| Processor | UltraSPARC 400 MHz or higher<br>**Note** Uni-processor, dual processor, and quad processor systems are supported. |
| Operating Systems | Solaris 8, 64 bit 12/02 Edition or higher (This corresponds to kernel Generic_108528-18 or higher.)<br>**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<br>**Note** This includes program and data. |
| Network | Ethernet<br>**Note** Maximum of 64 IP addresses supported on a system. |

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

*Table A-3 Agent Requirements (Linux)*

| System Component | Requirement |
|---|---|
| Processor | 500 MHz or faster x86 processor<br>**Note** Uni-processor, dual processor, and quad processor systems are supported. |
| Operating Systems | RedHat Enterprise Linux 3.0 WS, ES, or AS |
| Memory | 256 MB minimum |
| Hard Drive Space | 15 MB or higher<br>**Note** This includes program and data. |
| Network | Ethernet<br>**Note** Maximum of 64 IP addresses supported on a system. |

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

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

# Network Shim Optional

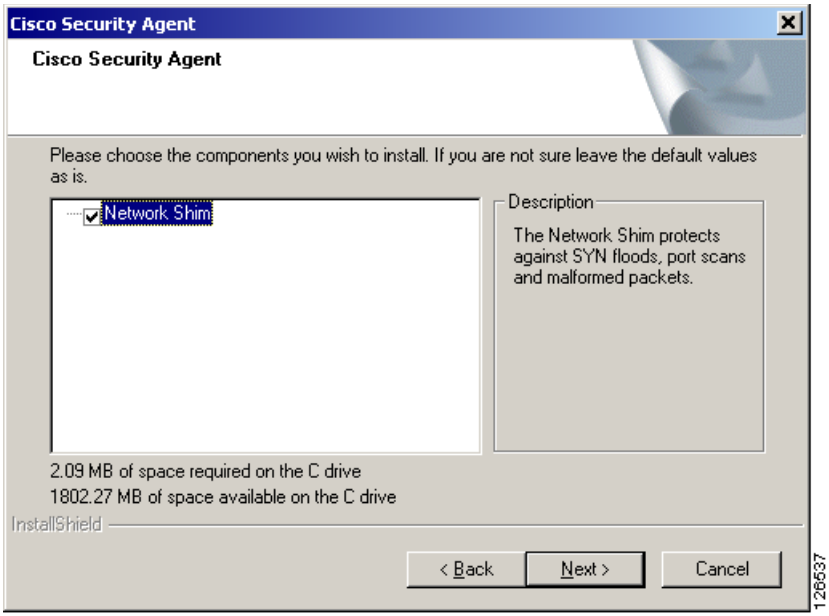
In some circumstances, you may not want users to enable the network shim on their Windows systems as part of the agent installation. (Note that the network shim is not optional on UNIX systems.) For example, if users have VPN software or a personal firewall installed on their systems, the network shim's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

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

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

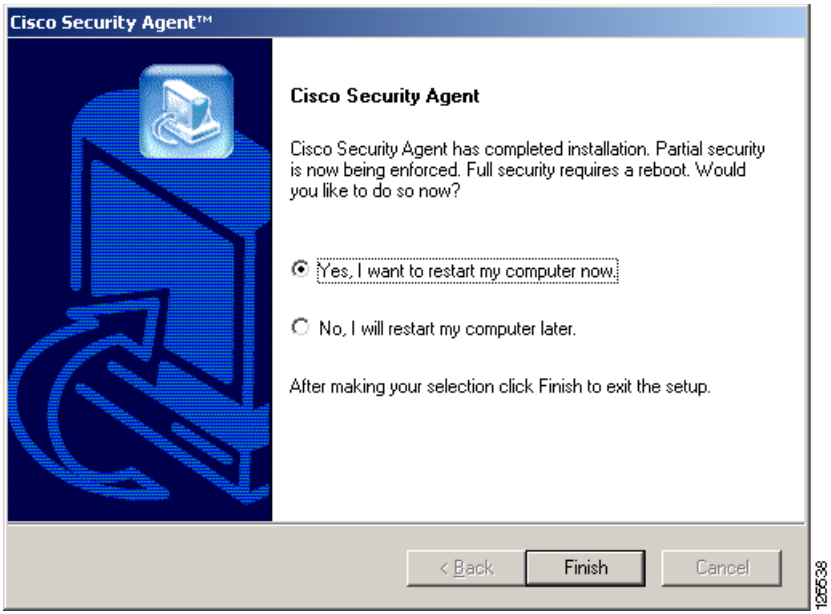
**Note** Not enabling the network shim does not mean that Network Access Control rules won't work. It only means that the system hardening features mentioned in the previous paragraph are not enabled.

*Figure A-1 Optional Network Shim*




Once users install agents on their systems, they can optionally perform a reboot (if Automatic reboot is not selected at kit creation time). 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*




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

Windows agents

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

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

- Network access control rules only apply to new socket connections. Network server services should be stopped and restarted for full network access control security without a system reboot.
- Buffer overflow protection is only enforced for new processes.

- File access control rules only apply to newly opened files.
- Data access control rules are not applied until the web server service is restarted.

At this time, 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. Agents are now ready to receive policies.

# The Agent User Interface

**Note** The Cisco Security Agent user interface does not run on Solaris systems. The Solaris agent has a utility (csactl) to provide some of the capabilities that the Windows and Linux agents provide in their user interface. See UNIX Agent csactl Utility, page A-27 for details. The Cisco Security Agent user interface appearance and functionality is the same on all Windows and Linux platforms.

As the administrator, you decide which agent UI options to provide to the end user. These options are controlled by the Agent UI control rule. See Agent UI Control, page 4-48. Available options are as follows:

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

- **Allow user access to agent configuration and contact information**—Selecting this checkbox in the Agent UI control rule provides Status, Messages, and Contact Information features, including the ability to manually poll the MC. It also provides the User Query Responses window.
- **Allow user to modify agent security settings**—Selecting this checkbox in the Agent UI control rule provides System Security and Untrusted Applications features.
- **Allow user to modify agent personal firewall settings**—Selecting this checkbox in the Agent UI control rule provides Local Firewall Settings and File Protection features. (If you select this checkbox, you are providing the end user with controls that you have limited access to. Firewall queries and other information will not log the CSA MC event log.)

To open the agent user interface, users can double-click on the agent icon in their system trays. The user interface opens on their desktop. The options available in the agent UI depend upon the features selected in the Agent UI control rule governing the agent in question. All possible agent features are described here.

**Status**

- The host name of the machine on which this agent is installed.
- 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 in to 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.
- If users have the Cisco Trust Agent installed and are using Network Admission Control, the Network Admission Control posture result for the agent is displayed on the UI. For example, it may display the status as Healthy, Quarantine, Infected, etc.
- When the end user clicks the **Poll** button, it forces the agent to poll the management center immediately rather than waiting for the configured time interval to trigger a poll. This way, the agent receives any rule changes right away.
- **Reset Cisco Security Agent**

This setting is available from the Start>Programs>Cisco Security Agent>Reset Cisco Security Agent menu on Windows systems and the System Menu>Cisco Security Agent menu on Linux systems where the agent is installed. Selecting the "Reset Cisco Security Agent" option puts all agent settings back to their original states and clears almost all other user-configured settings. This does not clear configured Firewall Settings or File Protection settings. But if these features are enabled, they are disabled as this is the default factory setting. The information entered into the edit boxes for these features is not lost.

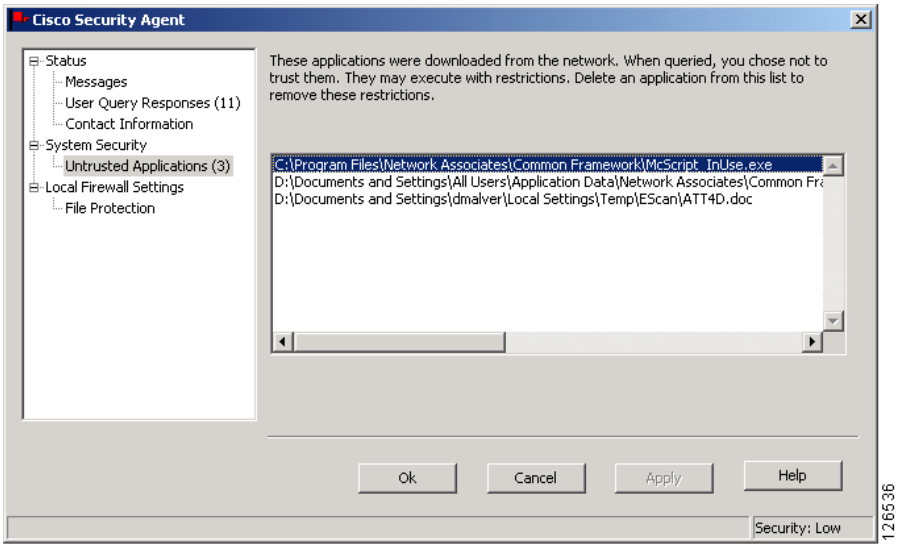
- **Cisco Security Agent Diagnostics (collecting troubleshooting data)**

  This utility is available (for Windows agents only) from the Start>Programs>Cisco Security Agent>Cisco Security Agent Diagnostics menu on systems where the agent is installed. Selecting "Cisco Security Agent Diagnostics" causes the agent to gather self-describing diagnostic information on the system and on the agent itself (e.g. information pertaining to any configured system states). Generally, users should only select this if you (the administrator) has requested that they do so. It may take some time to collect this data.

