



Using Management Center for Cisco Security Agents 6.0

Updated: October 17, 2008

Americas Headquarters

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

Customer Order Number: 78-18652-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.their names and products are trademarks or registered trademarks of their respective holders.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

Using Management Center for Cisco Security Agents V6.0
Copyright © 2008 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface **xxi**

Audience **xxi**

Conventions **xxii**

Obtaining Documentation, Obtaining Support, and Security Guidelines **xxiii**

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**

 Communicating Over Secure Channels **1-8**

 Distributing Policy Updates **1-9**

CHAPTER 2

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

 Overview **2-1**

 Browser Requirements **2-3**

 Accessing Management Center for Cisco Security Agents **2-4**

 Simple View and Advanced View Modes **2-5**

 Interface Overview of Management Center for Cisco Security Agents **2-5**

 Home Page **2-5**

Global Command Buttons	2-10
Menu Bar	2-10
Heading Links	2-14
Configuring Role-Based Administration	2-14
Changing Administrator Passwords	2-18
Configure Monitor Role Administrator Access Restrictions	2-19
Manage Administrator Active Login Sessions	2-20
Administrator LDAP Authentication	2-21
Distributing Cisco Security Agents	2-23
How Cisco Security Agents are Distributed	2-24
Host Security Page	2-24
System Monitoring	2-27
Home Page	2-27
Status Summary	2-27
Event Log	2-31
Reports	2-32
Using Audit Trail	2-32
CSA MC Page Types, Tasks, and Shortcuts	2-33
List View Pages	2-33
Configuration View Pages	2-33
Creating, Saving, and Deleting Data	2-34
Configuration Task Menus	2-35
Shortcuts and Hints	2-36
Using Search	2-39
Using CSA MC Utilities	2-41
Using the Correct Syntax	2-41
Object Names	2-41
Configuration Variable Names	2-41
Special Character Syntax	2-42

Directory and Filename Syntax Requirements	2-43
File and Directory Protection	2-48
Network Address Set Syntax Requirements	2-50
Network Services Syntax	2-53
Data Set Interface Matching Syntax	2-55
Data Set Pattern Matching Syntax	2-55
Content Matching in File Sets	2-57
Referencing Values Stored on Clients	2-58

CHAPTER 3

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

Overview	3-1
Grouping Hosts Together	3-2
Mandatory Group Enrollment	3-3
Configuring Groups	3-4
Resetting Cisco Security Agents	3-9
Managing Agent Kits	3-12
Creating Agent Kits from Existing Groups	3-12
Creating Agent Kits and Groups Using a Wizard	3-16
Distributing Agent Kits	3-18
Agent Reboot vs. No Reboot	3-24
Registration Control	3-25
Agent Registration	3-26
Scripted Agent Installs	3-26
Managing Hosts Using CSA MC	3-26
Viewing General Host Statuses with CSA MC	3-27
Viewing All Hosts Managed by CSA MC	3-27
Viewing Host Details	3-28
Searching for Hosts	3-36
Deleting Hosts from the CSA MC	3-38

Changing Host Memberships in Groups **3-43**

 Host Managing Tasks **3-51**

 Distributing Software Updates **3-54**

 Scheduling Software Updates **3-56**

 Software Updates in a Distributed Configuration **3-60**

CHAPTER 4

Building Policies 4-1

 Overview **4-1**

 Preparing a Security Policy **4-2**

 Configuring Rule Modules and Policies **4-2**

 Developing a Security Policy **4-3**

 Combining Policies **4-6**

 Making a Policy Mandatory **4-7**

 Building Policies and Rule Modules **4-8**

 Configure a Policy **4-8**

 Attaching Rule Modules to Policies **4-11**

 Attaching Policies to Groups **4-12**

 Overall Policy Methodology **4-14**

 Analyzing Applications **4-14**

 Configuring Policies —The Methodology **4-16**

 General Server Policy **4-17**

 Sample Web Server Policy **4-18**

 Combined General Server and Sample Web Server Policies **4-19**

CHAPTER 5

Rule Module Configuration 5-1

 Overview **5-1**

 About Rule Modules and Rules **5-3**

 Rule Module Components **5-4**

Available Rule Types 6-1

Overview 6-1

Rules Common to Windows and UNIX 6-3

Agent Service Control 6-3

Configuring Rule Modules	5-4
Adding Rules to a Rule Module	5-6
Filtering the Rules Display	5-9
Copying Rules between Modules	5-9
Comparing Configurations	5-10
Merging or Copying Rule Modules	5-12
View Change History	5-12
Explanation of Rules	5-13
Consistency Check	5-14
Attaching Rule Modules to Policies	5-14
Generating Rule Programs	5-16
Common Rule Page Configuration Items	5-17
Rules: Action Options and Precedence	5-18
Rules: Action Definitions	5-19
Rules: Manipulating Precedence	5-22
The Monitor Action	5-24
The Notify User Action	5-24
Using the Set Action	5-25
Querying the User	5-39
Caching Responses	5-43
Query Rule Priority Information	5-44
Rule Overrides	5-44
Using Audit Mode	5-44
Using Learn Mode	5-48

Agent UI Control	6-6
Application Control	6-11
Connection Rate Limit	6-15
Data Access Control	6-19
File Access Control	6-23
Network Access Control	6-29
Network Shield Rule	6-34
Windows Only Rules	6-42
Clipboard Access Control	6-42
COM Component Access Control	6-45
File Version Control	6-49
Kernel Protection	6-53
NT Event Log	6-57
Printer access control	6-59
Registry Access Control	6-61
Scan Event Log	6-64
Service Restart Rule	6-67
Sniffer and Protocol Detection	6-69
System API Control Rule	6-71
UNIX Only Rules	6-78
Buffer Overflow Rule	6-78
Network Interface Control	6-81
Resource Access Control	6-84
Rootkit / kernel Protection	6-86
Syslog Control	6-90

CHAPTER 7

Using Global Settings 7-1

Overview	7-1
Application Trust Levels	7-2
Setting Application Trust Levels	7-2

Using the Event Management Wizard to Set Trust Levels	7-3
Identifying Members of the White List, Grey List, and Black List	7-4
AntiVirus Exemptions	7-5
Event Correlation	7-7
Correlation	7-7
Signature Settings	7-13
Scanning Data Tags	7-15
Static Data Tags	7-15
Report Configuration	7-16
Configuring Reports	7-16
Deleting Report Configurations	7-17

CHAPTER 8**Using Application Classes** 8-1

Overview	8-1
About Application Classes	8-2
Processes Created by Application Classes	8-2
Removing Processes from Application Classes	8-2
Shell Scripts and Application Classes	8-3
Built-in Application Classes	8-4
Built-in Configurable Application Classes	8-7
Configuring Static Application Classes	8-8
Dynamic Application Classes	8-12
Defining Dynamic Classes	8-13
Configuring Dynamic Application Classes	8-14
Configure an Application-Builder Rule	8-17
Configure a Rule Using a Dynamic Application Class	8-21
Create New Application Classes from Rule Pages	8-22
Application Class Management	8-23

CHAPTER 9

Configuring Variables and State Conditions 9-1

- Overview 9-1
- Where Variables are Used 9-2
- COM Component Sets 9-4
 - COM Component Extract Utility 9-6
- Data Sets 9-7
- File Sets 9-12
 - Network Address Sets 9-18
 - Network Interface Sets 9-21
 - Network Services 9-24
 - Notification Settings 9-27
 - Query Settings 9-29
 - Notification and Query Tokens and Syntax 9-32
 - Localized Language Version Support 9-35
 - Registry Sets 9-35
 - Setting State Conditions 9-40
 - System State Sets 9-40
 - User State Sets 9-46

CHAPTER 10

Event Logging and Alerts 10-1

- Overview 10-1
- The Event Log 10-2
 - Filtering Events 10-5
 - Event Aggregation and Suppression 10-9
 - Graphing Similar Events 10-11
 - Reading Event Details 10-13
 - Reading Packet Details 10-14
- Event Monitor 10-14

Event Analysis	10-15
Viewing Events Using the Event Analysis Filter	10-15
Configuring An Event Analysis Filter	10-16
Event Managing Tasks	10-17
How Logging Works	10-21
Verbose Logging	10-22
Logging and Query User Rules	10-22
About the Event Management Wizard	10-23
Creating Exception Rules	10-24
Configuring Exceptions	10-30
Perform an Application Behavior Investigation	10-33
Suppressing Similar Events	10-36
Purge Similar Events	10-38
Event Sets	10-39
Third Party Access to Events	10-43
Configuring Alerts	10-45
Generate an Alert Log File for Third Party Applications	10-50

CHAPTER 11**Generating Reports** **11-1**

Overview	11-1
Types of Reports	11-2
Viewing Reports	11-2
Generating Reports	11-3
Events by Severity	11-3
Events by Group	11-5
Host Detail	11-6
Policy Detail	11-7
Group Detail	11-8
Clam AntiVirus Reports	11-9

Data Loss Prevention Reports	11-14
Signature Information Detail	11-19

CHAPTER 12

Using Management Center for Cisco Security Agents Utilities 12-1

Overview	12-1
Start and Stop Server Service	12-2
Start and Stop Agent Service	12-2
Backing Up Configurations	12-3
Restoring Backup Configurations	12-6
Database Maintenance (Free Up Disk Space on CSA MC)	12-8
Using the Webmgr Utility	12-10
Using the COM Extract Utility	12-11
Manual Agent Data Filter Installation	12-11
Internet Information Services Installation for Windows Vista	12-12
Install Data Filter on Windows	12-13
Uninstall Data Filter on Windows	12-13
Install Data Filter on Linux	12-14
Uninstall Data Filter on Linux	12-15
Install Data Filter on Solaris	12-16
Uninstall Data Filter on Solaris	12-16
Exporting and Importing Configurations	12-17
Exporting Configurations	12-17
Importing Configurations	12-19
View Import History	12-21
Cisco Security Agent Posture Plug-in for CTA	12-22

CHAPTER 13

Using Cisco Security Agent Analysis 13-1

What is Analysis	13-1
------------------	------

The Application Deployment Investigation Process	13-3
Reporting Categories	13-3
Turning Application Deployment Investigation On	13-4
Configure Group Settings	13-4
Configure Product Associations	13-7
Associate Unknown Applications	13-10
About Data Management	13-11
Generating Application Deployment Reports	13-12
AntiVirus Installations Report	13-13
Installed Products Report	13-14
Unprotected Hosts Report	13-16
Unprotected Products Report	13-18
Product Usage Report	13-19
Network Data Flows Report	13-21
Network Server Applications Report	13-23
Viewing Reports	13-25
Exporting Reports	13-25
What is Application Behavior Investigation	13-26
How Application Behavior Investigation Works	13-26
The Application Behavior Investigation Process	13-26
Behavior Analyses	13-27
Creating, Saving, and Cancelling Analysis Data	13-28
Configure a Behavior Analysis Investigation	13-29
Start Behavior Analysis	13-33
Importing the Rule Module	13-33
Application Behavior Reports	13-34
Report Components	13-34
Working with Reports	13-37
The Behavior Analysis Rule Module	13-37

Reviewing the Rule Module	13-37
Behavior Analysis Methodology	13-38

CHAPTER 14

Automatic Signature Generation 14-1

Overview	14-1
Basics	14-3
Automatic Signature Generation	14-3
Preventing Denial of Service Attacks	14-4
Stack Recovery	14-5
Protected Interfaces	14-5
Untrusted vs. Unchanged Payloads	14-6
Signature Confidence Levels	14-6
Signature Grouping and Tagging	14-7
Refining Signatures	14-7
Permanent and Expiring Signatures	14-7
Offline Agents and Correlated Signatures	14-8
Differences Between Signature-based AntiVirus and Automatic Signature Generation	14-8
Managing Global and Local Signatures	14-9
Managing Global Signatures	14-11
Managing Local Signatures	14-17
Importing, Exporting, and Upgrading Signatures	14-17
Signature Reporting	14-18
Deploying the Signature Feature	14-18
Distinguish Legitimate Signatures from False Positives	14-19
Use the Wizard to Create Exceptions for Generated Signatures	14-20

CHAPTER 15

AntiVirus Protection 15-1

Overview	15-1
----------	------

AntiVirus Basics	15-2
Signature-based AntiVirus	15-2
Behavior-based AntiVirus	15-3
Enabling AntiVirus Protection	15-3
How AntiVirus Signatures are Updated	15-4
Signature-based Scanning for Viruses	15-5
AntiVirus Tagging	15-7
The @virusscan Token	15-8
Quarantined Files	15-9
Differences Between Signature-based AntiVirus and Automatic Signature Generation	15-10
Administrative Signature-based AntiVirus Tasks	15-10
Scheduling a Background Scan	15-11
Performing an On-Demand AV Scan	15-12
Identifying a Host AntiVirus Scan Schedule	15-13
Forcing a Signature Update for a Group	15-13
Forcing a Signature Update for a Host	15-13
Creating Exemptions for AntiVirus Tags	15-14
AntiVirus Reporting	15-17
Creating Signature-based AntiVirus Rules and Components	15-17
Creating Virus Scanning Rules	15-18
Configuring Behavior-based AntiVirus Policy	15-27
End-user AntiVirus Tasks	15-28

CHAPTER 16**Data Loss Prevention** **16-1**

Overview	16-1
Data Loss Prevention Basics	16-3
Enabling Data Loss Prevention Protection	16-3
Scanning Data Tags and Static Data Tags	16-4

Scanning Data Tag Search Patterns	16-5
The @datascan Token	16-9
Managing Scanning Data Tags	16-9
Data Classification - Scanning Data Tags List Page	16-9
Built-In Data Scanning Tags	16-11
Creating a Scanning Data Tag	16-11
Editing a Scanning Data Tag	16-12
Cloning a Scanning Data Tag	16-13
Deleting a Scanning Data Tag	16-14
Managing Static Data Tags	16-14
Data Classification - Static Data Tags List Page	16-14
Adding Descriptions to Static Data Tags	16-15
View References to Static Data Tags	16-15
Data Loss Prevention Scanning Tasks	16-16
Scheduling a Background DLP Scan	16-16
Performing an On-Demand DLP Scan	16-17
Identifying a Host's DLP Scan Schedule	16-18
Identifying a Group's DLP Scan Schedule	16-18
Data Loss Prevention Reporting	16-19
Creating Data Loss Prevention Rules and Components	16-19
Creating File Access Control Rules to Apply Scanning Data Tags	16-19
Creating File Access Control Rules to Apply Static Data Tags	16-22

CHAPTER 17

Cisco Partner and Third Party Product Integration 17-1

Overview	17-1
Cisco IPS Integration Support	17-2
Cisco VPN Client Support	17-2
Cisco MARS Integration Support	17-3
netForensics Integration Support	17-3

CHAPTER 18

Using the Scripting Interface (CSAAPI) 18-1

Overview 18-1

CSAAPI/Scripting Overview 18-2

API Function Summary 18-3

Scripting Interface Fundamentals 18-4

Before You Begin 18-4

WSDL/SOAP 18-5

Choosing a Scripting Language 18-6

Sample Scripts and README Files 18-7

Encryption and Authentication 18-8

Object Expressions 18-9

Object Types 18-10

Supported Names per Object Type 18-10

Object Expression Values 18-12

Object Type Names 18-16

Wildcarding 18-17

Using the Escape Character 18-17

Using the Limit Name to Prevent Unwanted Actions 18-19

Blocking vs. Non-blocking 18-19

API Function Descriptions 18-21

Getting the Status of Functions and Waiting for Functions to Complete 18-21

Testing Object Expressions 18-23

Modifying the State of the Overall System 18-24

Host Group Assignment 18-27

Manipulating Hosts 18-29

Getting Host Information 18-30

Getting Overall System Information 18-32

Getting Event Information 18-33

Getting Reports 18-33

APPENDIX A

Cisco Security Agent Overview A-1

Overview	A-1
Downloading and Installing	A-2
The Agent User Interface	A-8
Agent User Interface Control Rule	A-8
Agent User Interface Screens	A-9
Assigning Sounds to Agent Events	A-29
Cisco Security Agent Diagnostics	A-29
Resetting Cisco Security Agent	A-30
Cisco Security Agent Shortcut Menu	A-30
Turn Agent Security Off	A-31
Installing the Windows Agent	A-32
Uninstalling the Windows Agent	A-33
Agent Interaction with Windows Security Settings	A-33
Agent Disables Windows Firewall	A-33
Agent Status is not Reported in the Security Center	A-34
Common Windows Cisco Security Agent Error Codes	A-34
Installing the Solaris Agent	A-35
Uninstalling the Solaris Agent	A-36
UNIX Agent csactl Utility	A-37
Installing the Linux Agent	A-39
Uninstall Linux Agent	A-40
Command line method	A-40
GUI method	A-41

APPENDIX B

System Components B-1

Overview	B-1
CSA MC Components	B-2

APPENDIX C

Agent Components **B-4**

Open Source License Acknowledgements and Third Party Copyrights **C-1**

OpenSSL/Open SSL Project **C-2**

License Issues **C-2**

Apache [version 2.0.59] **C-5**

TCL license **C-9**

Perl **C-10**

Socket6 **C-10**

libpcap **C-11**

CMU-SNMP Libraries **C-12**

Open Market FastCGI **C-13**

CGIC License **C-14**

Mozilla 1.xx (libcurl) **C-14**

MICROSOFT SOFTWARE LICENSE TERMS **C-15**

.Net Framework 2.0 **C-19**

MarshallSoft Computing SMTP/POP3 Email Engine **C-20**

Jasper Reports V1.2.0 and JFreeChart V1.0.5 **C-21**

iText version 1.3.1 **C-32**

Java Runtime Environment JRE 1.5.0.06 **C-42**

The GNU General Public License (GPL) **C-46**



Preface

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

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

Audience

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

Conventions

This manual uses the following conventions.