  This diagnostic utility temporarily disables agent security while it executes. If queried to disable agent security, the end user should response "Yes," to allow the diagnostic to occur. Security is automatically re-enabled when the utility finishes collecting data.

  When the collection is complete, a message appears informing users that a "csa-diagnostics.zip" file has been created in the `Cisco Systems\CSAgent\log` directory. Users can then send this file to you.

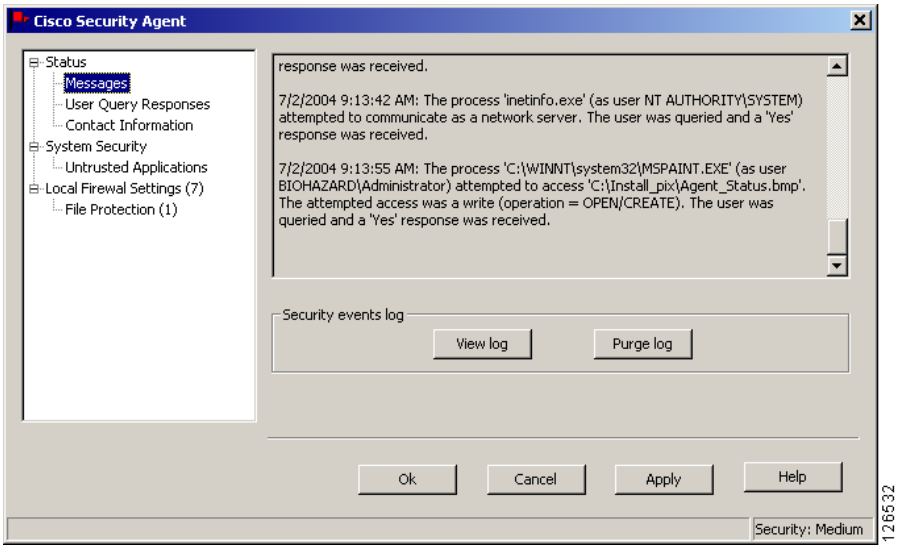
*Figure A-3 Agent Status Screen*




## Messages

When an agent denies a system action, a message informing the user of this event is placed in the Messages field. The user can click Messages in the left pane to view these events. Also note that the user can click the View log button to launch a text file containing all security events that have occurred on the system. This text file presents more detailed information on system events that have been logged by the agent. Click the Purge Log button to clear the text log file (if it begins to grow too large and takes up too much disk space). Note that the Purge Log file feature does not clear the messages viewable in the Messages field. It clears the log text file.

*Figure A-4 Agent Messages Screen*




## User Query Responses

When users respond to queries, the agent can remember their responses permanently or temporarily. This way, if the same query is triggered again, the action is allowed, denied, or terminated based on what was answered previously with no pop-up query box appearing again either permanently or for some period of time. In order to reduce the number queries users must respond to, it is generally advantageous, when possible, to permanently remember query responses.

It is the Don't ask again checkbox available from the Query Settings page in the MC that controls whether the end user has the ability to have a query response remembered permanently. As the administrator, you decide whether or not users have the option to choose Don't ask again. If user queries do not include a Don’t ask again option and responses are only cached temporarily (for approximately an hour) users can click the Clear button in the agent Query User Responses window to delete all temporarily cached responses.

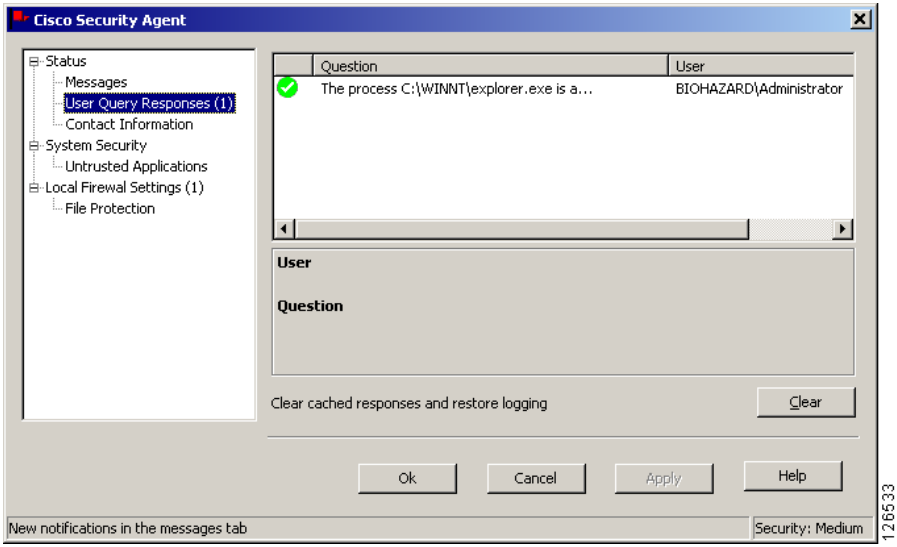
**Note** For a Query setting, the response to the query is relevant to the question, not to the resource. For example, if a File access control rule queries the user for a response and that identical query is also configured for a Network access control

rule, the user is not queried again when the Network access control rule triggers. The query response from the previous File access control rule is automatically taken.)

To clear permanent responses listed in the agent Query User Responses window edit field, users select the response in the edit field and press the Delete key. Permanent responses are remembered across reboots. Temporarily cached responses are not remembered across reboots.

Note that query response is tied to the user who responded. On multi-user machines, multiple users may be asked the same question.

***Figure A-5 Agent User Query Responses Screen***



### Contact Information

This window allows users to enter their contact information including name, telephone number, location, and email address.

### System Security

This window provides users with a security slide bar. The Low, Medium, and High security levels allow users to select an administratively defined security policy. Each setting maps to a specified system state configured on the central management center. If you have not defined different levels of security states for agents, when users move the slidebar between security levels, it will not alter their agent security. Note that in all cases, whether you have states defined for all security levels or not, if you permit end users to turn off agent security, when the slidebar is moved to the Off setting, it will disable all agent security.

Here are some examples of how you might define various security states to correspond to specific security levels:

- Configure a system state and a corresponding policy that applies when the agent security level is set to High. This security setting may cause the agent to detect a wide range of both known attacks and potential attack behavior. With high security enabled, these actions could be automatically denied when they are detected rather than giving the user the option of allowing them via a query user pop-up box (as might be available in lower settings).
- Configure a system state and a corresponding policy that applies when the agent security level is set to Medium. A Medium security setting may cause the agent to detect a wide range of attacks similar to those detected at the high setting. But this level might cause the user to be presented with more query pop-up boxes to ensure that the action taking place is intended and not a type of attack.
- Configure a system state and a corresponding policy that applies when the agent security level is set to low. A Low security setting may cause the agent to detect the more commonly known attacks that are easily distinguished from normal system behavior. In most cases, the user could be queried as to whether the detected action should be allowed or not.