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



Tip

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



Note

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



Caution

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>



CHAPTER 1

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](#)
- [Communicating Over Secure Channels, page 1-8](#)
- [Distributing Policy Updates, page 1-9](#)

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	<ul style="list-style-type: none">ping server IP addressesrun traceroute on IP addressessniff passwordsimpersonate mail users
Penetrate	<ul style="list-style-type: none">email attachmentsJava applets and ActiveX controlsbuffer overflowsbackdoors and trojans
Persist	<ul style="list-style-type: none">weaken security settingsinstall new services
Propagate	<ul style="list-style-type: none">emailInternet connectionsIRCFTPinfected file shares
Paralyze	<ul style="list-style-type: none">reformat disksdestroy or corrupt datadrill security holescrash computersconsume work cyclessteal 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

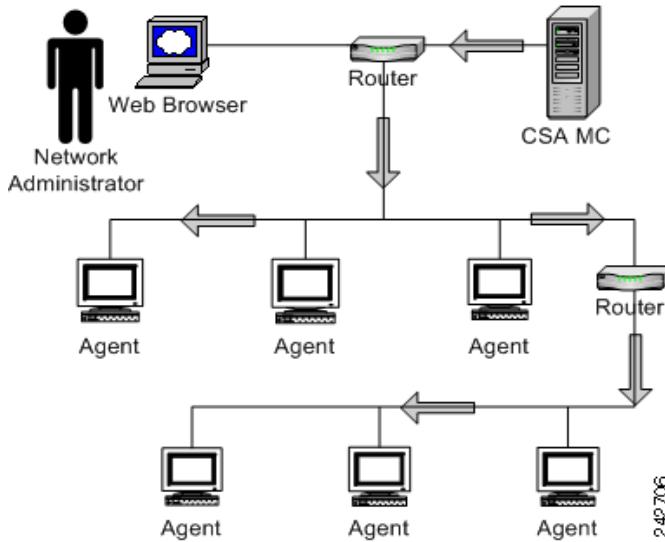
Management Center for Cisco Security Agents contains two components:

- CSA MC—installs on designated Windows 2003 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

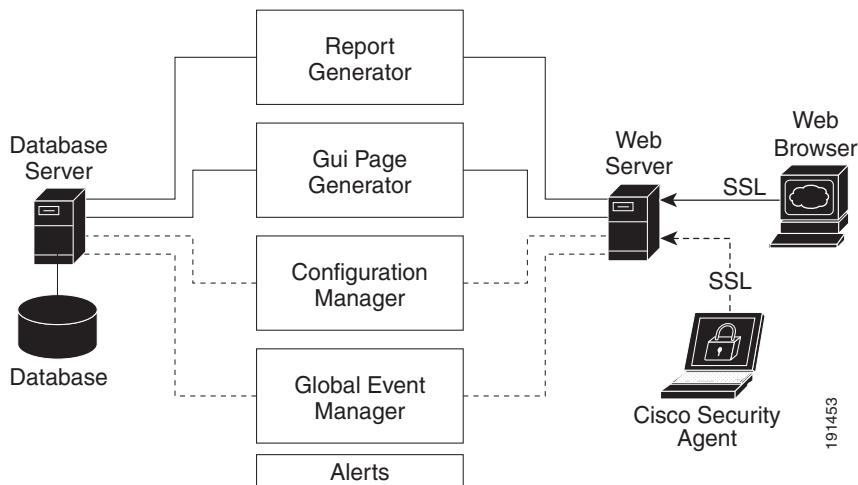
The CSA MC architecture model consists of a central management center which maintains a database of policies and system nodes, all of which have Cisco Security Agent software installed on their desktops and servers.

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

191453

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)
Cisco Security Agent Windows Architecture

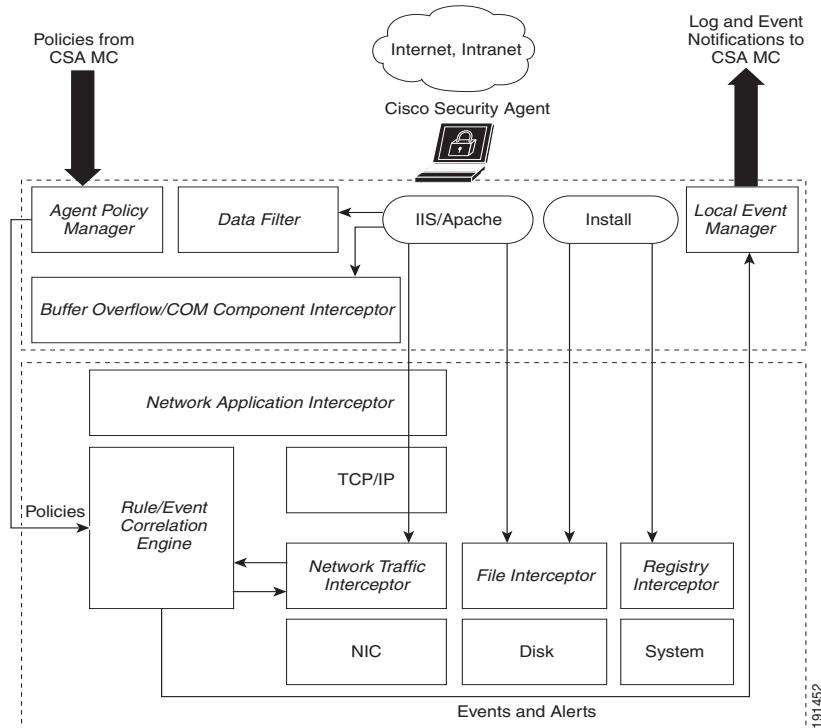
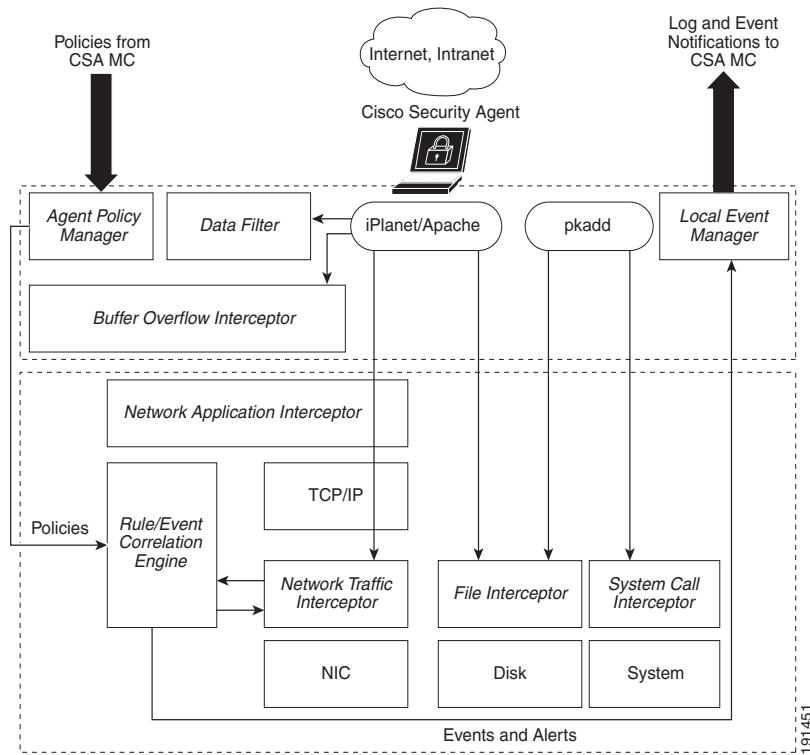


Figure 1-4 Cisco Security Agent Software Architecture (UNIX)
Cisco Security Agent UNIX Architecture



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.

Distributing Policy Updates



CHAPTER 2

Management Center for Cisco Security Agents Administration

Overview

Management Center for Cisco Security Agents (CSA MC) provides centralized management for Cisco Security Agents installed on endpoints throughout your organization. All Cisco Security Agent policies are configured and deployed through the CSA MC web-based user interface.

CSA MC's web-based user interface can be accessed from any computer connected to the Internet and running a web browser. Multiple administrators can be logged on to CSA MC simultaneously. Administrators must identify themselves and authenticate to CSA MC before they can access any CSA MC configuration data.

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.

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.

CSA MC also provides a reporting tool, letting you generate reports with varying views of your network enterprise health and status.

This section contains the following topics:

- [Browser Requirements, page 2-3](#)

- [Accessing Management Center for Cisco Security Agents, page 2-4](#)
- [Simple View and Advanced View Modes, page 2-5](#)
- [Interface Overview of Management Center for Cisco Security Agents, page 2-5](#)
 - [Home Page, page 2-5](#)
 - [Global Command Buttons, page 2-10](#)
 - [Menu Bar, page 2-10](#)
 - [Heading Links, page 2-14](#)
- [Configuring Role-Based Administration, page 2-14](#)
 - [Changing Administrator Passwords, page 2-18](#)
 - [Configure Monitor Role Administrator Access Restrictions, page 2-19](#)
 - [Manage Administrator Active Login Sessions, page 2-20](#)
 - [Administrator LDAP Authentication, page 2-21](#)
- [Distributing Cisco Security Agents, page 2-23](#)
 - [How Cisco Security Agents are Distributed, page 2-24](#)
 - [Host Security Page, page 2-24](#)
- [System Monitoring, page 2-27](#)
 - [Home Page, page 2-27](#)
 - [Status Summary, page 2-27](#)
 - [Event Log, page 2-31](#)
 - [Reports, page 2-32](#)
 - [Using Audit Trail, page 2-32](#)
- [CSA MC Page Types, Tasks, and Shortcuts, page 2-33](#)
 - [List View Pages, page 2-33](#)
 - [Configuration View Pages, page 2-33](#)
 - [Creating, Saving, and Deleting Data, page 2-34](#)
 - [Configuration Task Menus, page 2-35](#)
 - [Shortcuts and Hints, page 2-36](#)
- [Using Search, page 2-39](#)

- [Using CSA MC Utilities, page 2-41](#)
- [Using the Correct Syntax, page 2-41](#)
 - [Object Names, page 2-41](#)
 - [Configuration Variable Names, page 2-41](#)
 - [Special Character Syntax, page 2-42](#)
 - [Directory and Filename Syntax Requirements, page 2-43](#)
 - [File and Directory Protection, page 2-48](#)
 - [Data Set Interface Matching Syntax, page 2-55](#)
 - [Data Set Pattern Matching Syntax, page 2-55](#)
 - [Content Matching in File Sets, page 2-57](#)
 - [Network Address Set Syntax Requirements, page 2-50](#)
 - [Network Services Syntax, page 2-53](#)

Browser Requirements

The browser you use to access CSA MC 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.
- Pop-up blockers must be disabled.
- JavaScript must be enabled.

Firefox:

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

Accessing Management Center for Cisco Security Agents

An initial administrator account was created as part of the CSA MC installation process. Use that administrator account to log into CSA MC.

You access CSA MC locally or remotely from a supported Web browser. No more than 12 users may be logged on to the CSA MC at the same time.

- To access CSA MC locally, double-click the shortcut icon created on the desktop during the installation.
- To access CSA MC from a remote location, launch a browser application and enter

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

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

The CSA MC login appears. Enter your administrator account name and password in the edit fields provided in the initial screen.

**Note**

When you login to the CSA MC system, you are presented with the CSA MC Home page. Various messages or warnings may appear in the Things to Do area. See [Home Page, page 2-5](#) for more information.

**Tip**

Once you have logged on, look at the global command buttons in the top right corner of the Home Page. One will indicate “All OSes,” “Windows,” or “Unix.” Click the command button to view the components relevant to the operating system you choose. Clicking Unix displays components for both Solaris and Linux operating systems.

**Caution**

If you have not obtained a valid license from Cisco, when you login to CSA MC, you’ll receive a warning informing you that your license is not valid. Any newly deployed agents will not be able to register with the unlicensed CSA MC. Refer

back to “Licensing Information” in Chapter 2, Installing the Management Center for Cisco Security Agents, in *Installing Management Center for Cisco Security Agents* for further licensing information.

See [Configuring Role-Based Administration, page 2-14](#) for user-management tasks such as [Changing Administrator Passwords](#).

Simple View and Advanced View Modes

When you first login to CSA MC, the administrator created during the installation process has a simplified view of CSA MC. This “Simple Mode” view provides everything you need to deploy and administer the product. Default groups are pre-configured and shipped with the MC to provide out-of-the-box security policies for servers and desktops. Through the use of a wizard, you can refine the policies to match the security needs of your site and of the applications that run on your network.

For advanced users there is the “Advanced Mode” view. This view exposes all CSA MC menus and pages to administrators. This gives the administrator the ability to create or configure any component, view all possible reports, and have access to the full range of analytical and maintenance utilities. Advanced view is best for administrators who need to create customized policies for their enterprise or who want more granular control of the system.

Interface Overview of Management Center for Cisco Security Agents

This section describes the prominent and commonly used features of the CSA MC interface.

Home Page

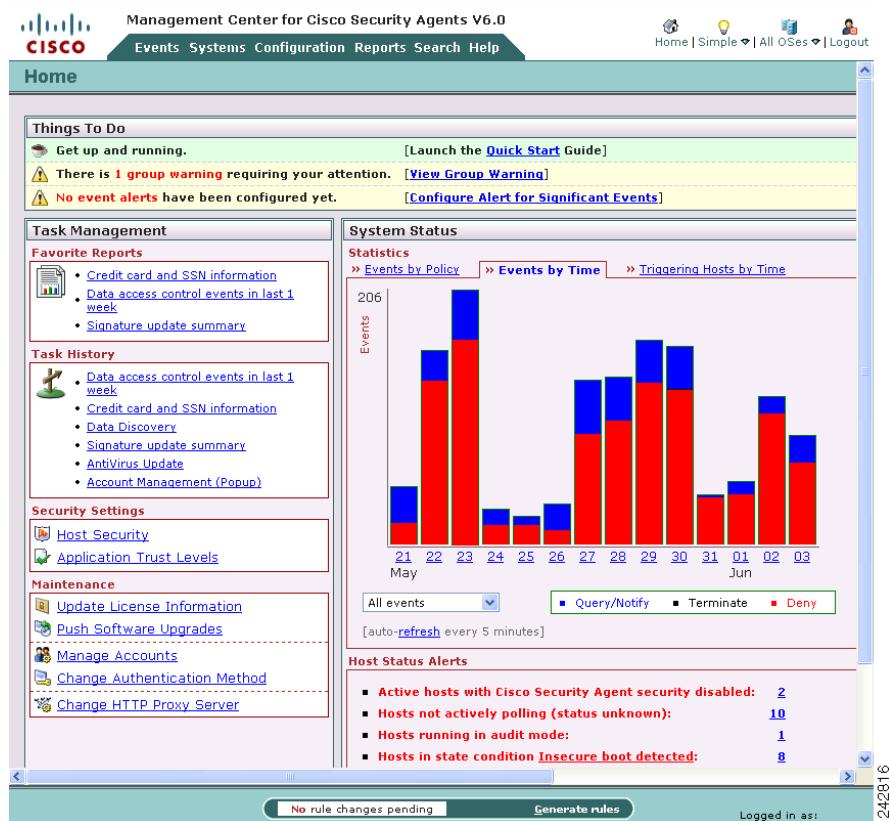
Upon first logging in, administrators are directed to CSA MC’s Home page. The Home page facilitates CSA Administrators’ work by pointing out and prioritizing problem areas, summarizing recent security events, and providing convenient

■ Interface Overview of Management Center for Cisco Security Agents

links to common tasks and reports. The Home page is available to both Advanced Mode and Simple Mode users. Administrators can reach the Home page from anywhere in the CSA MC interface by clicking the Home button.

The Home page is broken into three sections: Things To Do, Task Management, and System Status. See [Figure 2-1](#).

Figure 2-1 **Home Page**



Things to Do

The Things To Do area provides links to information or to administrative tasks that need your attention. There are three levels of tasks: red, yellow, and green. The red tasks are the most urgent, the yellow tasks are the next most urgent, and the green tasks are for your information. Though this list of tasks is prioritized, CSA MC does not force you to perform them in any particular order.

Clicking the link in the task row launches a pop-up window from which you can perform the entire task or a pop-up window with links to sub-tasks. If you need help performing a task, many pop-up windows provide help by right-clicking the background of the pop-up window and then clicking Help in the shortcut menu.

Task Management

These are the task management areas:

- [Favorite Reports](#)
- [Task History](#)
- [Security Settings](#)
- [Maintenance Tasks](#)

Favorite Reports. The Favorite Reports area provides links to reports that are configured with the “Put this report on the Home page favorite list.” check box selected. If there is a report that you would like to list here, follow this procedure:

1. From the CSA MC menu click the Reports menu and navigate to the report that you want to display on the home page.
2. Select the **Put this report on the Home page favorite list** check box.
3. Click **Save**. You do not need to generate rules for this configuration to take effect.

Task History. Generally speaking, the Task History area lists the last six pages that you viewed for at least three seconds. A link to a page that you used to configure the CSA MC will be displayed in the Task History but the page you clicked-through on your way to that configuration page will not be included in the Task History list.

The Task History list contains pages that are visible for the viewing mode you are using. Therefore, a page that you viewed in Advanced Mode will not be visible in the Task History area when you are using Simple Mode.

If you can't recognize the destination of a link displayed in the Task History area, mouse-over the link to view a short description in a tool-tip.

Security Settings. There are tasks available to you in the Security Settings area:

- Host Security - Clicking this link pops up the Host Security page. This page allows you to select the policies associated with a group and to make agent kits and groups using a wizard.
- Application Trust Levels - Clicking this link pops up the Application Trust Levels page. This page allows you to define applications as those you trust, those you aren't sure of, and those you don't trust by adding the applications to a White list, Grey list, or a Black list.

If you need help with these tasks, right-click the background of the pop-up window and click Help in the shortcut menu.

Maintenance Tasks. These are the tasks available in the Maintenance area:

- Update License Information - Clicking this link launches a pop-up window in which you can upload your site licenses.
- Push Software Upgrades - Clicking the link launches a pop-up window in which you can manage software updates using a wizard.
- Manage Accounts - Clicking this link brings you to a complete list of CSA MC accounts.
- From the list, you can click the links to CSA MC users to configure them.
- Change Authentication Method - Clicking this link allows you to configure an LDAP server against which CSA MC users can authenticate their user credentials.
- Change HTTP Proxy Server - Clicking this link allows you to specify an HTTP Proxy Server for the CSA MC so that it can reach the Clam AntiVirus mirror and so that it can properly display Call Stack information for the details of an event.

The CSA MC's Proxy Server setting is independent of your web browser's proxy server setting, which is used by your browser to reach external web sites. Note that your web browser may reside on a different machine from the CSAMC server, and as such, the two proxy settings could be different.

To specify a HTTP proxy server, enter the domain name of the proxy server and the port on which it allows access to the Internet. Click **Save**. Clicking **Test** will test the connection to the proxy server and you will receive a message in the case of success or failure.”

If you need help with these tasks, right-click the background of the pop-up window and click Help in the shortcut menu.

System Status

The System Status area summarizes event statistics and host status alerts.

Statistics. The Statistics area graphically displays information about CSA's query, deny, and terminate actions.

- Events By Policy - This tab lists your most-active policies as measured by the number of event triggered. Each policy's bar in the graph corresponds to the number of triggered events grouped by action (deny, terminate and query).
In Simple mode, only the policies that are configured to be displayed in Simple Mode report their events in the Events by Policy tab. In Advanced Mode, the events from all policies are reported in the Events by Policy tab. Click the policy name link to view the contents of the policy. Click a color in the bar chart to view the events related to the event type. Click the total number of events link to view all the events associated with the policy.
- Events By Time - This tab displays the number of query, deny, and terminate events reported per day. Click a color in the bar chart to view the events related to the event action. Click the total number of events link to view all the events reported on a particular day.
- Triggering Hosts By Time - This tab displays the number of hosts that have reported query, deny, and terminate events per day.

Host Status Alerts. The Host Status Alerts area displays a number of trouble-areas that require attention. Click the number at the end of the task to view the hosts affected by the different alerts.

Global Command Buttons

The command buttons at the top right of the CSA MC user interface provide quick access to the Home page, the ability to toggle between Simple and Advanced Mode, a way to filter information by operating system, and a logout button. These command buttons are displayed on every page.

The buttons that filter your view of the CSA MC user interface affect all the pages you visit while you are logged in or until you change the filter. For example, if you select Windows from the Operating System filter, only Windows components will be visible on the pages you visit. Likewise, if you choose the Simple view from the Advanced/Simple toggle button, you will only be able to visit pages visible in Simple Mode.

Figure 2-2 Global Command Buttons

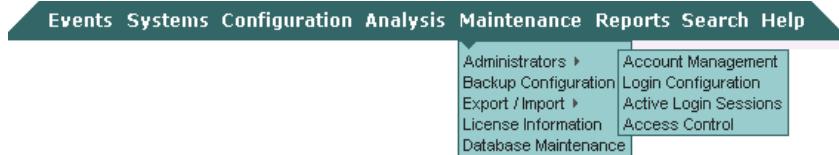


Menu Bar

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 2-3](#)). 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.

The menu bar for Advanced Mode displays all menus and submenus. The menu bar for the Simple Mode displays only those menus and submenus intended for the Simple Mode users.

Figure 2-3 **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. You can also set alerts and alert parameters from here. (See [Chapter 10, “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. These menus 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 8, “Using Application Classes.”](#))

Configuration>Variables. 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 9, “Configuring Variables and State Conditions.”](#))

Configuration>Global Settings. The items in the Global Settings menu provide configuration tools used to categorize and apply tags to processes, files, and IP addresses and to correlate events across multiple systems. When tags are applied and certain correlation rules are triggered, the MC registers this occurrence and automatically builds application classes or tokens and sends them out to Cisco Security Agents. In some cases, the MC can prevent actions from executing on any additional systems based on noticing the action taking place on a small number of systems. (See [Chapter 7, “Using Global Settings.”](#))

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 13, “Using Cisco Security Agent Analysis.”](#))

Maintenance. The items available from the Maintenance drop-down list let you administer CSA MC user accounts, 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 [Configuring Role-Based Administration, page 2-14](#), 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 11, “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.

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. The Help available in Advanced Mode provides all help topics. The Help available in Simple Mode only provides help topics for those features and functions available to the Simple Mode user.

**Note**

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

Figure 2-4 Main Help System

The screenshot shows the 'Main Help System' interface. On the left is a sidebar with 'CONTENTS', 'INDEX', and 'SEARCH' buttons. Below these are links to 'Product Overview', 'CSA MC Administration' (which is expanded to show 'Simple Mode and Advanced Mode', 'Home Page', 'Status Summary', 'Host Security', 'Monitor Role Administrator Access', 'Manage Administrator Active Login', 'Using the Correct Syntax', 'Using Search', 'License Information', 'Available Software Updates', 'Groups and Hosts', 'Policies and Rule Modules', 'Global Settings', 'Event Logging and Alerts', 'Reports', and 'Data Classification'), and 'Help' buttons. The main content area has a title 'Home Page'. It describes the goal of the CSA MC Home page and its sections: 'Things To Do', 'Task Management', and 'System Status'. It also explains how to reach the Home page from anywhere in the CSA MC interface by clicking the 'Home' button. The 'Things To Do' section lists tasks prioritized by color (red, yellow, green). The 'Task Management' section lists areas like 'Favorite Reports', 'Task History', 'Security settings', and 'Maintenance'. The 'Favorite Reports' section provides instructions for adding reports to the home page. A status bar at the bottom right shows the number '242818'.

Heading Links

The heading link contains hierachal links for the item you are configuring. Use these header links to switch between top level list views and subcategory configuration views. For example, in [Figure 2-5](#), the header bar contains links to the top level Reports list view and the group of reports referred to as DoS Detail.

Figure 2-5 Heading Link



Configuring Role-Based Administration

Administrators can have different levels of CSA MC database access privileges. The initial administrator created by the CSA MC installation automatically has “Configure” privileges and views the CSA MC in Simple Mode. When you create new administrators on the system, you can give them one of the following roles.

CSA MC Administrator Roles:

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

Create new administrator accounts or manage existing ones by doing the following:

Step 1 Log on to the CSA MC and switch to Advanced Mode.

Step 2 From the CSA MC menu bar, go to **Maintenance>Administrators>Account Management**. The administrator created during the installation should already exist in the list page.

Step 3 Click the **New** button to create a new administrator account or click on an existing account to edit it.

Step 4 For each new administrator you create, enter the following information (see [Figure 2-6](#)):

- **Login Name** - This is the name the administrator uses each time he/she logs into the database. (This name must be unique.)
- **LDAP Login Name** - If the LDAP login name is different than the Login Name for this account, enter the LDAP login name to which this account corresponds.
- **Role** - Configure role-based administration privileges for this administrator. The options are configure, deploy, and monitor privileges.
- **Description** - This is an optional line of text that is displayed in the list view and helps you to identify this particular administrator.

Step 5 Configure administrator **Preferences** as follows

- **Automatically log out after X minutes of inactivity** — By default, administrator sessions time out after 15 minutes of inactivity. Enter a value here from 1 to 120 minutes to change the default.
- **Preferred OS View** — For this administrator, you can select to view configuration items for all operating systems or to view only those for a particular type of 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. Otherwise you may select Windows to view only Windows configuration items or UNIX to view only Solaris and Linux configuration items.
- **Show suppressed events** — Event suppression is best used when you have a reoccurring event that is more noisy than useful to you. When event suppression is enabled (this checkbox is not selected), all events of a particular type are no longer displayed in the event log. Suppressing an event removes all viewable instances of that event and causes further events of the same type to be hidden. Event suppression is configured through the Event Log Wizard. Select this checkbox to have all configured event suppression ignored and to display all events in the event log.

- **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.)

Step 6 Choose **Advanced** or **Simple** radio button to specify the preferred user mode for CSA MC. See [Simple View and Advanced View Modes, page 2-5](#) for more information.

Step 7 If you chose Advanced in the previous step, these additional preferences are available to you. All these preferences are optional.

- **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 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 **Show expanded configuration views** check box.

- **Show all configuration objects (hidden included)** — If you have hidden configuration items 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.



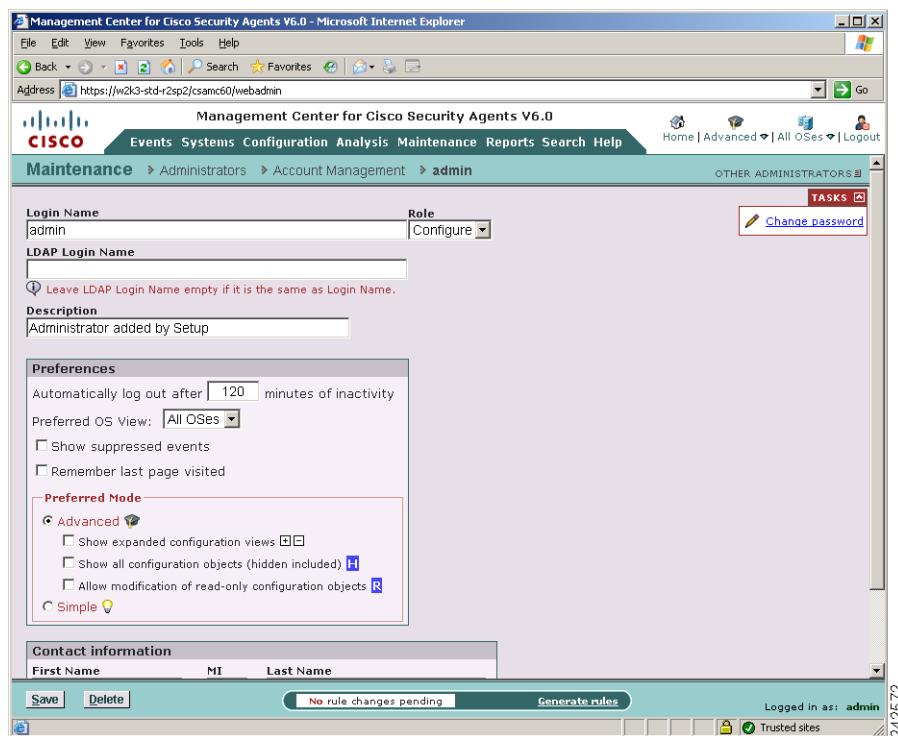
Note The **Change visibility** link in the tasks menu on configuration pages makes configuring CSA MC easier by paring down configuration items to only those you use most.

- **Allow modification of read-only configuration objects** — Administrators with “configure” privileges can select a Read-only option when configuring certain CSA MC objects. If an object is read-only, it cannot be edited or deleted. Selecting this checkbox allows the administrator in question to disable read-only specifications and edit or delete items marked as Read-only.

**Note**

Providing Read-only objects is intended to prevent the accidental modification of those objects. Configured objects (variables, rule modules, etc.) that ship with CSA are all marked as Read-only. This is done to discourage the altering of these pre-configured objects. You should use the administrator read-only override checkbox judiciously.

Figure 2-6 Administrator Account Management Window



2-02572

- Step 8** **Contact information (optional)** - Name, E-mail, Telephone number
- Step 9** Click the **Save** button.
- Step 10** Go to [Changing Administrator Passwords, page 2-18](#) to set the user's password.

Changing Administrator Passwords

You can set or change an administrator's password at any time by accessing that administrator's configuration page.

**Note**

If you are using LDAP authentication for administrators, it is not required that you set a password. However, if LDAP authentication fails, the administrator cannot login unless a local password is set as well (as a fallback authentication means).

-
- Step 1** From the **Maintenance** menu navigate **Administrators > Account management**.
- Step 2** On the Account Management list page, click the login name for the administrator whose password it is you want to change.
- Step 3** Expand the red **Tasks menu** at the top right of the page and click the **Set Password** link to define a password for this administrator.
- Step 4** In the Set Password dialog box:
- In the **Current Session Password** field, type the password of the current logged-in administrator that is entering the new administrator information, not the password of the administrator you are entering.
 - In the **New Password for Login Name** field, type the new password.
 - In the **Confirm Password** field, retype the new password.
- Checking the **Enforce password policy** checkbox places these constraints on the new password:
- Password cannot be the same as, or contain, the login name
 - Password must be between 6 and 32 characters long
 - Password must contain characters from at least three of the following classes:
 - lower case letters
 - upper case letters
 - digits
 - non-alphanumeric characters
- Step 5** Click the **Save** button.

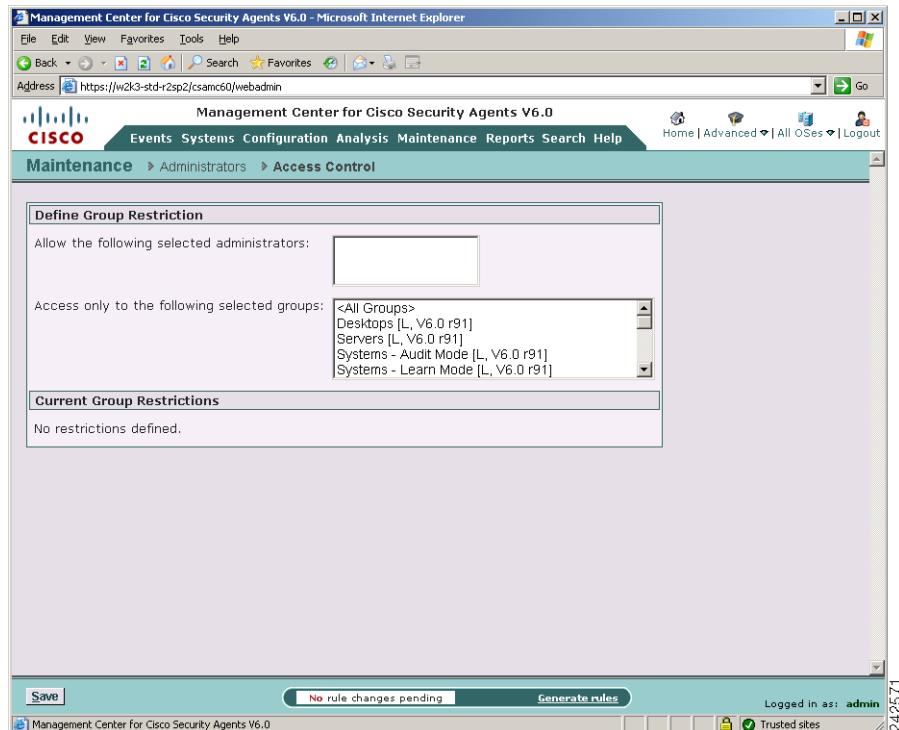
Configure Monitor Role Administrator Access Restrictions

You can configure CSA MC administrators with a Monitor role to have access to only those configuration items you wish to allow viewing of. Therefore, you can place extra restrictions on that administrator's performing of monitor tasks on CSA MC.

-
- Step 1** Log on to the CSA MC as a user with configure privileges and switch to Advanced Mode.
 - Step 2** From the CSA MC menu bar, go to **Maintenance>Administrators>Access Control**. The existing administrators configured to have a Monitor role appear in the administrator selection box in the Define Group Restrictions section.
 - Step 3** By selecting particular administrators and then selecting particular groups, you are indicating that the selected administrators can only view items pertaining to the selected 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.
All configured settings appear at the bottom of the single global page.

Configuring Role-Based Administration

Figure 2-7 Administrator Access Restrictions



Manage Administrator Active Login Sessions

You can view actively logged in CSA MC administrators and look at login information such as Role, Remote login address, the period of time for which the administrator has been logged in, and the time that has passed since the administrator has made changes on the system.

-
- Step 1** Log on to the CSA MC as a user with configure privileges and switch to **Advanced Mode**.
 - Step 2** From the CSA MC menu bar, go to **Maintenance > Administrators > Active Login Sessions**.

The list of logged in administrators appears. You can log an administrator out of the system by selecting the checkbox beside that administrator name and clicking the **Logout** button at the bottom of the page.

Administrator LDAP Authentication

The CSA MC default authentication method for authenticating administrators to the system is local database configuration authentication. This is when administrator names and passwords are entered via CSA MC. Alternatively, you can configure CSA MC to authenticate administrators using LDAP. You must already have a configured LDAP server that can communicate with CSA MC to use this authentication type. See [Figure 2-8](#).

**Note**

Configuring the CSA MC to authenticate administrators using your LDAP server requires knowledge of that server and the LDAP protocol. If you are unsure what the proper value is for one of the LDAP configuration fields, contact your system administrator.