#### Network Lock

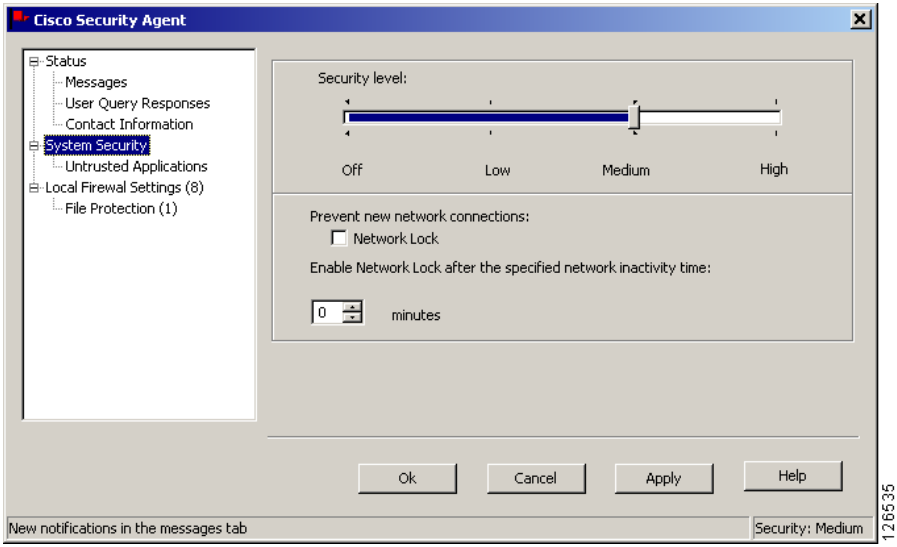
Users can select the Network Lock checkbox from the System Security window. When the Network Lock checkbox is enabled, the agent will not allow any new network connections until the lock is disabled. Alternatively,

users can set a time frame of 0-60 minutes of network access inactivity before the agent automatically enforces a network lock on the system. When that time frame is reached, the Network Lock checkbox is automatically selected by the agent itself. Users must unselect the checkbox to turn it off again. When a network lock is enforced on the system, existing network connections are not lost, but no new connections (in or out) are allowed.

If the Network Lock is enabled when users reboot the system, Network Lock is no longer turned on after the reboot. (All other agent settings. except temporary query response caching, remain constant across reboots.)

**Note** A **Resume** button may appear in this agent window. See Installation Applications Policy, page 5-19 for information on the Resume button.

***Figure A-6 Agent System Security Screen***



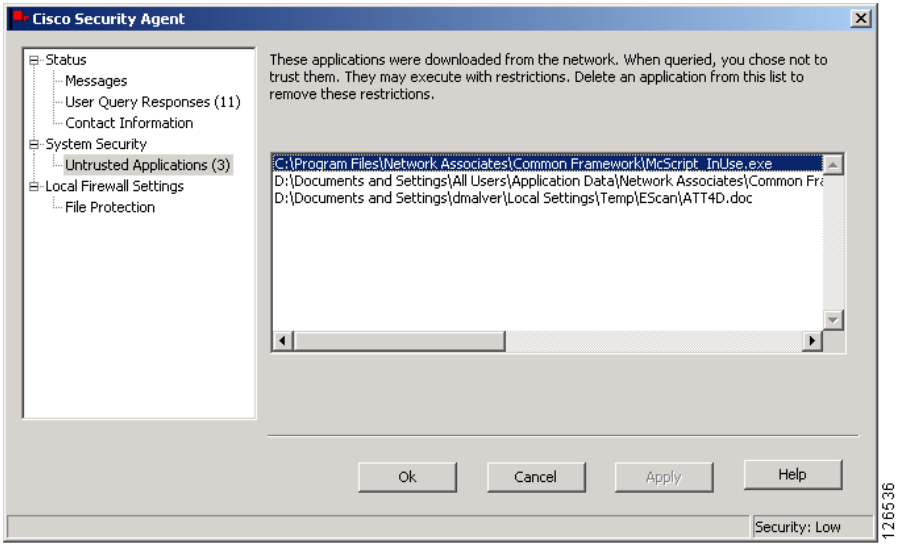

## Untrusted Applications

Applications that have read downloaded content from the network are generally considered to be more vulnerable than other application types. The central management center and the agent keep track of applications and file types that read downloaded content and place this information in the Untrusted Applications edit box. Applications and files listed there can

continue to operate under restrictions. Therefore, being listed as an untrusted application is a result of management center definitions and agent actions (query responses, for example). But the consequences of being labeled an untrusted application are defined by the management center. The management center imposes the appropriate restrictions. For example, untrusted applications cannot write to registry keys that are typically targeted by viruses and it cannot write to system executables.

If users want to remove a file or program from the list of untrusted applications, from the Untrusted Applications window, select the entry in question in the edit box and press the Delete key.

***Figure A-7 Agent Untrusted Applications Screen***




## Local Firewall Settings

You can enable these firewall settings on the agent UI to allow end users to control which applications have security permissions on their systems and what those permissions are. This feature allows local control but the centrally defined policy assigned by you must also allow for it. Settings defined here must pass both local and central permissions in order to work. Firewall setting permissions are assigned locally when end users are queried as to whether or not the application in question can access the network. These permissions can also be assigned during a learning mode period. Also note,

that this feature is intended for interactive workstations as opposed to servers which should only be managed by a central policy. If this feature is present, users must select the Enable checkbox to turn on firewall settings.

Users can see what permissions have been assigned to specific applications based on the graphic that appears beside the application name in the edit box. If there is no graphic present for an application, that network permission type has not yet been assigned. If users want to change the assigned permissions of a given application, they can select it in the edit box and press the Delete key.

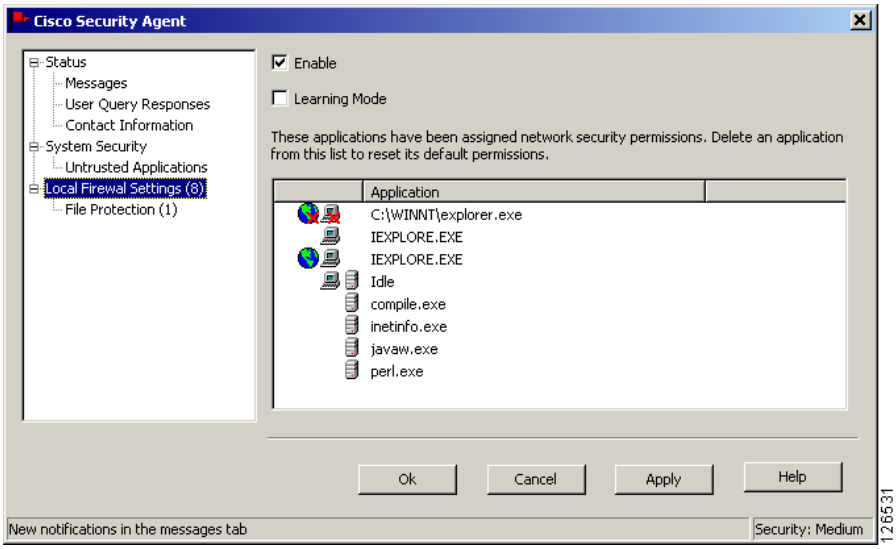
**Note** If a host belongs to a group operating in Test Mode, local firewall settings are ignored.

### Learning Mode

Users can enable learning mode for the firewall settings feature. While in learning mode, the agent is noting which applications run on the system and what those applications are allowed to do. Running the agent in learning mode for a certain amount of time allows it to learn the system's normal operating behavior and then provide security accordingly once learning mode is disabled. While in learning mode, the agent notes what applications are used to access the network and assigns those permissions automatically.

When the agent is taken out of learning mode, it will allow only those applications it previously noted to run in the manner in which they were used during the learning period. If the agent notices a new action that it has not learned taking place on the system, the agent queries the user, asking if it is okay for the application in question to access the resource in question. Once users reply to the query, the agent remembers the response and the next time the application is used, the same action is allowed or denied based on the initial response and users are not queried again.

*Figure A-8 Agent Local Firewall Settings Screen*



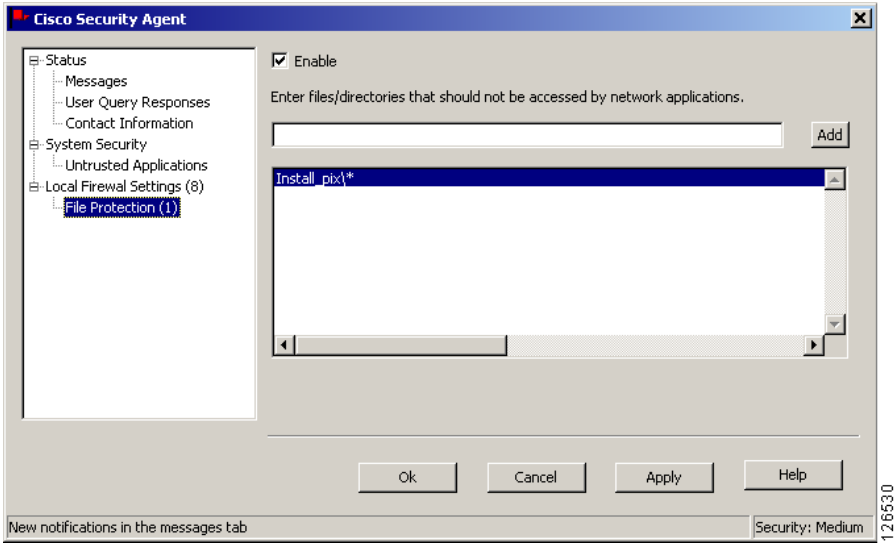

## File Protection

Through some simple configuration, the agent can protect specified local files and directories on systems from all network access. This is useful if there is sensitive personal information stored on user systems. Entering the name of the file or directory that users want protected cuts off all network access to that resource.

Users must select the Enable checkbox to turn on File Protection. From the File Protection window, users can enter the file or directory name in the top edit field and click the Add button. This file or directory is now protected from all network access. (Note that if a network application attempts to access a protected file, users are queried. In some instances, users may want to allow this access.) To remove file protection, select the file name or directory name in the edit field and press the Delete key.

In order for the agent to determine if an entry is a file or a directory, users must use a specific syntax. That syntax is explained to end users in the Cisco Security Agent online help.

*Figure A-9 Agent File Protection Screen*




**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.

# Turn Agent Security Off

Provided there is not an Agent service control rule or Agent UI control rule (See Agent Service Control, page 4-44 and Agent UI Control, page 4-48 for rule details) that denies this action, all users can stop the security the agent provides on a Windows or Linux host by accessing the agent UI and clicking on the flag in the menu bar. If users move the slidebar (if present) to the Off setting, agent security enforcement stops.

**Note** If there is no agent UI on a system (no user interaction), the ability to turn off agent security is not available to non-administrative users.

Provided there is not an Agent service control rule that denies this action, Windows administrators can run the following commands from a command prompt window on the agent host system to stop and start the agent service:

```
net stop "Cisco Security Agent"
net start "Cisco Security Agent"
```

Provided there is not an Agent service control rule that denies this action, administrators can stop and start the agent service on a UNIX (Solaris and Linux) host by running the following commands from a command prompt window on the agent host system:

```
/etc/init.d/ciscosec stop
/etc/init.d/ciscosec start
```

**Caution** Stopping agent security and/or stopping the agent service on any system disables all rules on that system. Starting the agent service and resuming security reinstates all rules.

# Installing Software Updates on Agents

Cisco occasionally provides software updates for Cisco Security Agents. You configure CSA MC to distribute the appropriate software updates to specified agents across the network. When agents poll in to check for new rules, if there is an update available for the agent in question, it transparently receives the update at that time. The update installs without any interaction from the end user. See Distributing Software Updates, page 3-39 for CSA MC configuration details

**Note** Use the csactl utility (see page A-27) on Solaris systems to check for updates and install them.

In some cases, you may require agent systems to be rebooted after installing an update. Users are prompted that the system will reboot within 5 minutes if this is necessary. Note that configuration changes are not applied until the system is rebooted.

Agent systems contain online help explaining how software updates work. You may want to refer users to it.

## Uninstall Windows Cisco Security Agent

To uninstall the Cisco Security Agent, do the following:

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

# Installing the Solaris Agent

This section details the commands you enter and the subsequent output that is displayed when you install the Cisco Security Agent on Solaris systems. When you download the agent kit from CSA MC, do the following to unpack and install it. (Note that you can put the downloaded tar file in any temp directory. Do not put it in the opt directory, for example, as you may then experience problems with the installation.)

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

```
$ su
```

**Step 2** Untar the agent kit.

```
# tar xf
CSA-Test_Mode_Server_V4.5.0.265-sol-setup-f734064be5a448b88
e2a27867059113c.tar
```

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

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

[Output:]
The following packages are available:
 1 CSCOcsa CSAagent
         (sun4u) 4.5.0.15
```

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

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

[Output:]
Processing package instance <CSCOcsa> from </space/user>
```

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

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

```
This package contains scripts which will be executed with
super-user permission during the process of installing this
package.
Do you want to continue with the installation of <CSCOcsa>
[y,n,?]y
Installing CSAagent as <CSCOcsa>
```

**Step 6** The installation continues to copy and install files. When the install is complete, the following is displayed:

```
The agent installed cleanly, but has not yet been started.
The command: /etc/init.d/ciscosec start
will start the agent. The agent will also start
automatically upon reboot. A reboot is recommended to
ensure complete system protection.
The following packages are available:
       1 CSCOcsa CSAagent
          (sun4u) 4.5.0.15
```

**Step 7** Quit (q) when installation is finished.

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

**Step 8** Optionally, reboot the system by entering the following.

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

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

The agent installs into the following directory:

```
/opt/CSCOcsa
```

Some files are put into additional directories such as `/kernel/strmod/sparcv9`, `usr/lib/csa`, `/etc/init.d` and `/etc/rc?.d`.

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

## Uninstall Solaris Agent

To uninstall the 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 system are not changed to restrict this access.) See Agent Service Control, page 4-44 for details on this rule type.

# UNIX Agent csactl Utility

Because the Solaris Cisco Security Agent has no user interface, a utility is provided which allows you to check the Solaris agent status, poll in to CSA MC and re-enable logging. The command you enter to perform these functions is **csactl**.

**Note** Note that this utility has also been made available for Linux systems. Because Linux does provide an agent UI, using the csactl utility on Linux is optional.

Enter the csactl command as follows:

```
# /opt/CSCOcsa/bin/csactl <command>
```

Available commands are:

| | |
|---|---|
| `poll` | Triggers an immediate poll of the management server. (Also lets you know if there is a software update available.) |
| `resetlog` | Resets the logging holdback -- allows all log messages. |
| `status` | Displays a small amount of status information. (Also lets you know if there is a software update available.) |
| `swupdate` | Updates agent software. |
| `info <text>` | This is a mechanism for directly sending custom (informational) textual events to CSA MC. Once the message reaches the CSA MC, it can be viewed or a notification can be sent to an administrator. |
| `warning <text>` | This is a mechanism for directly sending custom (warning) textual events to CSA MC. Once the message reaches CSA MC, it can be viewed or a notification can be sent to an administrator. |

| | |
|---|---|
| `alert <text>` | This is a mechanism for directly sending custom (alert) textual events to CSA MC. Once the message reaches CSA MC, it can be viewed or a notification can be sent to an administrator. |
| `about` | Displays agent software version number. |

The commands listed above are only available to root.

For example, poll in to CSA MC by entering the following:

```
# /opt/CSCOcsa/bin/csactl poll
Poll of management center succeeded
```

For example, check the status of the agent by entering the following:

```
# /opt/CSCOcsa/bin/csactl status
Status:
Management center: stormcenter
Registration time: 2002-03-20 15:19:16
Host id: {FG9DA858-6131-45E9-18BD-EE32BA2D0676}
Last download time: 2002-03-20 15:19:23
Last poll time: 2002-03-20 15:20:42
Software update: newer version is available
```

For example, to perform a software update:

```
# /opt/CSCOcsa/bin/csactl swupdate
```

**Note** You must reboot the system after performing a software update.

For example, re-enable logging if duplicate messages are being throttled:

```
# /opt/CSCOcsa/bin/csactl resetlog
Reset Log throttle sent to kernel
```

# Installing the Linux Agent

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

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

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

```
$ mv
CSA-Server_V4.5.0.218-lin-setup-1a969c667ddb0a2d2a8da3e7959
a30b2.tar /tmp
```

**Step 2** Untar the file.

```
$ cd /tmp
$ tar xvf
CSA-Server_V4.5.0.218-lin-setup-1a969c667ddb0a2d2a8da3e7959
a30b2.tar
```

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

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

**Step 4** Run script install_rpm.sh as root.

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

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

**Note** CSAagent rpm packages are not relocatable.

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

## Uninstall Linux Agent

To uninstall the Cisco Security Agent, do the following.

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

```
# rpm -qf /opt/CSCOcsa/bin/ciscosecd CSAagent-4.5-218
```

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

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

**Caution** If an agent is running a policy which contains an Agent 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, page 4-44 for details on this rule type.

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


# System Components

## Overview

This appendix contains information on CSA MC and agent core components, explaining how these components relate to each other, including details on various CSA MC and agent services.