To use LDAP authentication, do the following:

-
- Step 1** Log on to the CSA MC as an administrator with configure privileges and switch to **Advanced Mode**.
 - Step 2** Configure an administrator account on CSA MC using the steps described in [Configuring Role-Based Administration, page 2-14](#). If you are using LDAP authentication for administrators, it is not required that you set a password for the new administrator account. However, if LDAP authentication fails, the administrator cannot login unless a local password is set as well (as a fallback authentication means).
 - Step 3** On the MC, navigate to **Maintenance > Login Configuration**. This takes you the LDAP server configuration page. Once selected, this LDAP server authentication is global to the system. All administrators logging into CSA MC will first be authenticated to CSA MC using the LDAP server.
 - Step 4** To use LDAP authentication, select the **Use LDAP server for authentication** checkbox.
 - Step 5** In the **Base DNs** area, specify the users who can be authenticated.

For example, in the **User Prefix** field, enter:

CN=

and in the **Base DN** field enter:

DC=csaadmins, DC=mycompany, DC=com

If you specify more than one Base DN, CSA MC attempts to validate administrator logins, in order, against each entry in the Base DNs field. If administrators are not part of one organizational unit, CSA MC attempts to find them in the next organizational unit. As soon as an administrator's authentication attempt succeeds or fails against one Base DN, CSA MC makes no further authentication attempts.

- Step 6** (Optional) If you want to restrict access to the CSA MC to only one AD/LDAP group, select the **Group Restrictions** check box and specify that group's Attribute and Group DN name in the Attribute and Group DN fields in the Group Restriction area.

In AD/LDAP Attribute and Group DN can be derived from **ldif** file.

- Step 7** (Optional) You may configure LDAP User Search Mode by selecting the **LDAP User Search Mode** checkbox and configuring the relevant fields.

LDAP User Search Mode is useful if many users are scattered under different DNs. Administrators can specify a single Base DN in the Base DN field and use the LDAP User Search Mode with an account specification that can recursively check various DNs under the Base DN to authenticate users without having to specify all Base DNs.

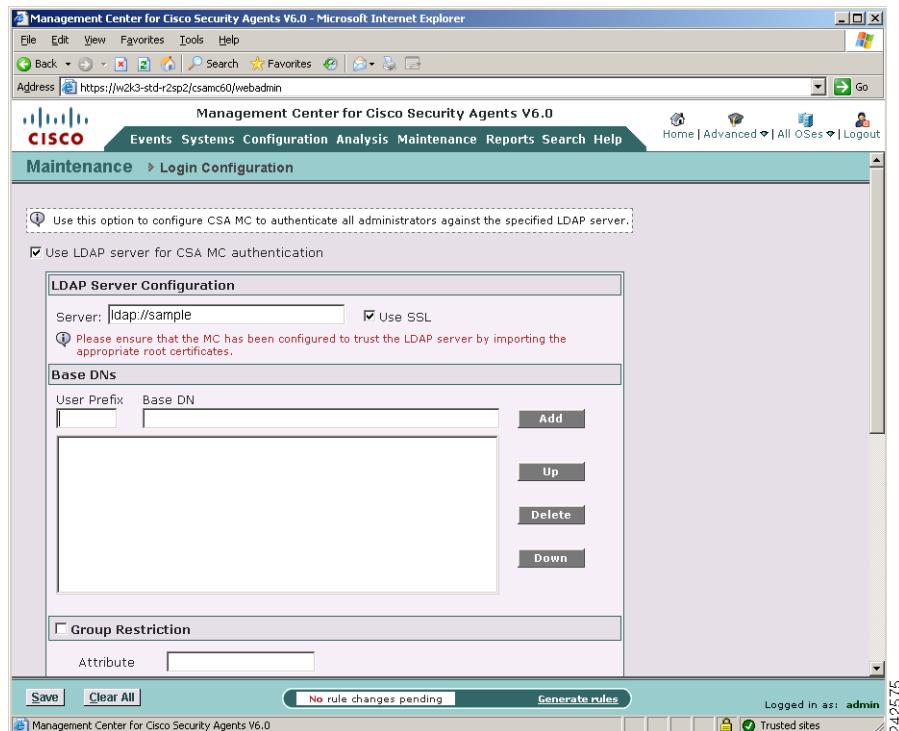
In the **User DN** field, enter the complete path. For example:

CN=Admin, DC=csaadmins, DC=mycompany, DC=com

In the **Password** field, enter the password for the administrator account that has privileges to search the LDAP directory. This is required if AD/LDAP is configured with only one account that is allowed to perform a recursive search on the LDAP directory.

- Step 8** (Optional) If you want to test LDAP authentication, select the **Test Configuration** checkbox and enter a login name and password that should be authenticated by the LDAP server based on this configuration

- Step 9** Click **Save**. If you specified a test account in the previous step, the save will only succeed if the test LDAP authentication succeeds.

Figure 2-8 Global LDAP Server Configuration

Distributing Cisco Security Agents

This section summarizes how Cisco Security Agent agent kits are distributed and describes the Host Security page which simplifies the process of distributing agent kits. For information about creating agent kits, begin with [Managing Agent Kits, page 3-12](#).

How Cisco Security Agents are Distributed

Cisco Security Agents are installed from a CSA agent kit. After the agent kit is installed on the host, the host is associated with a group and with the security policies assigned to that group. After the host is rebooted, it receives the full protection of all the security policies with which it is associated.

Some agent kits are provided by default. You may also create your own agent kits if you want to customize the mix of policies you assign to hosts.

See [Distributing Agent Kits, page 3-18](#) for more information.

Host Security Page

For Windows deployments, the Host Security page allows you to associate policies with groups, put groups and policies in Audit Mode, create agent kits and groups using a wizard. You can view the agent kits associated with a group by clicking the number of agent kits listed in the group row. If there are hosts associated with a group, you can view them by clicking the number of hosts listed in the group row. See [Figure 2-9](#) for more information.

Figure 2-9 Host Security Page

The screenshot shows the 'Host Security' page of the Management Center for Cisco Security Agents V6.0. The top navigation bar includes links for Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, Help, Home, Advanced, All OSes, and Logout. The main content area displays a table of policy groups:

Group	Version	OS	Type	Audit Mode	Hosts	Kits
<input checked="" type="checkbox"/> Deployed-Desktops		Windows		<input type="checkbox"/>	2	1
Policies <input checked="" type="checkbox"/> Anti-Rootkit (desktops) [V6.0 r193] <input type="checkbox"/> Anti-Sniffer [V6.0 r193] <input checked="" type="checkbox"/> Anti-Spyware [V6.0 r193] <input checked="" type="checkbox"/> Anti-Virus - Behavior based (desktops) [V6.0 r193] [warning] <input checked="" type="checkbox"/> Anti-Virus - Signature based (desktops) [V6.0 r193] <input checked="" type="checkbox"/> Audit System Integrity [V6.0 r193] <input type="checkbox"/> Block wireless bridging [V6.0 r193] [warning] <input type="checkbox"/> Block writing files to USB devices [V6.0 r193] <input checked="" type="checkbox"/> Data Loss Prevention [V6.0 r193] [warning] <input checked="" type="checkbox"/> Firewall - Centrally Managed (desktops) [V6.0 r193] [warning] <input checked="" type="checkbox"/> Firewall - User Managed [V6.0 r193] [warning] <input checked="" type="checkbox"/> Quarantine compromised applications [V6.0 r193] <input type="checkbox"/> Quarantine compromised hosts [V6.0 r193] <input type="checkbox"/> Require VPN for hosts on insecure networks [V6.0 r193] [warning]						
Hosts attached to this group: 2 hosts Available kits for this group: 1 agent kit <small>(Changes to this group will affect the hosts and kits referenced above.)</small>						
<input type="checkbox"/> Desktops	6.0 r193	Windows	<input type="checkbox"/>	<input type="checkbox"/>	0	1
<input type="checkbox"/> Servers	6.0 r193	Windows	<input type="checkbox"/>	<input type="checkbox"/>	0	1

Legend:
 Desktop Group Server Group

Buttons at the bottom: Save, New, Delete, 5 rule changes pending, Generate rules, Logged in as: admin, 242800.

Changing Policies Associated with Groups

Changing the policies attached to groups changes the kind of security enforced on the hosts that are members of that group.

If a host is a member of a group, changing the policies that are attached to the group will change the security enforced on the host after rules have been generated and after the agent has polled-in.

Step 1 Click the group you want to modify. The policies associated with a group are displayed.

Step 2 Select the check box for the policy you want to attach to the group or clear the check box for the policy you want to remove from the group.



Note You can mouse-over the policy name to read a short description of the policy.

- Step 3** If a policy you want to add to a group displays a [warning] link, click the warning link and follow the links in the Policy Warning pop-up box to rules that require customization.
- Step 4** Click **Save**.
- Step 5** Click **Generate rules** when you are ready to distribute the updates to hosts.

Displaying Groups and Policies on the Host Security Page

You can configure most groups and policies to be displayed on the Host Security page.

To configure groups to be displayed on the Host Security page:

-
- Step 1** Mouse-over the **Systems** menu and select **Groups**.
 - Step 2** Click the group you want to display on the Host Security page.
 - Step 3** Expand the **Simple Mode Settings** area.
 - Step 4** Select **Expose this group also in Simple Mode (on the Host Security page)**.
 - Step 5** Select the type of host for which this group is recommended.
 - Step 6** Click **Save**.

To configure policies to be displayed on the Host Security page:

-
- Step 1** Mouse-over the **Configuration** menu and then click **Policies**.
 - Step 2** Click the policy you want to display on the Host Security page.
 - Step 3** Expand the **Simple Mode Settings** area.
 - Step 4** Select **Expose this policy also in Simple Mode (on the Host Security page)**.
 - Step 5** Select the type of host for which this policy is recommended.
 - Step 6** Click **Save**.

Putting Groups and Policies in Audit Mode

Groups and policies can be placed in Audit Mode by checking their audit mode check box on the host Security page.

When a group or policy is running in audit 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 logging is enabled for the rule).

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 audit mode designation. See Audit Mode for more important information.

Creating Agent Kits and Groups Using a Wizard

Clicking the **New** button launches a wizard that helps you create a new group containing the policies you have chosen and a new agent kit to deploy that group to hosts. See [Creating Agent Kits and Groups Using a Wizard, page 3-16](#) for this procedure.

System Monitoring

This section describes some of the features you can use to monitor the hosts managed by CSA MC.

Home Page

The Home page provides an excellent summary of the system status. The Home page points out and prioritizes problem areas, summarizes recent security events, and provides convenient links to common tasks and reports. It also provides a System Status window that graphically displays event information. See [Home Page, page 2-5](#) for more information.

Status Summary

The Status Summary page supplies overall system summary information including recorded events and agent rule versions (see [Figure 2-10](#)). Advanced users can access this page at any time by selecting **Status Summary** from the **Events** menu. The various summary categories available from this page are as follows.

Network Status

Generally, items in the Network Status category do not appear in the list if their number is 0. Simply expand the Network Status view to see all available status items. The status items listed here generally have to do with overall host statistics such as hosts that are not running with up-to-date software versions or the latest rule programs. You can view the number of hosts running in audit mode or learn mode, etc. Additionally, the numbers that appear in this status section are clickable and take you to a list of the hosts that comprise that number.

Events recorded in the past 24 hours: The number listed here provides a link to the most recent events as described.

Host history collection enabled: Host history collection is a feature that you enable and disable from this page. You optionally, globally enable Host history collection for all hosts if you want to maintain individual host histories of the following types of information: host registration, audit mode setting changes, learn mode setting changes, IP address changes, CTA posture changes, CSA version changes, host active/inactive status changes.

When you enable Host history collection, a two week history of the previously listed host status changes is maintained for every host registered with the MC. Once this feature is enabled, to view a host's history, you access the details page for that host from **System>Hosts** in the menu bar and then click the link for that host. From the host details page, click the **Detailed status and diagnostics** link. A pop-up window lets you view collected host history information. See [Viewing General Host Statuses with CSA MC, page 3-27](#).



Note

Host history collection can cause your database to fill up faster if you have tens of thousands of hosts and an abundance of configuration changes.

Active hosts with Cisco Security Agent security disabled: The host is polling in at scheduled intervals and it is running the latest agent software and the latest policies, but agent security has been disabled and there is no policy enforcement.

Active hosts with the current configuration: The host is polling in at scheduled intervals and it is running the latest agent software and the latest policies.

Active hosts running an old configuration: The host is polling in at scheduled intervals and it is running the latest agent software but it has not downloaded the latest policies.

Active hosts running old software: The host is polling in at scheduled intervals and it is using the latest policies but it is not running the latest agent software.

Active hosts with software update pending: The host is polling in at scheduled intervals and it is using the latest policies but it is not running the latest agent software. It has a software update pending.

Unprotected hosts: The Cisco Security Agent on the host is not enforcing any policies or agent security as been disabled.

Hosts running in audit mode: This number of hosts are in audit mode. See [Using Audit Mode, page 5-44](#).

Hosts running in learn mode: This number of hosts are in learn mode. See [Using Learn Mode, page 5-48](#).

Hosts with BIOS supported boot detection: This number of hosts have BIOS supported boot detection enabled. See [Setting State Conditions, page 9-40](#).

Hosts in state condition Insecure boot detected: This number of hosts are in the Insecure boot detection state. See [Setting State Conditions, page 9-40](#).

Hosts in state condition Untrusted rootkit detected: This number of hosts are in the Untrusted rootkit detection state. See [Setting State Conditions, page 9-40](#).

Hosts in state condition Unprotected access detected: This number of hosts are in the Unprotected access detection state. See [Setting State Conditions, page 9-40](#).

Hosts with unsupported platform: These hosts are attempting run Cisco Security Agent software on an unsupported operating system.

Hosts without Cisco Trust Agent installed: These hosts do not have CTA software installed.

Hosts with Cisco Trust Agent installed but inactive: These hosts are running CTA software that is inactive and not providing a posture.

Hosts not actively polling (status unknown): These host are running agent software that has missed three polling intervals or has not polled into the CSA MC in 5000 seconds, whichever is greater. A host is also considered inactive if it has not polled in within 24 hours, no matter how many polling intervals it has missed. A host's polling status is updated on the CSA MC every hour.

Hosts without Application Deployment Investigation data upload: These hosts do not have Application Deployment Investigation enabled. See [Configuring Groups, page 3-4](#).

Groups with no policies attached: The MC has this number of groups configured with no policies attached and therefore no policy enforcement associated with these groups.

Query rules with saved answer in the past 24 hours: The number displayed here links to query rules that have triggered and been responded to on host systems.

Most Active

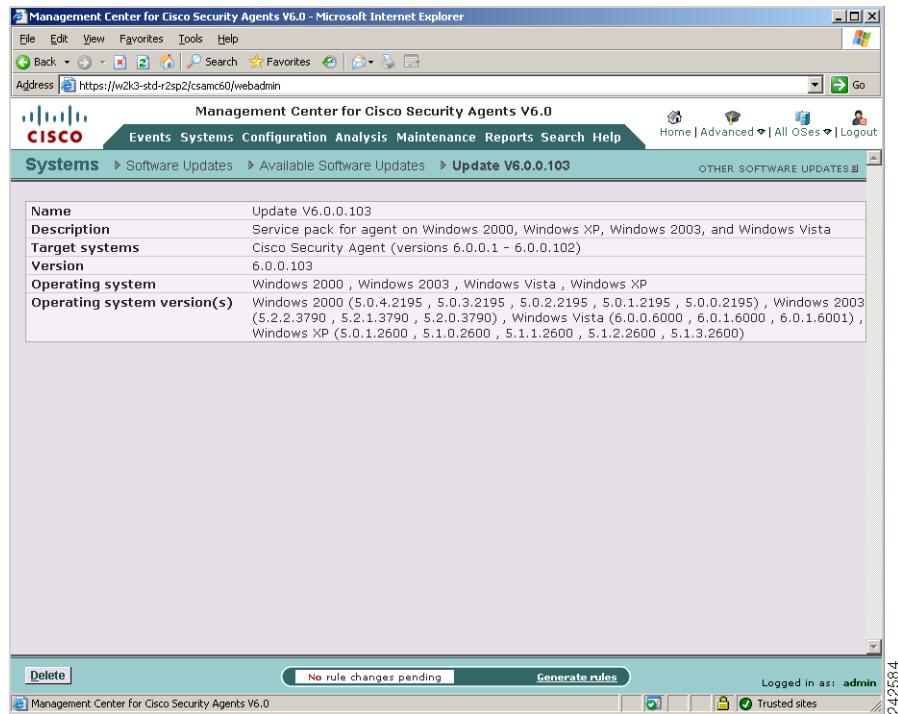
Use the links available in the Most Active section to view the Hosts, Rules, Applications, or Rule/Application pairs that have been the most active or triggered the most (logged the most events to the MC). This information is useful to help you tune your policies for rules that are being tripped too 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.

Event Counts Per Day

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.

Database Maintenance

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 12-8](#) for details.

Figure 2-10 Status Summary View

Event Log

From the Events menu, select **Event Log**. This displays the events reported by hosts registered with the CSA MC. This gives you a detailed view of what is happening throughout the system. See [Chapter 10, “Event Logging and Alerts”](#) for a full discussion of how to view, filter, and monitor events.

Reports

Click **Reports** in the CSA MC menu bar to view a complete list of report types that can help you monitor and analyze events reported to the CSA MC. See [Chapter 11, “Generating Reports”](#) for a complete discussion of what reports are available to you and how they can be configured.

Using Audit Trail

Advanced Mode users can access the Audit Trail page by selecting **Audit Trail** from the **Reports** menu. The Audit Trail page displays a list of changes administrators have made to the CSAMC 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. Note that you can select <All> here to display all entries. This may be useful if you intend to archive or save the audit trail data.
- Filter by included or excluded text.