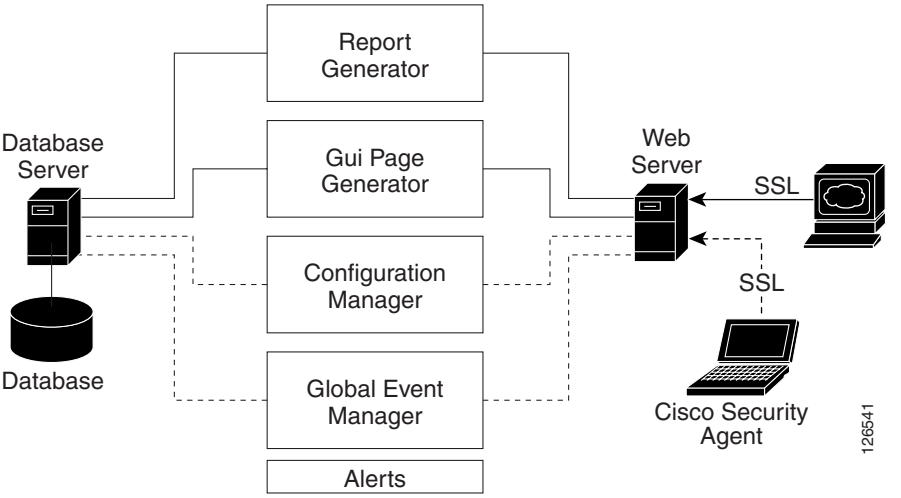
This section contains the following topics.


- CSA MC Components, page B-2
- Agent Components, page B-4

# CSA MC Components

CSA MC architecture is displayed in this appendix. Note that although the agent is mentioned often here, it is only in terms of CSA MC's relation to the agent. Agent software does have its own system components which are described in this chapter. It is CSA MC that pushes security policies to the agents and coordinates the events it receives back from the agents. The mechanisms that are required to perform those tasks are described here as part of the CSA MC architecture.

***Figure B-1 CSA MC Components***




The **web browser**, shown on the right in the diagram, represents any web browser on any system across an enterprise from which administrators can securely access the CSA MC web-based interface. Communications between the web browser and the web server occur over SSL, allowing administrators to securely access the database of rule configurations from any location.

The *web server* provides the means of communication between the web browser and all other CSA MC system components. The web server displays reporting information, configuration version data, and event logging data.

It is through the **web server** that the agents installed on systems across an enterprise can exchange data with the CSA MC **configuration manager** and the **global event manager**. When agents poll in to CSA MC for rule set updates, it is the configuration manager that pulls the rules from the database and distributes

them to the particular agents for which they are intended. Agents also send events to the global event manager which stores this information in the central SQL server database.

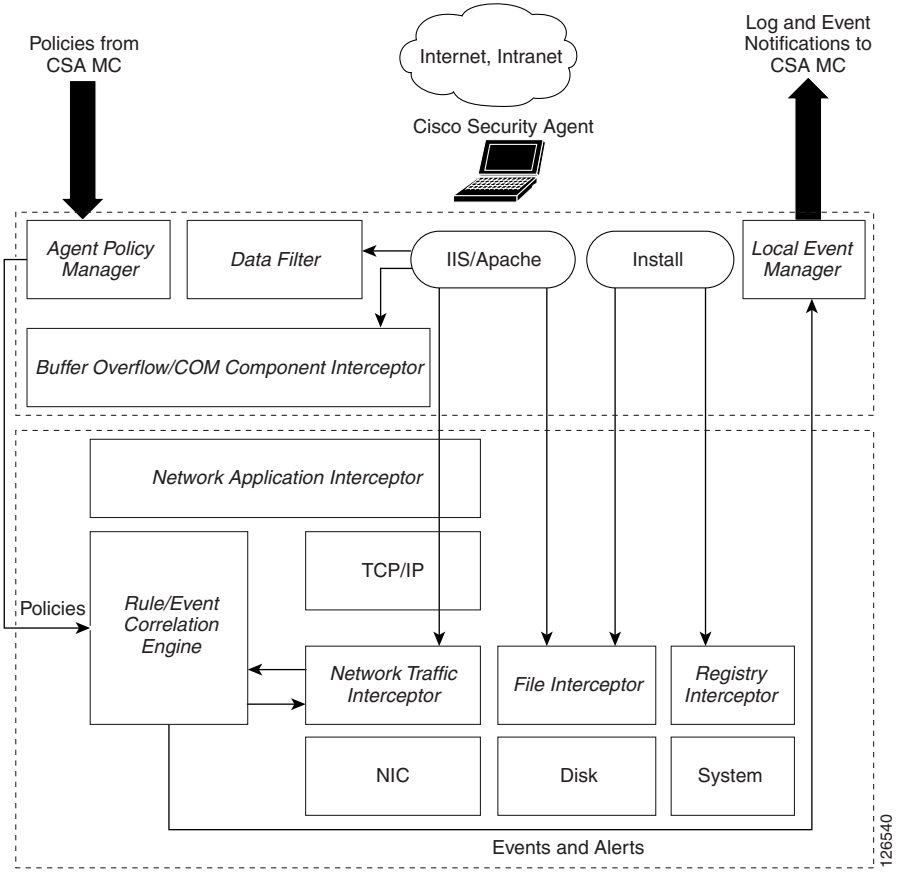
The **SQL server database** is the central repository for configuration data (host agents, groups, file rules, network rules, registry rules, etc.) created by the administrator and for the system event information provided by the agents. It is in this database that rules and information on system groupings are stored when the administrator generates rules and policies through the web-based interface. When reports are requested by the administrator, the **report generator** component gathers rule and event data kept in the database and produces reports using this information.

All information (rule configurations, event logs, etc.) passed between CSA MC and the agents distributed across your enterprise is encrypted providing a secure communication channel for the exchange of data.

# Agent Components

Figure B-2 shows the agent in terms of its system components, displaying where those components operate in relation to general system functions. For example, the interceptors shown in the diagram install and work at the kernel level.

***Figure B-2 Cisco Security Agent Components (Windows)***



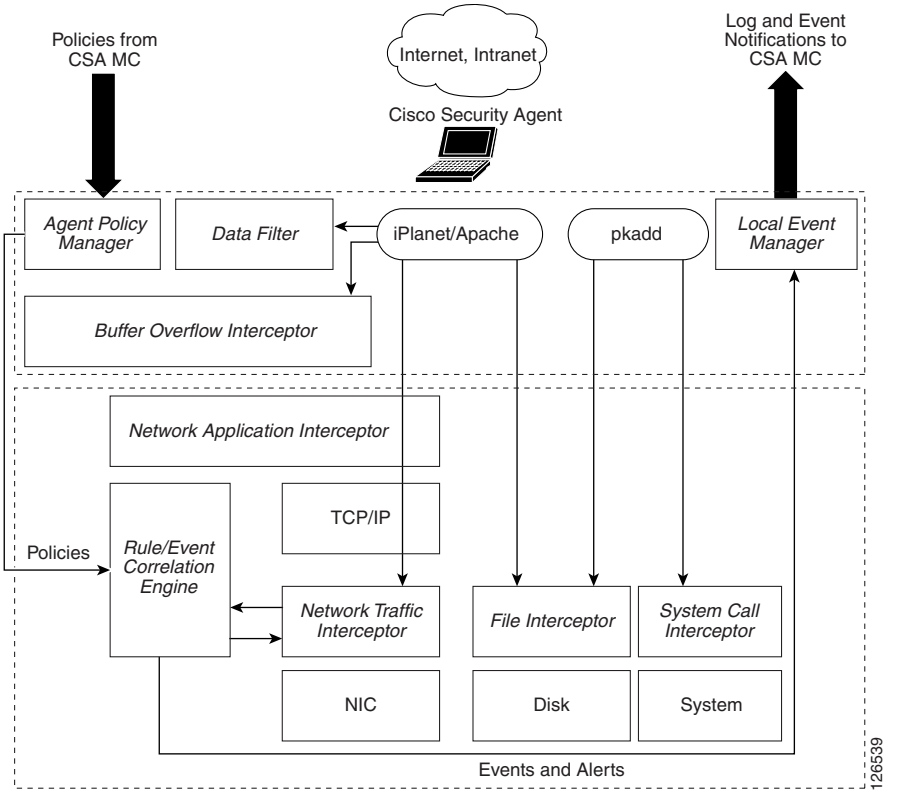

Starting from the left side of the diagram, the agent **policy manager** receives the rules configured by the administrator from CSA MC. These rules are sent to the agent's **rule/event correlation** engine. If a rule set already exists there, those rules are updated or replaced with the newest rule set.

The **interceptors** do as their name indicates, they intercept key actions that are attempted on the system and check the action in question against the rule correlation engine to determine if a rule set allows or denies it. Based on the information the interceptors receive, they either allow the action to take place or they stop it cold.

Actions are stopped based on certain criteria that are part of each rule and consequently each interceptor acts based on a component-targeted set of criteria. For example, the **network application interceptor** controls which applications are allowed to communicate with the network, while the **network traffic interceptor** provides system hardening features such as SYN flood protection and port scan detection. The **file interceptor** controls which applications can read and/or write to specified system files and directories. The **registry interceptor** controls system behavior, preventing applications from writing to particular registry keys. All of these controls can be as broad or as granular as necessary.

As the interceptors are allowing or denying actions, they produce an event each time a rule set is triggered by a system action. These events are stored in the rule/event correlation engine which forwards them on to the **local event manager** and **global event manager**. Events are also stored in the NT event log or W2K event viewer on the agent system.

*Figure B-3 Cisco Security Agent Components (UNIX)*




# Open Source License Acknowledgements

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

# OpenSSL/Open SSL Project

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

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

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

## License Issues

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

**OpenSSL License:**



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

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

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

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

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

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

**Original SSLeay License:**

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

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

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

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

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

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

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

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

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

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

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

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

# Apache license



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 acknowledgment:
   "This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/)."

4. The names "Apache Server" and "Apache Group" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache" nor may "Apache" appear in their names without prior written permission of the Apache Group.

6. Redistributions of any form whatsoever must retain the following acknowledgement:
   "This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/)."

THIS SOFTWARE IS PROVIDED BY THE APACHE GROUP "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 APACHE GROUP OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

# 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.

# 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.

THIS FASTCGI APPLICATION LIBRARY SOURCE AND OBJECT CODE (THE "SOFTWARE") AND ITS DOCUMENTATION (THE "DOCUMENTATION") ARE COPYRIGHTED BY OPEN MARKET, INC ("OPEN MARKET"). THE FOLLOWING TERMS APPLY TO ALL FILES ASSOCIATED WITH THE SOFTWARE AND DOCUMENTATION UNLESS EXPLICITLY DISCLAIMED IN INDIVIDUAL FILES.

OPEN MARKET PERMITS YOU TO USE, COPY, MODIFY, DISTRIBUTE, AND LICENSE THIS SOFTWARE AND THE DOCUMENTATION SOLELY FOR THE PURPOSE OF IMPLEMENTING THE FASTCGI SPECIFICATION DEFINED BY OPEN MARKET OR DERIVATIVE SPECIFICATIONS PUBLICLY ENDORSED BY OPEN MARKET AND PROMULGATED BY AN OPEN STANDARDS ORGANIZATION AND FOR NO OTHER PURPOSE,

PROVIDED THAT EXISTING COPYRIGHT NOTICES ARE RETAINED IN ALL COPIES AND THAT THIS NOTICE IS INCLUDED VERBATIM IN ANY DISTRIBUTIONS.

NO WRITTEN AGREEMENT, LICENSE, OR ROYALTY FEE IS REQUIRED FOR ANY OF THE AUTHORIZED USES. MODIFICATIONS TO THIS SOFTWARE AND DOCUMENTATION MAY BE COPYRIGHTED BY THEIR AUTHORS AND NEED NOT FOLLOW THE LICENSING TERMS DESCRIBED HERE, BUT THE MODIFIED SOFTWARE AND DOCUMENTATION MUST BE USED FOR THE SOLE PURPOSE OF IMPLEMENTING THE FASTCGI SPECIFICATION DEFINED BY OPEN MARKET OR DERIVATIVE SPECIFICATIONS PUBLICLY ENDORSED BY OPEN MARKET AND PROMULGATED BY AN OPEN STANDARDS ORGANIZATION AND FOR NO OTHER PURPOSE. IF MODIFICATIONS TO THIS SOFTWARE AND DOCUMENTATION HAVE NEW LICENSING TERMS, THE NEW TERMS MUST PROTECT OPEN MARKET'S PROPRIETARY RIGHTS IN THE SOFTWARE AND DOCUMENTATION TO THE SAME EXTENT AS THESE LICENSING TERMS AND MUST BE CLEARLY INDICATED ON THE FIRST PAGE OF EACH FILE WHERE THEY APPLY.

OPEN MARKET SHALL RETAIN ALL RIGHT, TITLE AND INTEREST IN AND TO THE SOFTWARE AND DOCUMENTATION, INCLUDING WITHOUT LIMITATION ALL PATENT, COPYRIGHT, TRADE SECRET AND OTHER PROPRIETARY RIGHTS.

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.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER

RESULTING FROM LOSS OF USE, DA A 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.

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

# INDEX

## Symbols


@CD 2-35
@desktop 2-36
@dynamic 2-34, 2-38, 4-67, 4-71, 5-23, 7-12, 7-16
@fixed 2-29, 2-35
@floppy 2-35
@local 4-71
@network 2-37
@recent 2-38
@regpath 2-34
@remote 2-37
@removable 2-35
@smb-null-session 2-38
@startmenu 2-36
@startup 2-36
@subnet 2-37
@system 2-34


## A


ActiveX
- crystal report viewer 9-10
- preventing download 5-4

ActiveX reports 11-38
Address set syntax 2-37
Add to application class 4-9, 6-19
Admin Access Control 2-10
Administrator
- role-based administration 2-6

Admin Preferences 2-6
- Admin Access Control 2-10
- pre-configured preferences 2-9

Agent
- architecture 1-6
- kits 3-8
- optional reboot after install A-9
- scripted silent installs and uninstalls 3-18
- user interface A-10

Agent (Linux)
- commands A-27
- csasctl utility A-27
- installing A-29
- uninstalling A-30

Agent (Solaris)
- commands A-27
- csasctl utility A-27
- installing A-24

uninstalling A-26
Agent (UNIX)
check status A-27
polling A-27
re-enable logging A-27
software update A-27
Agent kits
adding or removing groups from 3-19
downloading 3-17
download URL 3-12
Linux installation A-29
modifying 3-19
network shim enable 3-10
preconfigured sample 3-4, 3-8, 4-20
quiet install 3-10
reboot vs. no reboot 3-15
Solaris installation A-24
status 3-14
Agent registration 3-17
Registration control 3-18
Agent service
stop and start A-22
Agent service control 4-44
Agent UI
Contact Information A-16
File Protection A-20
Learning Mode A-19
Local Firewall Settings A-18
Messages A-13
Network Lock A-16
Status A-11
System Security A-16
Untrusted Applications A-17
User Query Responses A-14
Agent UI control 4-48
Alert types
configuring 8-34
log file, generate 8-41
Analysis overview 11-1
Analysis Reports 11-52
Application Behavior Investigation
analysis process overview 11-39
Behavior Analyses Reports 11-52
Behavior Analysis 11-40
Configure Behavior Analysis 11-42
monitor event log 11-46
Overview 11-38
Policy creation methodology 11-59
Policy enforcement 11-44
progress status 11-46
Application Behavior Reports
Overview 11-52
Application-builder rule 6-18
Application Classes 6-2, 6-9
application-builder rule 6-18
application class management 6-24
Authorized rootkit 6-7
built-ins 6-4

creation from rule page 6-23
double-click to view 6-24
dynamic 6-13
enable/disable for product 6-24
First Time Application Execute 6-5
Installation Applications 6-7
managing application classes 6-24
Network Applications 6-5
Processes communicating with untrusted hosts 6-7
Processes copying untrusted content 6-7
Processes created by Network Applications 6-6
Processes created by Servers (TCP and UDP) 6-6
Processes executing untrusted content 6-7
Processes monitoring the Keyboard 6-6
Processes requiring kernel only protection 6-7
Processes requiring OS stack execution protection 6-8
Processes requiring Security Level 6-8
Processes with elevated privileges 6-6
Processes writing untrusted content 6-8
Recently created untrusted content 6-6
Remote clients 6-6
remove process 6-10, 6-16
Server (TCP based) 6-6
Server (UDP based) 6-6
shell scripts 6-3
static application classes 6-9
Suspected Virus Applications 6-8
System Process 6-6
Unauthorized rootkit 6-8
Application class management 6-24
Application control 4-52
Application Deployment Investigation
Application Classes 11-8
Data Management 11-14
Enable options 11-5
Group Settings 11-4
investigation process overview 11-3
Product Associations 11-7
Unknown Applications 11-12
Application Deployment Reports
AntiVirus Installations 11-17
Installed Products 11-20
Network Data Flows 11-30
Network Server Applications 11-34
Product Usage 11-27
Unprotected Hosts 11-23
Unprotected Products 11-25
Are you there?, VPN client 13-2
Attributes matching, file sets UNIX 7-12
Audit trail 2-11
Authorized rootkit 6-7
Auto-enrollment 3-3, 4-14
Available button
agent A-11
Available software updates 3-39