CSA MC Page Types, Tasks, and Shortcuts

This section describes the kinds of page formats used in the CSA MC interface and the kinds of tasks the user can perform from those pages. Throughout the documentation, CSA MC pages are described using this terminology. This section also points out menus, shortcuts, command buttons, and navigation tips that Advanced Mode administrators will use in their every-day work.

List View Pages

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. From the list view, you click an item link to access the configuration page for that item.

Buttons for New, Clone, Delete, and Compare actions are present on list view pages. See [Creating, Saving, and Deleting Data, page 2-34](#) for further details.

**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.

Configuration View Pages

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 2-34](#) for further details.

Creating, Saving, and Deleting Data

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.

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.

If you are creating a new configuration item and you want to start over, clicking Delete removes the configuration item from the database. Simply navigating away from the configuration page will leave the configuration item behind, partially configured.

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 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.

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.

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.

Changes are stored in the database when you click Save. Some configuration changes that only affect the CSA MC are available immediately after they are saved. Other configuration changes are not available until you generate rules and the agents poll in for the new configuration.

Configuration Task Menus

In the configuration view for many configurable items, there is a Tasks menu in the upper right corner of the page. Clicking the down arrow, expands the menu. This menu provides quick links to common tasks that are relevant to the item being configured. There are many different task links, they are descriptive and largely self-explanatory.

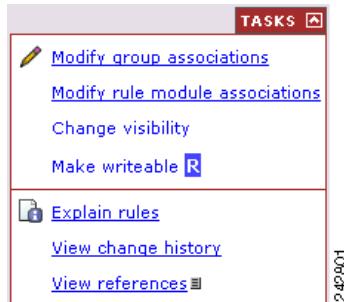
Figure 2-11 Policy Tasks Menu

Figure 2-11 shows an example of a Tasks menu for policies. Policies are associated with groups, so a link to **Modify group associations** is provided. Policies are made up of rule modules, so a link to **Modify rule module associations** is also provided.

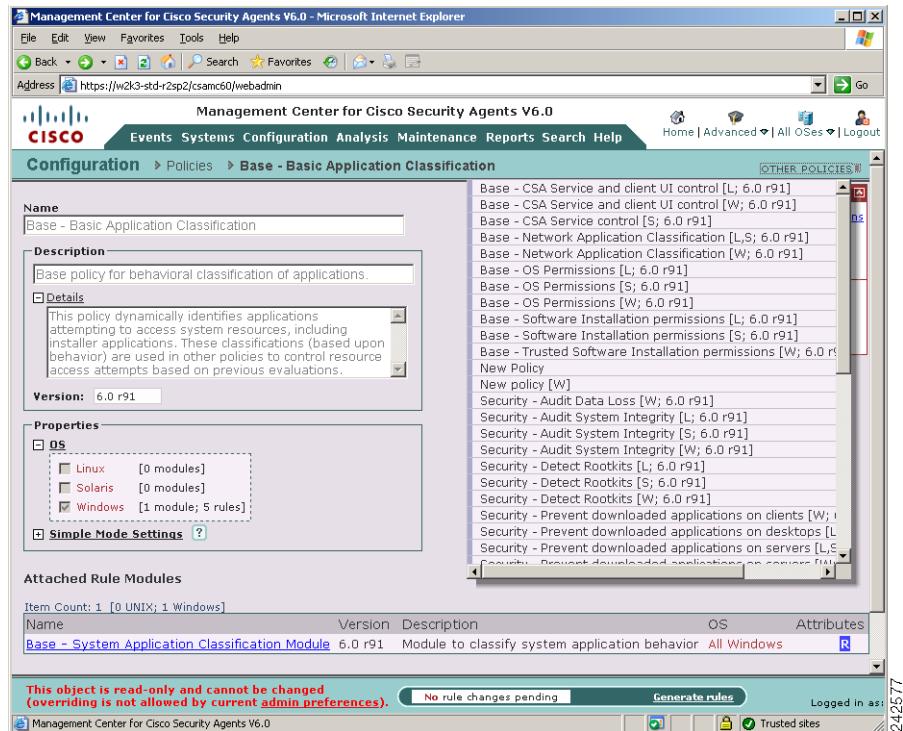
Change visibility and **Make writable** are common tasks for many different configuration items. **Change visibility** hides or exposes configurable items on the CSA MC interface. Make writable, allows an item that is read-only to be modified. Clicking the **View references** link displays all the configurations where the current item is used and provides links to those configurations.

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 2-12). 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 2-12 Other Policies Link

Configuration Shortcuts — Rule pages allow you to insert pre-configured variables such as file sets, data sets, and COM component sets. If there is no pre-configured variable that you wish to use and you want to create a new one while creating a rule, you can do so 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. Clicking **New** 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 also 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 2-13 Configuration Shortcuts

The screenshot shows the Management Center for Cisco Security Agents V6.0 interface. The title bar reads "Management Center for Cisco Security Agents V6.0". The menu bar includes Events, Systems, Configuration Analysis, Maintenance, Reports, Search, Help, Configuration, Rule Modules, Rule Module, and File access control [651]. A "TASKS" button is in the top right.

Description: File access control rule [651]
 Details

Enabled:

Take the following action:
 Deny
and:
 Log Take precedence over other Deny rules

when:

Applications in the following class:
 <All Applications> [\[+\]](#)

But not in any of the following selected classes:
 <none>
 <*Installation Applications>
 <*Processes Executing Untrusted Content>
 <*Processes requiring Kernel Only Protection>
 <*Suspected Virus Applications>
New double-click application class to view

Attempt the following operations:
 Read File
 Write File
 Write Directory (create/delete/rename) [\[?\]](#)

On any of these files:
 <none>
Insert File Set double-click variable to view

Buttons at the bottom: Save, Delete, **19 rule changes pending**, Generate rules.

242799

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 2-14.)

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.



Tip

Once you click Find on the search page and have a list of findings, you can view each item in the list in a new browser window. When you move the mouse over each item in the found list, an **open in new window** option appears by the item. If you click that option, the item opens in a new window for you to view. This way, your original list of found items is preserved while you view individual items in a new window. If you do not open the item in a new window, you cannot click back to the found list and you must run the search again.



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

Using Search

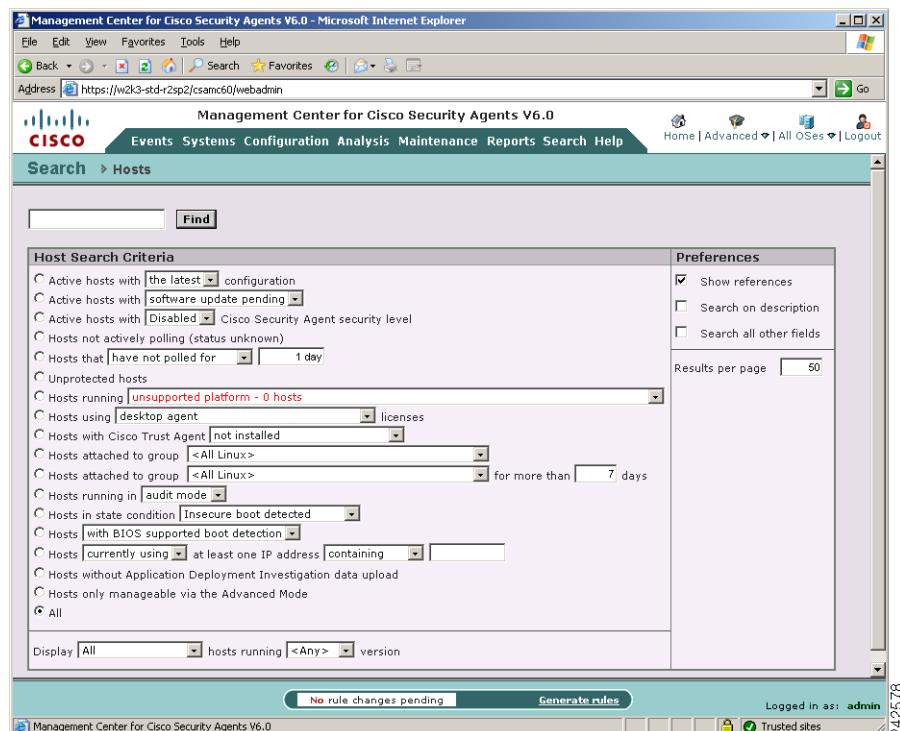
it where it appears with another item that you select. For example, you may want to replace all references to a certain variable across the system.

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” and “hosts that have not polled in for a specified time.” See [Viewing Host Details, page 3-28](#) for more information on Hosts.

Figure 2-14 Search Feature



Using CSA MC Utilities

The CSA MC Utilities give administrators more tools to maintain the CSA system. These utilities allow administrators to perform such tasks as backup the CSA MC configuration, import and export configurations and licenses, and manage administrator accounts.

See [Chapter 12, “Using Management Center for Cisco Security Agents Utilities”](#) for more information.

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.

Object Names

When entering a Name for any component you can configure, such as policies, rule modules, groups, rules, variables, etc. 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.)

Configuration Variable Names

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.

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.

Special Character Syntax

Use these syntax requirements when you want to specify special characters in any editable box.

- 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.

Directory and Filename Syntax Requirements

This section describes the syntax for specifying filenames and directories.

Local System Files Entered Using Full Path

Windows:

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



Note

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

UNIX:

```
/etc/passwd  
/usr/bin/*
```

Wildcard notation for directories and filenames

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

Table 2-1 *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.

Here are several examples of the use of wildcard notations:

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.

Short hand notation for directories and file names

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

Table 2-2 Short hand notations for directories and file names

Token Name	Description
@windows	<p>Use @windows to indicate the directory pointed to by %SystemRoot% environment variable.</p> <p>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.</p>
@system	Use @system to indicate %SystemRoot%\system32
@dynamic	<p>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.</p> <p>This list updates automatically (dynamically) as logged quarantined files are received.</p> <p>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 Global Event Correlation for more information.</p>
@reg	Use the @reg token to specify a registry key on the host that contains a directory path. See Referencing Values Stored on Clients, page 2-58 for more information.

Short hand notations for removable media

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 2-3 Removable Media Token Syntax

Token	Translation
@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 media. @CD or @CD:** means all files on the media.
@external	This indicates all removable drives. You can specify particular directory structures using the following syntax: @external:\<specify wildcards>. Note that @external:\ means only the top level files on the USB drive. @external or @external:** means all files on the drive. Note In a file set, @external can only be used in the Directories matching fields.
@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.
@removable	This indicates all removable media, excluding those drives that are bootable. That includes, floppies, CDs, zip drives, USB 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.

Short hand notation for internationalized Windows versions

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 2-4 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 @desktopdirectory	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.

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.

If you want to prevent an application from opening a file for reading, select **Read file**. If you want to prevent an application from opening a file for writing, select **Write file**.

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.



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.

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.

Using the Correct Syntax



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 6-84](#) for further symbolic link protection information.

Network system paths

Here is the syntax for specifying a network location:

```
\<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:\records\database.db
```



Caution

Do NOT enter a drive letter for network share paths.

Network Address Set Syntax Requirements

IPv4 and IPv6 address can be entered in the network address set text boxes.

IPv4 Syntax

IPv4 network address text boxes require addresses entered in any of the following formats:

Enter single fully qualified addresses.

a.b.c.d

Enter address ranges.

a.b.c.d-y.z

This address range indicates all addresses from a.b.c.d-a.b.y.z

Enter address ranges using “network address class” notation.

10.0.0.0/24

This address range indicates all address from 10.0.0.0 to 10.255.255.255

IPv6 Syntax

The IPv6 network address text boxes require addresses entered in any of the following formats:

Enter single fully qualified addresses.

2001:0DB8:0000:0000:00AB:CDEF:5000:6000

Enter a single fully qualified address with consecutive zeros replaced with colons:

2001:0DB8::AB:CDEF:5000:6000

Enter address ranges with complete addresses:

2001:0DB8:0000:0000:00AB:CDEF:5000:6000-2001:0DB8:0000:0000:00AB:CDEF:6000:7000

Enter address ranges in shorthand:

2001:0DB8:0000:0000:00AB:CDEF:5000:6000-6000:7000

Enter address ranges using “network address class” notation.

2001:0DB8:0000:0000::/64

This address range indicates all address from

2001:0DB8:0000:0000:0000:0000:0000:0000 to

2001:0DB8:0000:0000:FFFF:FFFF:FFFF:FFFF

Short hand notation for network address sets

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

Table 2-5 Short hand notation for network address sets

Token Name	Description
@local	Indicates all local addresses on the agent system.
@dynamic	Indicates 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 7-10 for more information.
@recent	Use this token 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.
@reg	Indicates a local registry key which stores an IP address. See Referencing Values Stored on Clients, page 2-58 for more information.

Table 2-5 Short hand notation for network address sets

Token Name	Description
@remote	Indicate all addresses that are not on the local agent system.
@subnet	Indicates 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.

**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 6-29](#) for more information.

Network Services Syntax

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

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

Using the Correct Syntax

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.

Short hand notation for network service sets

You can use the following "short hand" entries in Network Service Sets and in Network access control rules to indicate all local TCP or UDP ports on the agent system in question. The @ symbol must appear at the start of the short hand name.

Table 2-6 Short hand notation for network service sets

Token Name	Description
@reg	This token indicate a local registry key which stores a TCP or UDP port number. See Referencing Values Stored on Clients, page 2-58 for more information.
@smb-null-session	Use 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.

Data Set Interface Matching Syntax

The Interface ID matching field in a Data Set for the **HTTP protocol** is always URI.

These are the syntax requirements for the Interface ID matching field for **LPC protocol** interfaces:

- The service name, a path-like alphanumeric string of arbitrary length, followed by the optional API (a.k.a. opnum) integer expressed as @($api=N$).
LPC Interface ID matching example:

```
\LPC Control\OLE2@(api=7)
```

- A * can be used to represent any API number associated with the interface.
For example:

```
\LPC Control\OLE2@(api=*)
```

These are the syntax requirements the Interface ID matching field for **MSRPC protocol** interfaces:

- Mandatory 32-digit GUID in curly braces followed by the optional API (a.k.a. opnum) integer with the syntax @($api=N$) .
MSRPC Interface ID matching example:

```
{12341234-1234-1234-1234-123412341234}@(api=4)
```

- A * can be used to represent any API number associated with the interface.
For example:

```
{12341234-1234-1234-1234-123412341234}@(api=*)
```

Data Set Pattern Matching Syntax

For **HTTP protocol**, this pattern is used by HTTP Web servers to match against the request URI (Uniform Resource Identifier) to enforce allow/deny Data access control rules. Note that when entering data patterns, the * character is a generic wildcard specification.

For example, *cmd.exe* .

The **MSRPC and LPC protocol** pattern matching fields are used for the Automatic Signature Generation feature. For a full discussion of that feature, see [Chapter 14, “Automatic Signature Generation”](#). These are the descriptions of the tokens used in the automatic signature generation feature:

Table 2-7 Automatic Signature Generation tokens

Token	Explanation
@signatures	<p>Represents payloads that match dynamically generated signatures.</p> <p>For the MSRPC and LPC protocols, here are examples of syntax that indicate a group of automatically generated signatures represented by either the @signatures or @highrisk_signatures token:</p> <p><code>@(signatures) /<CONF></code></p> <p>(CONF is optional and represents a HIGH, MEDIUM, or LOW confidence level for the signature. For example, to indicate signatures in which you have medium confidence you would enter <code>@(signatures)/MEDIUM</code>. You do not have to use a confidence in combination with a signature. You can specify all signature confidence levels by entering <code>@(signatures)/*.</code>)</p>
@highrisk_signatures	<p>Represents payloads on an interface with a recent history of unsuccessful signature-generation attempts. In other words, it represents traffic on an interface that CSA believes is under a DoS attack.</p> <p><code>@(highrisk_signatures)</code></p> <p>(You cannot specify a confidence level for the <code>@(highrisk_signatures</code> token.)</p>



Note

Specifying <all> in the Pattern matching field indicates all signatures represented by the @signatures and @highrisk_signatures tokens.

**Note**

If you use either the @signature or @highrisk_signature token in the Pattern matching field, you can not use either token in the Pattern matching but not field.

Content Matching in File Sets

Use the Content Matching edit box to assign files to file sets based on the files' content. Files tagged with virus names are indicated by the @virusscan token.

AntiVirus Tag Token Syntax

In the Content matching field, the @virusscan token is equated with a signature-based or behavior-based virus tag. The tag describes the state of a virus scan, the name of a virus found in a file, or the static tag name describing an application's behavior. On one line, enter @virusscan token to classify files by the type of virus they are infected with. The syntax for the entry is

`@virusscan=<Tag>.`

See [AntiVirus Tagging, page 15-7](#) for further description of AntiVirus tags.

Below are examples of valid @virusscan syntax:

`@virusscan=<virus:Worm.CodeRed>` indicates a file tagged as having the CodeRed virus.

`@virusscan=<virus : *CodeRed*>` if the type of virus isn't known, use * before and after the virus name to indicate any virus with "CodeRed" name included.

`@virusscan=<virus : **>` indicates a file or application with any AntiVirus tag.

`@virusscan=<CSA_SCAN_IN_PROGRESS>` indicates a file that is in the middle of being scanned for a virus.

`@virusscan=<CSA_UNSCANNABLE>` indicates a file that cannot be scanned. For example, if a user does not regularly have privileges to open a file, the file is tagged CSA_UNSCANNABLE.

`@virusscan=<behavior_based_tag_name>` For example:

`@virusscan=<Virus:Behavior.Excessive Policy Violations>` indicates any application tagged with the Virus:Behavior.Excessive Policy Violations tag.

`@virusscan=<Virus:Behavior**>` indicates any application with any static behavior-based antivirus tags.

Data Classification (DLP) Tag Token Syntax

The @datascan token in the Content Matching field of file sets to associate files tagged with scanning data tags and static data tags to file sets.

The syntax for these entries is to enter an @datascan token on one line of the edit box and equate it to a tag name:

```
@datascan=<Tag>
```

For example:

```
@datascan=<SSN>  
@datatscan=<HIPAA Controlled>
```

Use the **Insert Content** link next to the field to add these data classification tags to the field. The tags that appear in the Tag list box are found on the Scanning Data Tags list box and the Static Data Tags list boxes. These list boxes may be reached by navigating from the **Configuration** menu, **Global Settings > Scanning Data Tags** or **Global Settings > Static Data Tags**.

Referencing Values Stored on Clients

Using the @reg token, you can configure file sets, network address sets, network services sets, and registry sets to reference data stored in the values of registry keys. This way, the same rule can enforce security based on different values stored locally on the client.

The @reg token can only be used for rules used on Windows-based operating systems. These are the instances in which you can use the @reg token:

- When a registry key's value contains a directory path.
- When a registry key's value contains a TCP or UDP port number for a network service.
- When a registry key's value contains an IP address.
- When a registry key's value contains another registry key.



Note The default= field is optional but it is recommended. If the registry key you provide for the @reg token does not exist, or does not use the proper syntax, the default value you specify will be used by CSA when evaluating rules.

Table 2-8 *Uses of @reg token*

Use of @reg token	Syntax
When specifying a directory in the Directories matching field of a file set or in the file set field of a file access control rule.	<p>Use @ (reg registry\path\stringvalue default=DefaultDirectory) 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. For example:</p> <pre>@(reg HKLM\Software\SoftwareName\InstallDirectory) default=**\Program Files\SoftwareName</pre>
When specifying a TCP or UDP port number in the network services field of a NACL, or in the protocol port fields of a network services set.	<p>This is the syntax for specifying a TCP or UDP port:</p> <pre>protocol/@(reg registry\path\stringvalue default=DefaultValue)</pre> <p>For example:</p> <pre>TCP/@(reg HKLM\Software\mykey\port default=80) UDP/@(reg HKLM\Software\mykey\port default=500)</pre> <p>In these examples, port is a string value contained in the mykey registry key.</p> <p>You can also specify ranges of ports in this way:</p> <pre>TCP/@(reg HKLM\Software\mykey\port1 default=100)-@(reg HKLM\Software\mykey\port2 default=200)</pre>

Note The default value of the first registry key in a range must be lower than the default value of the second registry key in the range, as it is in this example.

Note When expressing a range using registry keys, make sure that the value contained in the first registry key, in this case port1, is lower than the value if the second registry key, in this case port2. Otherwise, the default port values you specify in the range string will be used instead of the value in the registry keys.

■ Using the Correct Syntax

Table 2-8 **Uses of @reg token**

Use of @reg token	Syntax
<p>When specifying an IP address in the host address field of a NACL or in the address fields of a network address set.</p>	<p>This is the syntax for specifying an IP address:</p> <pre data-bbox="460 339 1213 363">@ (reg registry\path\stringvalue default=DefaultIPAddress)</pre> <p>For example:</p> <pre data-bbox="460 421 1132 445">@ (reg HKLM\key\subkey\IPAddress default=10.80.40.2)</pre> <p>In this example, IPAddress is a string value contained in the subkey registry key.</p> <p>The default IP address can be IPv4 or IPv6. However, IPv6 addresses can only be used in a rule, that is part of a module, that targets an operating system that supports IPv6.</p> <p>You can also specify ranges of IP addresses in this way:</p> <pre data-bbox="460 690 1227 739">@ (reg HKLM\key\subkey\IPAddress1 default=10.80.40.0)-@ (reg HKLM\key\subkey\IPAddress2 default=10.80.40.255)</pre> <p>Note The default value of the first registry key in a range must be lower than the default value of the second registry key in the range, as it is in this example.</p> <p>Note When expressing a range using registry keys, make sure that the value contained in the first registry key, in this case IPAddress1, is lower than the value of the second registry key, in this case IPAddress2. Otherwise, the default IPAddress values you specify in the range string will be used instead of the value in the registry keys.</p>

Table 2-8 *Uses of @reg token*

Use of @reg token	Syntax
When specifying a registry key in a registry set.	<p>This is the syntax for specifying a registry key using the @reg “shorthand” or “token.”</p> <p>The following string is entered on one line:</p> <pre data-bbox="460 409 1166 458">@ (reg RegistryHiveName\keyname1\keyname2\stringvalue default=RegistryHiveName\keyname3\keyname4)</pre> <p>Hive names must begin the registry key string and be represented by a wildcard (*) or by one of the following abbreviations.</p> <ul style="list-style-type: none"> • HKLM - refers to the HKEY_LOCAL_MACHINE • HKCR - refers to HKEY_CLASSES_ROOT • HKCC - refers to HKEY_CURRENT_CONFIG • HKU - refers to HKEY_USERS and HKEY_CURRENT_USERS (HKU* refers to all users) <p>Wildcards (*) may be used as they are for directories and filenames when expressing a path to a registry key. It is recommended that there be at least one non-wildcarded component in a registry key other than the hive itself. Otherwise, the specified key might be overly generalized.</p> <p>Examples of valid registry key entries:</p> <pre data-bbox="460 992 753 1106">**\MSSQLSERVER** HKLM\SOFTWARE\Cisco** *\SOFTWARE\Cisco**</pre> <p>Note The asterisk is a valid single character in a registry key. For example, HKEY_CLASSES_ROOT*\OpenWithList is a registry key. If you want to represent the * in that registry key with a wildcard, use the “?” character instead of a * character.</p>

■ Using the Correct Syntax



CHAPTER 3

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 3-4](#)
 - [Resetting Cisco Security Agents, page 3-9](#)
- [Managing Agent Kits, page 3-12](#)
 - [Creating Agent Kits from Existing Groups, page 3-12](#)
 - [Creating Agent Kits and Groups Using a Wizard, page 3-16](#)

- Distributing Agent Kits, page 3-18
- Agent Reboot vs. No Reboot, page 3-24
- Registration Control, page 3-25
- Agent Registration, page 3-26
- Scripted Agent Installs, page 3-26
- Managing Hosts Using CSA MC, page 3-26
 - Viewing General Host Statuses with CSA MC, page 3-27
 - Viewing All Hosts Managed by CSA MC, page 3-27
 - Viewing Host Details, page 3-28
 - Searching for Hosts, page 3-36
 - Deleting Hosts from the CSA MC, page 3-38
 - Changing Host Memberships in Groups, page 3-43
- Host Managing Tasks, page 3-51
- Distributing Software Updates, page 3-54
 - Scheduling Software Updates, page 3-56
 - Software Updates in a Distributed Configuration, page 3-60

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 audit 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** Log on to the CSA MC as a user with deploy or configure privileges and switch to **Advanced Mode**.
 - Step 2** 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 3** 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 [Configuring Role-Based Administration, page 2-14](#) for details. (You cannot combine hosts of differing OS architectures in the same group.)

-
- Step 4** 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

The screenshot shows the Management Center for Cisco Security Agents V6.0 interface. The main title bar reads "Management Center for Cisco Security Agents V6.0 - Microsoft Internet Explorer". The address bar shows the URL "https://wck3-std-2sp2/csacm60/webadmin". The top navigation menu includes File, Edit, View, Favorites, Tools, Help, Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, and Help. The sub-navigation menu under Systems shows "Groups > Servers". On the right side, there is a "TASKS" panel with links: "Modify host membership", "Modify policy associations", "Change visibility", "Explain rules", "View related events", and "View change history". The main content area displays the configuration for a group named "Servers". It includes a "Description" field with the value "Default group for systems that install the Server agent kit", an "OS" field set to "Windows", and a "Version" field set to "6.0 r100". Under "Properties", there are sections for "Polling", "Rule overrides", "Log overrides", and "Simple Mode Settings". In the "Features" section, "Anti-virus" is enabled (Background Scan: On | Force AV Update), "Data Leakage Protection" is disabled, and "Application Deployment Investigation" is disabled. The "Attached Policies" section lists a single policy named "Security Audit System" with version "6.0 r100" and a description "System Auditing for suspicious behavior". The status bar at the bottom indicates "Logged in as: admin" and the date "24/2/06".

- Step 5** Optionally, in the Properties area, click **Polling** to configure the polling attributes for the group.

- 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.

- 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.)

Users see the polling hint message on the Status screen of their agent interface.

Step 6

Optionally, click the **Rule overrides** link to configure the rule override attributes for the group.

- You can select the **Audit mode** checkbox for this group.

**Caution**

In audit 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 Audit Mode, page 5-44](#).

- You can enable **Learn mode** to localize policies on the agent and to prevent the flurry of query pop-ups that can appear to a user when the agent is first installed. Learn mode works in a specific manner, in combination with deployed query user rules. These queries are automatically answered and remembered persistent for the learning mode period. More information is provided in [Using Learn Mode, page 5-48](#).

**Note**

Using the Hosts Managing Tasks page, you can configure “timed” Learn Mode and “timed” Audit Mode. Basically, you can configure a task that causes hosts to move in and out of selected groups at timed intervals. This way, you can have all new hosts move out of a Learn Mode group or an Audit Mode group after a set time. Refer to [Host Managing Tasks, page 3-51](#) for configuration information.

Step 7 Optionally, click **Log overrides** to configure log override attributes.

- Enable **Log 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.
- Enable **Log set actions** to turn on logging for all set rules running on hosts within the group regardless of the individual rule settings for the policy attached to the group.
- Enable **Verbose logging mode** to change the event log timer to log all reoccurring events rather than suppressing duplicates. See [Chapter 10, “Event Logging and Alerts”](#) for more information on the event log.
- Enable **Filter user info from events** checkbox for this group if you do not want username information displayed in events or in the additional information screen available from the event Details link.

Step 8 Optionally, click the **Simple Mode Settings** link to configure this group's availability on the Host Security Page.

By selecting **Expose this group also in Simple Mode (on the Host Security page)** this group will be displayed to both Simple Mode and Advanced Mode users. If this feature is not selected, neither Simple Mode nor Advanced Mode users will be able to see this group on the Host Security Page. Next, select either the desktop or server radio button to indicate the kind of hosts for which this group is recommended.

Through the Host Security page, users can create an agent kit for this group, associate policies with this group, view the host membership in a group, view the agent kits created for the group, and move the group in and out of Audit Mode.

Step 9 Features area:

- **AntiVirus:** The field indicates if the AntiVirus feature has been enabled for the group as well as what kind of AntiVirus protection is being employed. This field is informational only. You can not enable this feature from this field directly.
If the *AntiVirus - Signature Based* policy has been deployed to the group, then you will see that AV protection is **Enabled (signature based)**.
If the *AntiVirus - Behavior Based* policy has been deployed to the group, then you will see that AV protection is **Enabled (behavior based)**.
- **Data Loss Prevention:** If the *Data Loss Prevention* policy has been deployed to the group, you will see that the feature has been **Enabled**. This field is informational only. You can not enable this feature from this field directly.
- **Application Deployment Investigation:** Optionally, for Windows groups, you can click the enable link next to **Application Deployment Investigation** to enable that feature. 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 13, “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 10 **Attached Policies:** To attach policies to the group, click the **change** link next to **Attached Policies** label. In the Modify Policy Associations pop-up, select the “**Unattached**” policy you want to add to the group, and click **Add**. When you are done close the Modify Policy Associations pop-up box.

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



Note

Once you attach policies to specific groups, you can click the expand link next to the Combined Policy Rules label to 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.

Resetting Cisco Security Agents

The CSA MC lets you centrally reset agent settings back to their original states and clears all user-configured settings. You may want to do this in order to clear cached user query responses or to reset system states.

Resetting Cisco Security Agents does not clear configured Firewall Settings or File Protection settings. But if Firewall Settings or File Protection settings are enabled, they are disabled after a reset as this is the default factory setting. The information entered into the edit boxes for these features is not lost.

To remotely reset all hosts in a group to the system default settings, follow this procedure:

-
- Step 1** Log on to the CSA MC as a user with deploy or configure privileges and switch to **Advanced Mode**.
 - Step 2** 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.
 - Step 3** Click the link for the group you want to reset.
 - Step 4** Expand the **Tasks** menu and click the **Reset Cisco Security Agents** link in the menu.
 - Step 5** Go to [Select the items you want to reset, page 3-10](#).

To remotely reset the Cisco Security Agent of a single host, follow this procedure:

-
- Step 1** Log on to the CSA MC as a user with deploy or configure privileges and switch to **Advanced Mode**.
 - Step 2** Move the mouse over **Systems** in the menu bar and select **Hosts** from the drop-down list that appears. The list of existing Groups is displayed.
 - Step 3** Click the link for the host you want to reset.
 - Step 4** Expand the **Tasks** menu and click the **Reset Cisco Security Agents** link in the menu.
 - Step 5** Go to [Select the items you want to reset, page 3-10](#).

To remotely reset the Cisco Security Agent of a single host while in **Simple Mode**, follow this procedure:

-
- Step 1** Log on to the CSA MC as a user with deploy or configure privileges.
 - Step 2** From the **Search** menu, select **Hosts**.
 - Step 3** Enter the search criteria for your host and click **Find**.
 - Step 4** Click the link for the host you want to reset.
 - Step 5** Expand the **Tasks** menu and click the **Reset Cisco Security Agents** link in the menu.
 - Step 6** Go to [Select the items you want to reset, page 3-10](#).

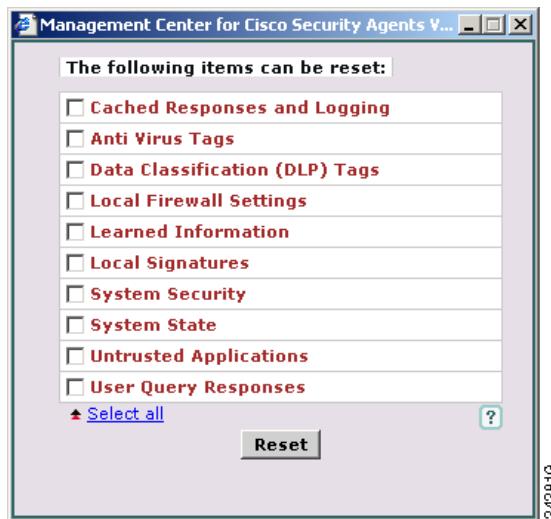
Select the items you want to reset

When you click the **Reset Cisco Security Agents** link, a pop-up window appears displaying various checkboxes that let you reset various specific agents settings or to reset all settings. After you select the items you want to reset, click **Reset**:

- **Cached Responses and Logging** - This clears the temporarily cached query user responses. These are query responses that are stored locally for approximately one hour.
- **AntiVirus Tags** - This clears the AntiVirus tags from files stored on the host. Files that were restricted because of their AntiVirus tags are no longer restricted. See [AntiVirus Tagging, page 15-7](#) for more information about AntiVirus tags.
- **Data Classification (DLP) Tags** - This clears the scanning data tags and static data tags from files stored on the host. Files that were subject to data loss prevention rules will no longer be. See [Scanning Data Tags and Static Data Tags, page 16-4](#) for more information about these data classification tags.
- **Local Firewall Settings** - This clears any local firewall network permissions or file protections that the end user has configured.
- **Learned Information** - This clears the learned, persistent query responses on the agent system. It also clears other learned information such as running applications and unusual system calls. This also causes the automatic 72 learning period to start again. See [Using Learn Mode, page 5-48](#).

- **Local Signatures** - This will delete any LPC or MSRPC attack signatures compiled on the host. See Chapter 14, “Automatic Signature Generation,” for more information about automatically generated signatures.
- **System Security** - This resets the Security level slide bar to its original deployment setting (Medium). This also clears the Network Lock if it is selected.
- **System State** - This resets the agent System State back to its original deployment state. It clears all custom system states as well as those defined in this release. This is useful if the end user system has been quarantined or been placed in a network lockdown state by the agent due to a rootkit detection or by some other means. The reset will be received by the agent regardless of a quarantine or network restriction being imposed.
- **Untrusted Applications** - This clears the Untrusted Applications list that is automatically kept by the agent.
- **User Query Responses** - This clears *all* the persistent query responses on the agent system.

Figure 3-2 Reset Cisco Security Agent Options



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 group associations for deployment. Groups are a collection of policies and an association of 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.

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.

Agent kits can be created in these ways:

- [Creating Agent Kits from Existing Groups, page 3-12](#)
- [Creating Agent Kits and Groups Using a Wizard, page 3-16](#)

Creating Agent Kits from Existing Groups

This procedure is for the Advanced Mode user. It describes creating an agent kit from existing groups. The procedure assumes that Advanced Mode users have created whatever groups they need to create an agent kit using this method.

If you want to create a group for your policies at the same time as you create the agent kit, use the [Creating Agent Kits and Groups Using a Wizard, page 3-16](#) procedure instead.

To create agent kits, do the following.

-
- Step 1** Log on to the CSA MC as a user with deploy or configure privileges and switch to Advanced Mode.
- Step 2** 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 3** Click the **New** button to create a new agent kit.