## B


Backing up configurations 10-3
  differential backup 10-4
  full backup 10-4
Behavior Analysis
  import policy 11-50
  start analysis 11-47
Behavior Investigation
  Behavior analysis process 11-39
BootExecute 7-24
broadcast messages 4-72
Browser requirements 2-2
Buffer overflow, Windows 5-5
Buffer Overflow rule 5-14
  replicate feature 5-7
Built-in Application Classes 6-4
Bulk transfer hosts 3-34
Bulk transferring hosts 3-34


## C


Caching query responses 4-18
CD ROM drives 2-35
Check Point
  integration 13-3
  Third Party directory 13-4
Check Point OPSEC integration 13-3
Cisco Security Monitor
  integration 13-2
Cisco Trust Agent (CTA) 3-11, 3-26, 4-25
  host posture status 3-26
  plugin 10-20
Cisco VPN client support 13-2
Cisco Works 3-12
Clear Pending Alerts 8-35
Clipboard access control 4-74
COM component
  access control rule 4-76
  extract utility 10-9
COM Component Sets 7-3
  extract utility 10-9
Compare configurations 2-27, 4-39
Compare policies 4-39
configuration manager B-2
Configuration shortcuts 2-24
Configuration view 2-23
Connection Rate Limit 4-56
Consistency check 4-43
Contact information
  agent 3-25
Copy rules 4-36
Correlating events 5-20
CSA_uninstall.bat 3-18
csactl Utility (UNIX agents) A-27
CSA MC
  logging in 2-4

## D


Data access control 4-60

Database Maintenance 10-8

Database restoring log 10-7

Data filter installation, required for data access control rule 10-10

Data Sets 7-7

Delete configurations 2-26

Deployment Overview 1-4

Detailed descriptions 4-3

Detailed status and diagnostics 3-26

Details link 8-5

Directory protection 2-31, 4-65

Disable

- application class 6-24
- policy rule enforcement 8-25, 11-44
- rule 4-34

Disk space

- shrink your database files 10-8

Display only in Show All mode 6-9, 6-15, 7-8

- checkbox 7-3

Distributed configuration software updates 3-45


## E


Email worm protection 5-18

Enable rule 4-34

Ephemeral ports

- using 2-39

ephemeral ports 7-19

Ethereal software 8-5, 8-6, 8-7

Event code 4-88

Event Correlation 5-20

Event ID 4-88

Event log 8-2

- packet details 8-6

Event logging exception wizard 8-22

Event Management Wizard 8-14

Event Monitor 8-7

Events 8-2, 8-6

- auto-pruning 8-9
- details 8-6
- event insertion tasks 8-8
- event log 8-2
- event log change filter 8-3
- event log details link 8-5
- event log management 8-8
- event log start and end dates 8-3
- Event Monitor 8-7
- Event Sets 8-27
- find similar 8-5
- log filter text 8-2
- managing 8-8
- minimum and maximum severity 8-3
- minimum severity 8-3
- packet details 8-5, 8-6
- reading details 8-6

reading logs 8-6
reading packet details 8-6
rule number link 8-5
searching details with Google 8-6
Status Summary 2-21
third party access 8-32
Events by Group reports 9-5
Events by Severity reports 9-3
Event Sets 8-27
Purge events 8-29
View button 8-29
Exception rule wizard 8-16
Expanded views 2-7
Explain rules link 4-42
Export configurations 10-14
Export reports 9-11
extract_com 10-9


## F


File access control 4-64
file interceptor B-5
File Protection A-20
File Sets 7-10
File set syntax 2-28
File version control 4-79
Filter user info from events 3-7
Find database items 2-16
Find Similar 8-5
First Time Application Execute 6-5
floppy drives 2-29, 2-35
Force reboot after install 3-42


## G


Generating Rules 4-118
Details link 4-118
pending changes 2-26
Global event correlation 5-19
Global Event Management
Correlation 5-20
global event manager B-2
Google 8-6
Google searches of details 8-6
Group
configure 4-19
preconfigured sample 4-20
Groups
about 3-2
adding or removing from agent kits 3-19
adding or removing hosts from 3-33
attaching policies to 4-112
bulk transferring hosts between 3-34
configure 3-3
Filter user info from events 3-7
mandatory enrollment in 3-3
membership 3-28
modifying group membership 3-25

modifying host memberships in 3-33, 3-36
Polling interval 3-5
preconfigured sample 3-4
reset agents 3-7
Rule overrides 3-6
search for hosts and change group membership 3-36
Send polling hint 3-6
Test Mode 3-6
Verbose Logging Mode 3-6


## H


Hard link protection
file access control 4-66
Help
online 2-18
Host details 3-22
Application Deployment 3-27
contact information 3-25
diagnostics 3-26
events in past 24 hours 3-26
filter user info from events 3-27
group membership 3-28
host description 3-25
host identification 3-25
host name 3-25
host settings 3-27
host status 3-26
last Application Deployment data upload 3-26
last known IP address 3-25
log deny actions 3-27
policies 3-28
policy inheritance 3-28
policy version 3-26
polling interval 3-27
product information 3-25
quick links 3-25
rules 3-28
send polling hint 3-27
software version 3-26
test mode 3-27
time since last poll 3-26
UID 3-25
verbose logging mode 3-27
view related events 3-25
Host identification
registration time 3-26
Hosts
about 3-3
add or remove from group 3-32
bulk transferring between groups 3-34
changing groups 3-31
copy from one group to another 3-34
deleting 3-30
diagnose 3-26
group membership 3-28
groups of hosts 3-2

modify group membership 3-32, 3-36
modifying group membership 3-34
move from one group to another 3-34
policy inheritance 3-28
posture status 3-26
registering with CSA MC 3-17
reset 3-27
search for and add to group 3-36
search for and change group membership 3-36
search for and delete 3-36
searching for 3-28
unprotected 3-29
unsupported platforms 3-29
viewing details 3-22
viewing hosts managed by CSA MC 3-21
viewing host statuses 3-21
view relevant event log 3-25
view status 3-21
Host settings 3-27
Host Status 3-26
Active 3-22
Last Poll 3-22
Latest Software 3-22
Protected 3-22
Test Mode 3-22
HTML frame reports 11-38
HTTPS A-6


## I


ID
rule 4-34
Import configurations 10-14
delete 10-19
Import history 10-19
Install
agent A-2
Installation Applications 6-7
Insufficient disk space event 10-8
interceptors B-5
file B-5
network application B-5
network traffic B-5
registry B-5
Internet Explorer
version requirements 2-2
Intrinsic security 1-1
IPlanet server data filter 4-60
IP security checks 5-8
IPV6 addresses 2-38, 7-16


## K


Kernel Protection 4-84
Keystroke trapping
preventing 5-3

## L


Learning mode A-19
Lifecycle of an attack 1-2
Listener option in NACL 4-72
local event manager B-5
Local Firewall Settings A-18
Localized directory paths 2-36
Location based states 4-27
  Remote VPN clients 4-28
Log all deny actions 3-6
Logging 8-12
  suppression of log messages 8-12
  verbose logging mode 3-27
Logging agent 11-39


## M


Maintenance
  Available Software Updates 3-39
  Event Log Management 8-8
Make kit button 3-12
Manage
  application classes 6-24
  dynamically quarantined files 5-23
  dynamically quarantined IP addresses 5-23
Mandatory group enrollment 3-3
Manual data filter installation 10-10
Media device monitoring 5-4
Media type syntax 2-35
Menu bar 2-12, 2-26
Merge
  analysis products 11-10
  configurations 2-27, 4-41
  rule modules 4-41
Messages A-13
minimum severity 8-3
Modify agent configuration
  self-protection 4-46
Modifying group membership 3-32
Modifying host membership 3-33, 3-34
Monitoring Access 4-14
Most active hosts 2-22
Most active rules 2-22
multicast packet signals 4-72, 8-12
Multiple MC software update 3-45