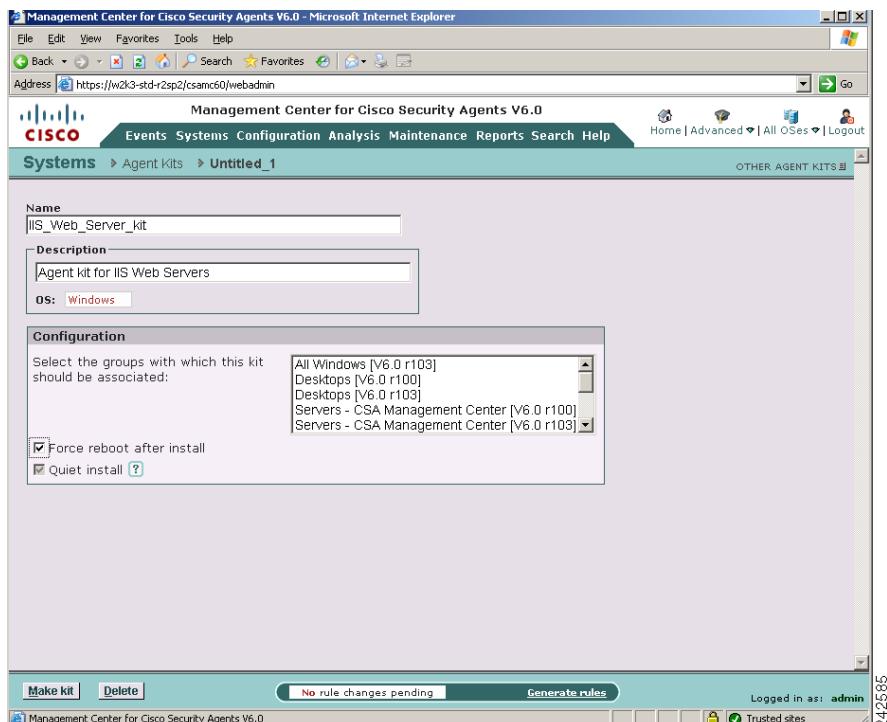
**Note**

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 [Configuring Role-Based Administration, page 2-14](#) for details. (You cannot select a Solaris group for an agent kit that you have configured for Windows systems.)

- Step 4** In the agent kit configuration view (see [Figure 3-3](#)), 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 5** (Optional) Enter a description in the Description field. The description appears in the agent kit list view to help you identify this particular kit.

■ Managing Agent Kits

Figure 3-3 Create Agent Kit



- Step 6** 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 7** 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. Refer to [Agent Reboot vs. No Reboot, page 3-24](#) for information on what security is not enforced if a system is not rebooted after an agent installation.

**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**

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. See [Agent Install Complete Prompt for Automatic Reboot, page 3-23](#) for details.

- Step 8** 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 selecting the installation directory, 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 Quiet install checkbox=enabled	The install ends by displaying a prompt indicating that a reboot will occur within 5 minutes.
Force reboot checkbox=disabled 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 Quiet install checkbox=disabled	The install prompts the user for directory path installation 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 9** Click the **Make Kit** button.

- Step 10** If you are ready to create the kit and generate all pending rule changes, click the **Generate Rules** link to advance to the Generate Rule Program page. The rules that require generation are listed at the bottom of the page.

- Step 11** Click **Generate** to generate all rule changes and make your kit available for deployment. Once the generation rules operation completes, you receive the message, “Rule program generation successful.” Once the agent kit has been created, you can view the contents of the kit and obtain the agent kit’s URL for deployment.

Creating Agent Kits and Groups Using a Wizard

The agent kit wizard allows you to create an agent kit, associate policies with the kit, and create a new group for those policies, all in one process. This is a good method of creating agent kits if you are not using any existing groups.

The agent kit Wizard is available to Advanced Mode and Simple Mode users. Both kinds of users can access the agent kit wizard from the Agent Kits page and Host Security page.

When you finish using the wizard to create an agent kit, the last step generates the kit along with generating all pending rule changes. If you prefer not to generate rule changes immediately after creating an agent kit or you want to create an agent kit using existing groups, use [Creating Agent Kits from Existing Groups, page 3-12](#) procedure instead of this one.

To create an agent kit using the wizard, follow this procedure:

-
- Step 1** Launch the agent kit wizard in one of two ways:
- In **Advanced Mode**, 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. Click **Wizard**.
 - In **Simple Mode** or **Advanced Mode**, move the mouse over **Configuration** in the menu bar and select **Host Security** from the drop-down menu that appears. The Host Security page is displayed. Click **New**.
- Step 2** In the **Identify Target Hosts** step, select the operating system for which the agent kit is intended and select Server or Desktop as the intended platform. Click **Next**.
- Step 3** In the **Host Security** step, select one or more policies you want to distribute through this agent kit. Click **Next** to continue or click **Back** to return to the previous step.
- Step 4** In the Settings step, specify the following attributes:

- Provide a **name** and **short description** of the new group in the Agents installed from this kit will be automatically added to the following group fields.
- Optionally, select the **Audit Mode** checkbox for this group. Audit mode causes agents to log events (if logging is enabled in the rule) for actions that trigger rules but allow those actions to take place. Read more about Audit Mode.
- Optionally, select **Force reboot after agent kit installation**. This installation method requires a quiet installation. The installation ends by displaying a prompt indicating that a reboot will occur within 5 minutes.
- Optionally, 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 selecting the installation directory, 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 Quiet install checkbox=enabled	The install ends by displaying a prompt indicating that a reboot will occur within 5 minutes.
Force reboot checkbox=disabled 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 Quiet install checkbox=disabled	The install prompts the user for directory path installation 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.

Click **Next** to continue or click **Back** to return to the previous step.

- Step 5** Read the Summary description of the new agent kit. If you want to change any aspect of the agent kit before creating it, click the **Back** button to return to the previous step, or click the **edit** link next to any of the previous steps to edit the attributes of that step.

When you’re ready to create the agent kit, and simultaneously generate all pending rule updates, click **Finish**.

- Step 6** Once the agent kit has been created, the description of the agent kit, including its URL is displayed in a pop-up dialog box. From this dialog box you can delete the kit or click **View Kit List** to see a complete list of available agent kits.

Distributing Agent Kits

After agent kits are created, they are assigned a URL, see [Figure 3-4](#). 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.

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

`https://<system name>/csamc60/kits`

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



Note

Note that the Registration Control feature also applies to the <system name>/csamc60/kits URL. If the Registration Control feature (see [Registration Control, page 3-25](#) for details on the feature) prevents your IP address from registering, it also prevents you from viewing this “kits” URL.



Note

You must generate rules after agent kits are created. See [Agent Kit Status, page 3-21](#) for details on when a kit is ready for download.

To view existing agent kits, follow this procedure:

-
- Step 1** In either Simple Mode or Advanced Mode, move the mouse over **Systems** in the menu bar and select **Agent Kits** from the drop-down menu. The list of available agent kits appears.
- Step 2** Click the name of the kit to see its agent kit page.

Step 3 The agent kit page provides a description of the kit and allows you to perform these actions:

- Click **links** in the Group Membership area to view the details of the groups included in this agent kit. Hosts that download this agent kit will become members of these groups.
- Copy the URL of the agent kit to the clipboard using the command button.

**Caution**

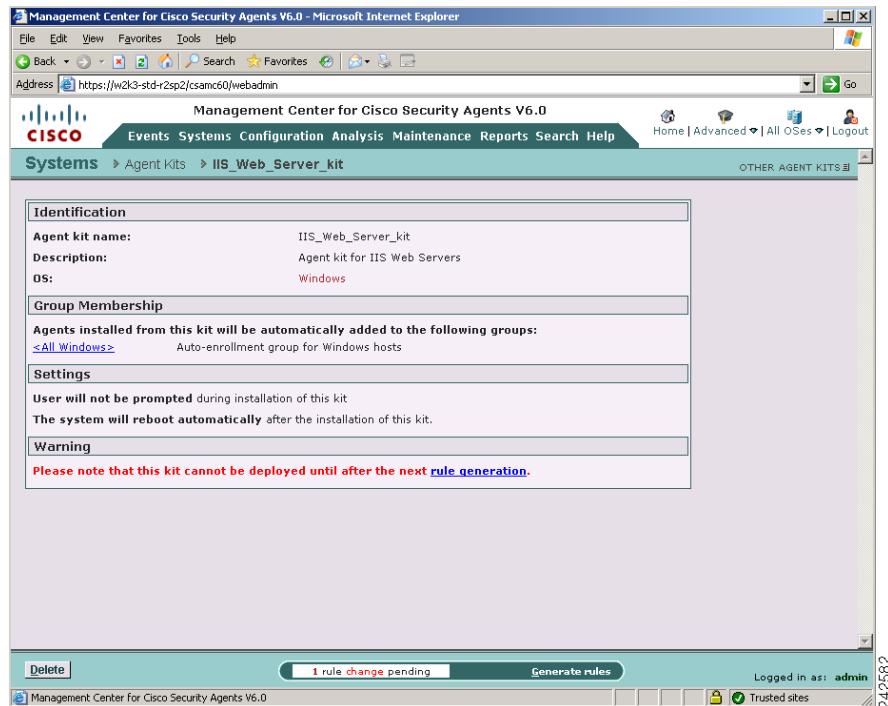
Clicking the URL itself begins the process of installing the agent kit on your local machine.

**Note**

The page for your agent kit also displays the status of the kit. See Agent Kit Status for details on when a kit is ready for download.

■ Managing Agent Kits

Figure 3-4 Agent Kit Download URL



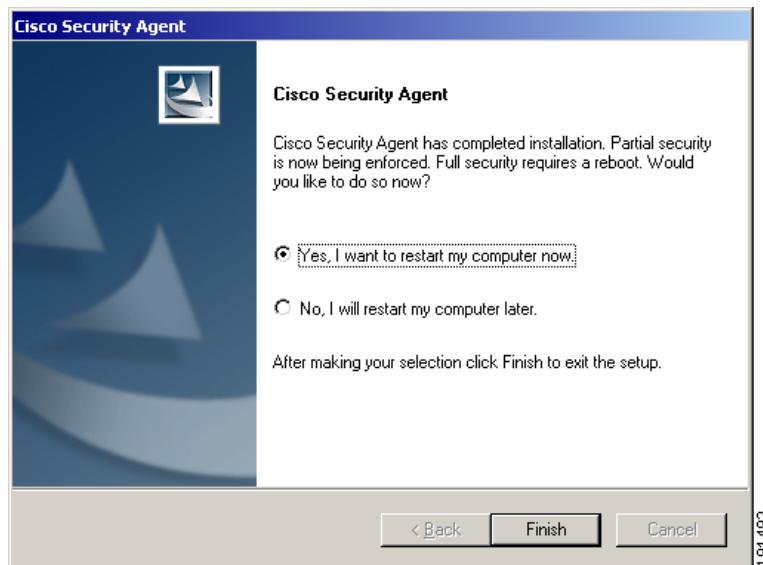
Note If you installed Management Center for Cisco Security Agents to the default directory, all agent kits are placed in the %Program Files%\Cisco\CSAMC\csamc60\bin\webserver\htdocs\deploy_kits directory.

Agent Kit Status

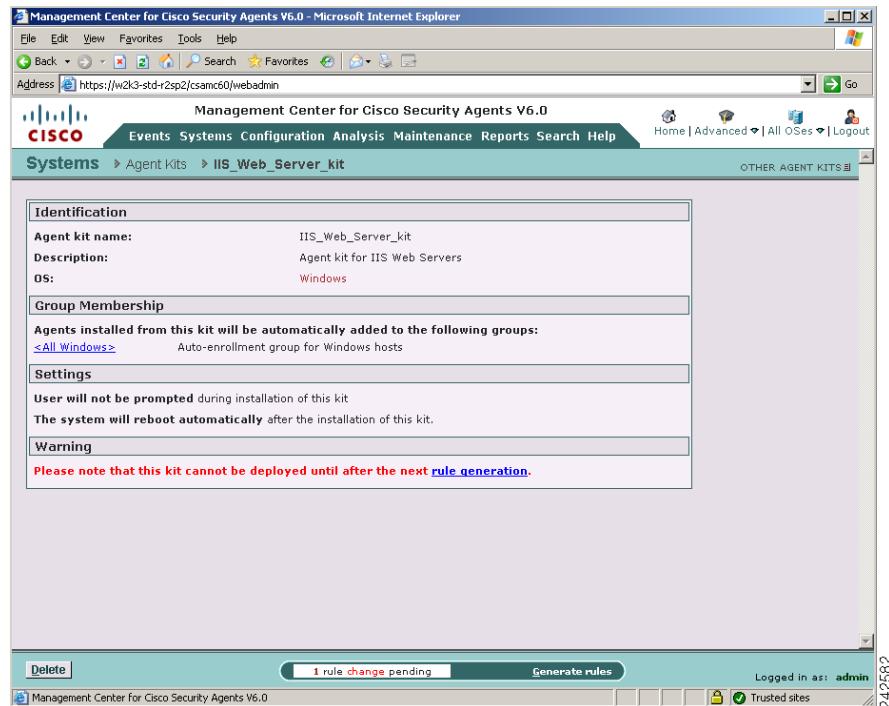
When you create an agent kit, it is given one of three status levels based on how far into the configuration you've progressed. Those status levels are as follows:

- 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 the MC and then you upgrade the MC to a newer version. Agent kits that were created but never generated and have an old version number can never be deployed and should be deleted.

Figure 3-5 Agent Install Complete Prompt for Optional Not-Automatic Reboot



191492

Figure 3-6 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.

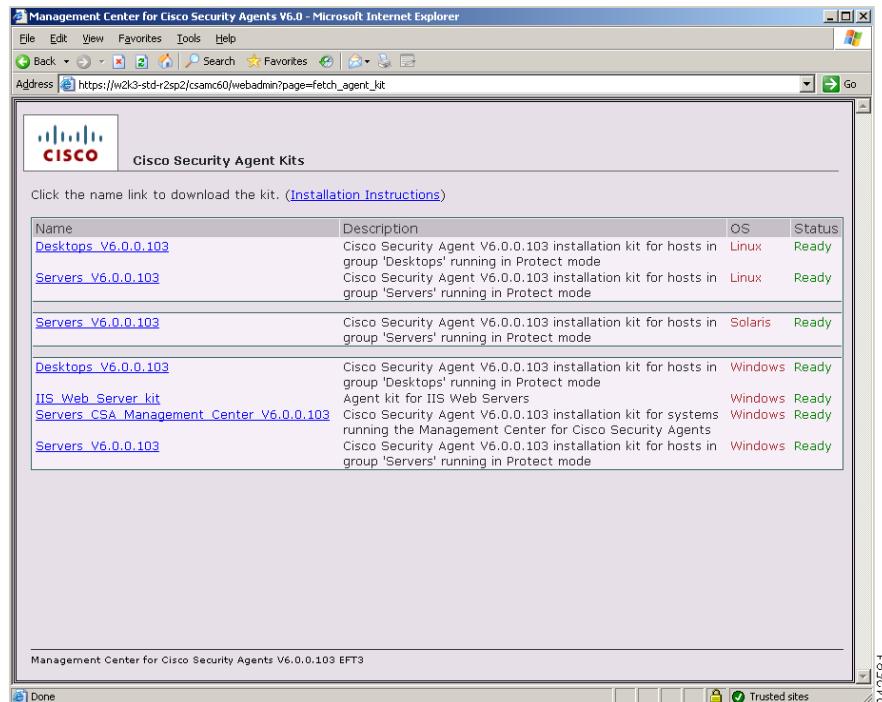
Solaris and Linux agents, when no reboot occurs after install, the following caveats exist:

- 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.



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 3-58](#) for software update reboot details.

Figure 3-7 Download Agent Kits

Registration Control

This feature is accessible from the Systems item in the menu bar. Enter a range of addresses in the registration control page to restrict agent hosts attempting to successfully register with CSA MC. Only those hosts with addresses entered here can register with CSA MC.