## N


NAC 3-12
Navigation shortcuts
  insert link 2-24
  new application class link 2-24
  show reference list 2-24
  variables 2-24
netForensics
  integration 13-2
Netscape

version support 2-2
net start command 10-2, A-22
net stop command 10-2, 10-9, A-22
Network access control 4-69
Network Address Sets 7-15
Network Admission Control 4-25
network application interceptor B-5
Network Applications 6-5
Network interface control 4-99
Network Lock A-16
Network service ephemeral ports 2-39
Network Services 7-18
Network service syntax 2-38
Network shield 5-7
detect port scans 5-10
ICMP covert channels 5-11
ICMP information/configuration 5-11
invalid IP addresses 5-9
invalid IP headers 5-8
malicious packets 5-11
prevent SYN floods 5-9
randomize TCP sequence numbers 5-10
replicate feature 5-7
source routed packet 5-9
TCP blind session spoofing 5-10
trace route 5-9
unrestricted network connectivity during boot 5-12
Network shim 3-10
optional A-7
network traffic interceptor B-5
NT Event log 4-87


## O


Operating system changes, agent A-4


## P


Packet details 8-6
packet sniffers 4-96, 4-99
Peers
groups 11-32
hosts 11-32
network address sets 11-32
Peripherals 2-29, 2-35
Policies
agent UI control 4-48
application control 4-52
applying 4-111, 4-112
attaching rule modules to 4-111
buffer overflow 5-14
buffer overflow protection 5-14
building 4-19
clipboard access control 4-74
combining 4-7
com component access control 4-76
compare, copy, merge 4-39
file access control 4-56, 4-60, 4-64, 4-76, 4-90

file version control 4-79
generate rules 4-118
network access control 4-69
network interface control 4-99
network shield 5-7
NT event log 4-87
port scan detection 5-10
preparing a security policy 1-9
registry access control 4-90
resource access control 4-102
rootkit /kernel protection 4-104
service restart 4-93
sniffer and protocol detection 4-96
SYN flood protection 5-9
Syslog control 4-107
system API control 5-3
Policy creation guidelines 12-1
Policy enforcement 8-25, 11-44
Policy inheritance 3-28
polling 1-10
Polling hint message 3-6
Polling interval 3-5
Port scan detection 5-10
Print Screen disabled 4-75
Processes communicating with untrusted hosts 6-7
Processes copying untrusted content 6-7
Processes created by Network Applications 6-6
Processes created by Servers (TCP and UDP) 6-6
Processes executing untrusted content 6-7
Processes requiring kernel only protection 6-7
Processes requiring OS stack execution protection 6-8
Processes requiring Security Level 6-8
Processes with elevated privileges 6-6
Processes writing untrusted content 6-8
Product data collection 11-5
Products
configure associations 11-7
promiscuous mode 4-100
Purge events 8-29


## Q


Quarantined files 5-22
Quarantined files and IP addresses 5-23
Quarantined IP addresses 5-23
Query responses
caching 4-18
challenge user 4-17
clear 4-18
configure prompt text 7-26
Don’t ask again 4-17, 4-18
Query settings 7-25
Query User 4-15
Quiet install 3-10, 3-42

## R


Reboot operations 7-24
Reboot optional
  agent A-8, A-9
Reboot vs. no reboot for agents 3-15
Recently created untrusted content 6-6
Registration control 3-18
Registry access control 4-90
registry interceptor B-5
Registry sets
  BootExecute 7-24
  Reboot operations 7-24
  Run keys 7-24
  Shell commands 7-24
Remote access 2-5
Remote clients 6-6
Removable media 2-35
Remove process from application class 6-10, 6-16
Replace items, search 2-17
replicate feature (rule option) 5-7
report generator B-3
Reports
  Events by Group 9-5
  Events by Severity 9-3
  Exporting 11-38
  exporting 9-11
  generating 9-3
  Group Detail 9-9
  Host Detail 9-6
  Policy Detail 9-8
  printing 9-11
  refresh 9-11
  Unprotected Products 11-25
Report viewer 9-10
Requirements
  agent A-3
Reset Cisco Security Agent 3-7, 3-27, A-11
Reset to factory A-10
Resource access control 4-102
Restoring configurations 10-6
Resume security after install 5-20
Right-click menu shortcuts 2-27
Role-based administration 2-6
Rootkit / kernel protection 4-104
Rule ID 4-34
Rule Modules
  adding rules 4-32
  configuring 4-22
  System state sets 4-25
  User state sets 4-30
Rule overrides 3-6
Rules
  about 4-6
  action definitions 4-10
  action options 4-9
  agent service control 4-44
  agent UI control 4-48

application control 4-52
buffer overflow 5-14
clipboard access control 4-74
com component access control 4-76
compare, copy, merge 4-39
connection rate limit 4-56
consistency check 4-43
copying rules between modules 4-36
data access control 4-60
email worm protection 5-18
enable/disable 4-34
Events column 4-34
explain link 4-42
explain rules running on a host 3-25
file access control 4-64
file version control 4-79
ID column 4-34
kernel protection 4-84
Logging options 4-13
manipulating precedence 4-13
network access control 4-69
network interface control 4-99
network shield 5-7
NT event log 4-87
port scan detection 5-10
precedence, ordering 4-9
registry access control 4-90
resource access control 4-102
rootkit / kernel protection 4-104
service restart 4-93
show enabled rules only checkbox 4-36
sniffer and protocol detection 4-96
SYN flood protection 5-9
syslog control 4-107
System API Control 5-3
View All rules 4-36
view change history 4-41
Run keys 7-24

## S

Sample policies 8-27
Save configurations 2-27
Scheduled database backups 10-4
Scheduled software updates 3-41
Scripted agent installs and uninstalls 3-18
Scripts, writing rules for 6-3
Search
host search 3-28
how to use it 2-16
replace 2-17
Security Monitor
integration 13-2
Security policy 4-3
preparing 1-9
Self-protection 4-10
Send polling hint 3-6, 3-27
Server (TCP based) 6-6

Server (UDP based) 6-6
service, agent start/stop 10-2, A-22
Service restart 4-93
Shell commands 7-24
Shell scripts, writing rules for 6-3
Show All mode 2-7, 6-9, 7-8
show enabled rules only checkbox 4-36
Show reference list 2-24
SID 4-31
Silent agent install and uninstall 3-18
Sniffer and protocol detection rule 4-96
Software updates 3-39
  agents A-23
  Distributed configuration software updates 3-45
  Force reboot 3-42
  Installing updates on agents A-23
  Quiet install 3-42
  Scheduled software updates 3-41
Solaris agent install directory A-25
Solaris requirements
  agent A-5
SQL Server database B-3
SSL 1-10
Start agent service 10-2, A-22
State conditions 4-24
Status A-11
  Event Log 8-2
Status, agent kits 3-14
Status Summary
  colored chart 2-21
Stop agent service 10-2, A-22
Stop and start agent security A-22
Stop logging button 11-44
Suspected Virus Applications 5-18, 6-8
Symbolic link protection
  file access control 2-32, 4-66, 4-103
  general 4-102
Syntax 2-28
Syslog control 4-107
System API Control 5-3
System calls, unusual 5-5, 5-16
System components B-1
System Process 6-6
System Security A-16
System Startup Security checks 5-12
System state
  DNS suffix matching 4-27
  installation process detected 4-28
  management center reachable 4-27
  network address ranges 4-27
  rootkit detected 4-28
  security level 4-27
  system booting 4-28
  virus detected 4-28
System State sets 4-25

## T


Take precedence over other rules 4-13
Terminal services A-3
Test Mode 3-6, 4-114
Test mode 3-27
Third party
    access to events 8-32
Third Party directory 13-4
Trace route, prevent 5-9
Transport security checks 5-9
Troubleshooting agent data
    diagnostics A-12
Turn agent off A-22


## U


Unauthorized rootkit 6-8
UNIX agent install directory A-25
Untrusted Applications A-17
User Query Responses A-14
User State sets 4-30
Utilities
    csactl (Solaris agent) A-27
    extract_com 10-9
    net stop/start 10-2


## V


Variables
    COM Component Sets 7-3
    Data Sets 7-7
    Event Sets 8-27
    File Sets 7-10
    Network Address Sets 7-15
    Network Services 7-18
    Query Settings 7-25
    Registry Sets 7-21
    using 7-2
Verbose logging mode 3-27, 8-13
View All rules
    filter rule display 4-36
View change history 7-13
View change history, rules 4-41
View reports
    ActiveX 11-38
Vulnerable applications 12-8


## W


Waving system tray flag A-21
Windows requirements
    agent A-3
WinPcap software 8-6
Wizard
    behavior analysis 8-22

events 8-14
exception rule 8-16