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
```

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

You can use scripts to silently install Windows Cisco Security Agents on end user systems. (Scripted agent installs 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%\Cisco\CSAMC\csamc60\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.

Whether or not an end user system is going to have a visible agent UI or a hidden one (see [Agent UI Control, page 6-6](#)), 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, page 3-26](#)).

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** Log on to the CSA MC and switch to Advanced Mode.
 - Step 2** Move your mouse over **Systems** in the menu bar and click **Hosts** in the drop-down menu.
 - Step 3** (Optional) Sort the host list by operating system.
 - Step 4** From the 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 at least once in 24 hours. When you select this viewing option, a “Yes” for Active or a “No” for Not Active appears in the column.
 - **Security level**: This option indicates if the user has set the security level on their local agent to Off, Low, Medium, or High.

- **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.
- **Audit mode:** When you select this viewing option, a “Yes” for running in Audit Mode or a “No” for Not Running in Audit Mode appears in the column.
- **Learn mode:** When you select this viewing option, “On” indicates the host is running in Learn Mode, “Off” indicates the host is not running in Learn Mode.
- **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** Log on to the CSA MC and switch to Advanced Mode.
 - Step 2** Move your mouse over **Systems** in the menu bar and click **Hosts** in the drop-down menu.
 - Step 3** (Optional) Sort the host list by operating system.
 - Step 4** 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:

- [Host 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

The screenshot shows the Management Center for Cisco Security Agents V6.0 interface. The top navigation bar includes tabs for Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, Help, Home, Advanced, Windows, and Log. The main content area is titled 'ang-wxp01.cisco.com'. It displays the following sections:

- Status:** Shows host identification (Name: ang-wxp01.cisco.com), host status (Events issued in past 24 hours: 12, Software version: Agent is running the latest software, Policy version: Up-to-date, Time since last poll: 0h 1m 50s, Time since last AV signature update: 2h 18m 38s [Force AV Update]), and security levels (Medium). It also lists various detection types like Insecure boot detected, Unprotected access detected, and Untrusted rootkit detected.
- Host Settings:** Lists polling interval (0h 10m 0s), audit mode (Off), learn mode (Off), verbose logging mode (Off), log deny actions (Off), filter user info from events (Off), AV protection (On ClamAV 0.93), and data leakage protection (On). It also shows Application Deployment Investigation enabled (No).
- Group Membership and Policy Inheritance:** Shows two groups: <All Windows> (Auto-enrollment group for Windows hosts) and CSOffice60_All_Desktop (CSA Office Desktop group with ALL policies enabled).
- Combined Policy Rules:** Shows 1 rule change pending and a link to generate rules.

A red box highlights the 'Tasks' menu on the right side of the interface.

Host Tasks

Expand the Tasks menu on the host details page to view links that will help you perform these host maintenance 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 3-43](#), for the complete procedure.
- Click the **Reset Cisco Security Agent** link to reset certain values that may have been configured or selected by the end user. See [Resetting Cisco Security Agents, page 3-9](#) for details.
- 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.
- **Last update time**— This is the time that the agent received its last software update.
- **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 status**—This displays whether optional CTA software is Installed, Not installed, Active, or Inactive on the system. This also displays the status of the CTA software version. If this field displays Not active, either CTA is not installed or NAC is not configured to check CSA attributes. If CSA attributes are not being queried by the NAC infrastructure, the status is Not active. (Note that if CTA software is active, this field also displays the current CTA posture status.)

Host Status

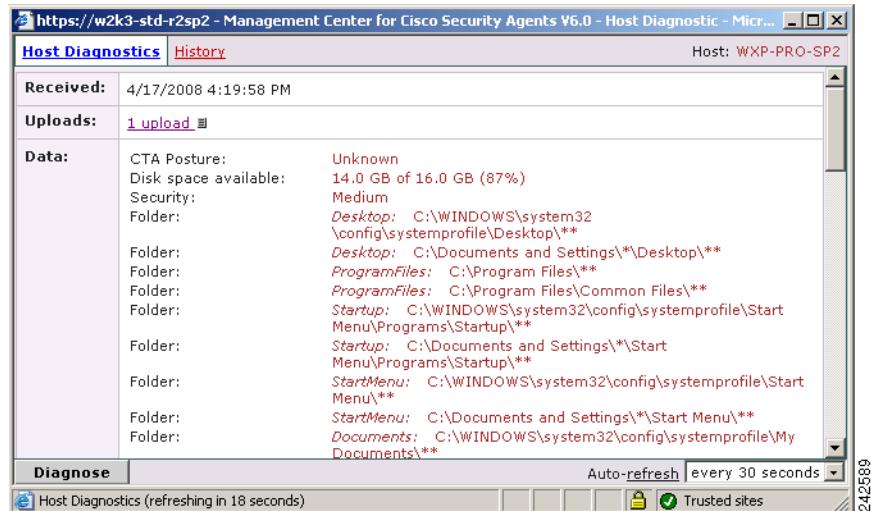
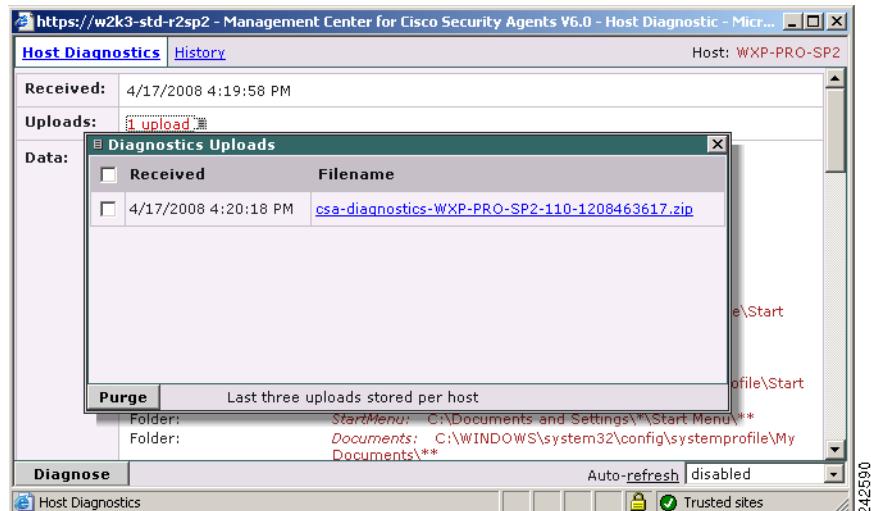
- **Events issued in the past 24 hours**—This is the number of events (rule triggers) that have occurred on the host system in the given time frame.
- **Software Version**—This is the version of Cisco Security Agent software the system is running. If there is a software update available for this host, 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 AV signature update**—This is the interval since the host system's last received a ClamAV signature update.
- **AV full scan schedule**—Displays the schedule for ClamAV scanning. Navigate Systems > Host Tasks > Host Scanning Tasks to see all scanning tasks.

- DL full scan schedule—Displays the schedule for Data Loss Prevention using scanning data tags. Navigate Systems > Host Tasks > Host Scanning Tasks to see all scanning tasks.
- Security level—This indicates the current level displayed by the Security Level bar in the agent UI.
- Untrusted rootkit detected (state condition)—This indicates that the host has been in this named state. The only way to clear this state is to reset the state on the host. See [System State Sets, page 9-40](#).
- Insecure boot detected (state condition)—This indicates that the host has been in this named state. The only way to clear this state is to reset the state on the host. See [System State Sets, page 9-40](#).
- BIOS supported boot detection—This indicates if the host system BIOS is compatible with BIOS dependent boot detection features. See [Kernel Protection, page 6-53](#).
- 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 Host Diagnostics window (see [Figure 3-9](#)) 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 and to view the current states and policies running on the agent system.

Clicking the **Diagnose** button also remotely triggers a program on the agent to gather additional self-describing diagnostic information on the system and on the agent itself. When the collection is complete, a “csa-diagnostics.zip” file is created and automatically uploaded to the MC. This zip file can be accessed from the Host Diagnostics window. The **Uploads** section of this window displays how many diagnostic zip files have been uploaded. The MC can store a maximum of 3 diagnostic files per host. Click on the <#> **Uploads** link on the Host Diagnostics pop-up window to access the individual .zip files (see [Figure 3-10](#)).

**Note**

The MC can store a total of 100 diagnostic files for all hosts.

Figure 3-9 Host Diagnostics Pop-up Window - Data**Figure 3-10 Host Diagnostics Pop-up Window - Uploads Window**

Note Host diagnostics are available locally to the Windows end user from the

Start>Programs>Cisco>Cisco Security Agent>Cisco Security Agent Diagnostics menu on systems where the agent is installed. The end user can manually select “Cisco Security Agent Diagnostics” which causes the agent to gather self-describing diagnostic information on the system and on the agent itself.

Host diagnostics are available locally to the UNIX and Linux end user by executing the ./diag shell script from the /opt/CSCOcsa/bin directory. This creates a csa-diagnostic.gz file in the /tmp directory.

Host **History** information is also available from the Host Diagnostics pop-up window. The feature itself (the collection of host history data) is enabled and disabled from the Status Summary page. Clicking the **History** link at the top of the Host Diagnostics pop-up window takes to a page that provides the following types of information: host registration, audit mode setting changes, learn mode setting changes, IP address changes, CTA posture changes, CSA version changes, host active/inactive status changes.

When you enable Host history collection, a two week history of the previously listed host status changes is maintained for every host registered with the MC.

You may want to use these various types of agent diagnosis information in conjunction with the **Reset Cisco Security Agent** option available from the host **Quick Links** section. This way, you can reset the values that you are viewing in the host diagnosis window through a combination of polling and clicking between windows.



Note

The same Reset Cisco Security Agent functionality is also available on the Groups page (see [Resetting Cisco Security Agents, page 3-9](#) for a description of the available reset options). To centrally reset *all* hosts in a group to the system default settings, use the reset functionality from 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 3-4](#) 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.
- Audit Mode—if this host is part of a group operating in “audit mode,” then the field shows Audit Mode is ON, otherwise, the field shows that Audit Mode is OFF.
- Learn Mode—if this host is part of a group operating in “audit mode,” then the field shows Audit Mode is ON, otherwise, the field shows that Audit Mode is OFF.
- 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 3-4](#) 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 3-4](#) for details on this setting.
- AV protection—Indicates what kind of AntiVirus protection is enabled. If the *Antivirus - Behavior based* policy is distributed to the host AV protection will indicate **behavior based**. If the *AntiVirus - Signature* based policy is distributed to the host, the AV Protection field will indicate **signature** and the version of ClamAV signatures active on the host.
- Data Loss Prevention—if the *Data Loss Prevention* policy is deployed to the host, the Data Loss Prevention field indicates ON, otherwise, the field indicates OFF.
- 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 13, “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 latest” or “an old” configuration.** The search finds hosts that poll into the management server at regular intervals and at least once in 24 hours. The search will find a host with either the “the latest” policy updates or “an old” policy.
 - **Active hosts with “software update pending” or “old software.”** The search finds hosts that poll into the management server at regular intervals and at least once in 24 hours. It will find hosts with Cisco Security Agent software updates pending or hosts with old software.
 - **Active hosts with “Disabled, Low, Medium, High” Cisco Security Agent level.** This finds host with the select level set in the agent UI System Security page slide bar.

- **Hosts not actively polling (status unknown).** This search finds hosts that have missed three polling intervals or have not polled into the CSA MC in 5000 seconds, whichever is greater. A host is also considered inactive if it has not polled in within 24 hours, no matter how many polling intervals it has missed.
- **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 using “desktop, server” licenses.** This search finds either all agents running under desktop system licenses or server system licenses.
- **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 attached to group for <#> of days.** This search finds hosts attached to the one group you pick from the drop down box for the number of days you enter in the available edit field.
- **Hosts running in audit mode.** Agents on hosts running in audit 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.
- **Hosts in state condition “Insecure boot detected, Untrusted rootkit detected”.** This search finds hosts that are in the system state condition selected. All the possible state conditions are not listed here. The state conditions listed here are persistent and can only be cleared using the Reset function. See [System State Sets, page 9-40](#) for details.
- **Hosts with BIOS supported boot detection.** This search finds host systems running with a BIOS that supports the “Insecure boot detected” system state functionality. See [System State Sets, page 9-40](#) for details.
- **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 from the CSA MC

To delete inactive or irrelevant hosts from the CSA MC, first move them to the host recycle bin and then purge them.

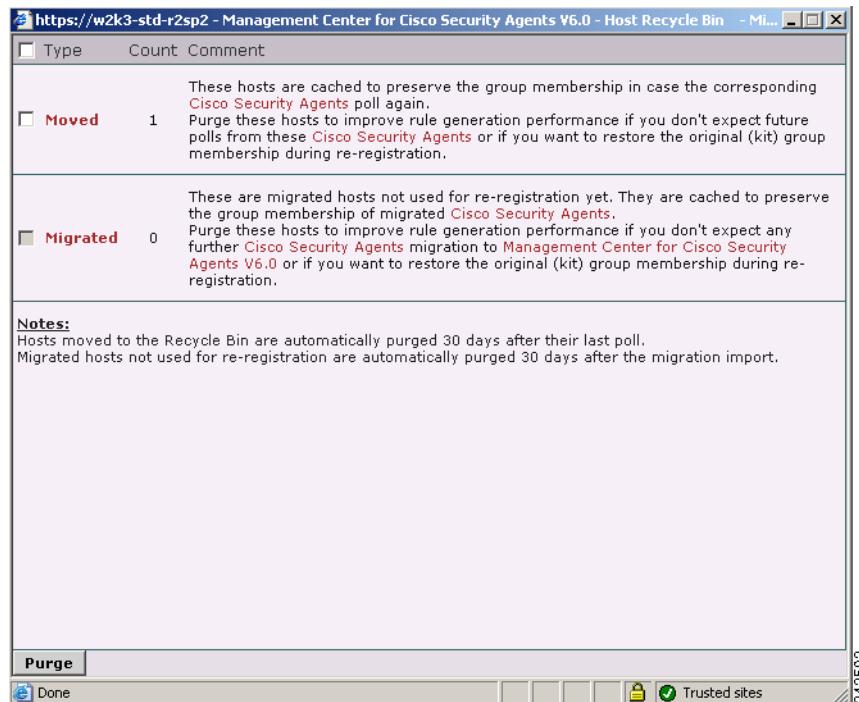
The Host Recycle Bin

The recycle bin window is available from the hosts list page. Hosts are moved to the recycling bin manually by the CSA MC administrator or automatically following a migration of hosts to an upgraded CSA MC. [Moving Hosts to the Recycle Bin From the Host List Page, page 3-40](#) and [Moving Hosts to the Recycle Bin that Meet a Search Criteria, page 3-41](#) describe two methods of manually moving hosts to the recycling bin.

This is how hosts end up in the recycle bin after a migration: If you upgraded your CSA MC to the current version, host and group information from the old MC was migrated to the new MC either automatically or by you when you ran a migration script. Then you scheduled a software update for the hosts so they could receive an upgraded agent. Before the hosts receive the software update, install it, and poll into the new MC, the hosts are included in the “Migrated” count of the recycle bin on the new MC. As hosts start polling in to the new MC, the number of hosts in the Migrated count of the recycle bin decreases. After the hosts polls in and registers with the new MC, the host appears on the hosts list page with an “active” status.

Keeping track of the number of migrated hosts allows you to purge inactive hosts that never migrated to the new CSA MC.

When a host is moved to the recycling bin, the host is cached by the MC but it is no longer visible on the MC. The host’s information is kept on hand by the MC in case the host polls in again. If it does, its group membership is re-established and the host is displayed again, in the active state, on the host list page.

Figure 3-11 Hosts Recycle Bin

Moving Hosts to the Recycle Bin From the Host List Page

Use this procedure to manually move hosts to the recycle bin and then permanently purge them.

-
- Step 1** Log on to the CSA MC as a user with configure privileges and switch to advanced mode.
 - Step 2** Mouseover **Systems** in the menu bar and click **Hosts** in the drop-down menu.
 - Step 3** (Optional) Use the column headers and filters at the top of the host list page to identify the host or hosts you want to move to the recycling bin.
 - Step 4** From the host list page there are two ways to remove hosts.

- Select the checkbox next to the hostname(s) you want to remove and then click **Move to Recycle Bin**. When prompted, make sure you are moving the correct host(s) and click **OK** to move the host(s) to the recycle bin.
- From the host list page, click the link to a host. Review the host details (see [Figure 3-8](#)) to make sure you are removing the correct host and then click **Move to Recycle Bin**. When prompted, make sure you are moving the correct host and click **OK** to move the host.

When a host is moved to the recycling bin, the host is cached by the MC but it is no longer visible on the MC. The host's information is kept on hand by the MC in case the host polls in again. If it does, its group membership is re-established and the host is displayed again, in the active state, on the host list page.

See [Purging Hosts from the CSA MC](#), page 3-42 for information about purging hosts.

Moving Hosts to the Recycle Bin that Meet a Search Criteria

Use this procedure to manually move hosts to the recycle bin.

-
- Step 1** Use the procedure “[Searching for Hosts](#)” section on page 3-36 to find the hosts you want to move and purge.
- 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 and select **Move to Recycle Bin**.
- Step 4** In the Move to Recycle Bin drop-down list box, select either **All hosts matching the current search criteria** or **Selected Hosts**.
- Step 5** Click **Execute**. This function moves the specified hosts to the recycle bin.
- Step 6** When prompted, click **OK** to move the hosts to the recycle bin.

The hosts are now in the recycle bin. If you click **View Recycle Bin**, you will see that the count of **Moved hosts** has increased by the number you moved to the recycling bin.

When a host is moved to the recycling bin, the host is cached by the MC but it is no longer visible on the MC. The host's information is kept on hand by the MC in case the host polls in again. If it does, its group membership is re-established and the host is displayed again, in the active state, on the host list page.

See [Purging Hosts from the CSA MC, page 3-42](#) for information about purging hosts.

Purging Hosts from the CSA MC

Once an agent installs on a host system and registers with CSA MC, that host is not immediately or automatically removed from the CSA MC hosts list if the agent is uninstalled from the system.

Hosts are automatically purged from the system if they have been inactive for either 30 days or 60 days. If a host's group membership is the same as it was when it registered, the host is automatically purged from the CSA MC after 30 days of inactivity. If a host's group membership has changed from the time it registered, the host will be automatically purged from the CSA MC after 60 days of inactivity.

Inactive hosts are running agent software that has missed three polling intervals or has not polled into the CSA MC in 5000 seconds, whichever is greater. A host is also considered inactive if it has not polled in within 24 hours, no matter how many polling intervals it has missed. Active hosts poll into the CSA MC at least once a day.

When a host is moved from the hosts list page to the recycling bin, the host is cached by the MC but it is no longer visible on the MC. The host's information is kept on hand by the MC in case the host polls in again. If it does, its group membership is re-established and the host is displayed again, in the active state, on the host list page.

To completely remove a host from the MC, both visible and non-visible cached host information, you must manually purge this data from the Recycle Bin. Lastly, purging old, cached host information may improve CSA MC rule generation performance.

To purge hosts from the CSA MC, follow this procedure:

-
- Step 1** Move the hosts you want to purge from the recycling bin using [Moving Hosts to the Recycle Bin From the Host List Page, page 3-40](#) or [Moving Hosts to the Recycle Bin that Meet a Search Criteria, page 3-41](#).
 - Step 2** On the hosts list page, click **View Recycling Bin**.

Step 3 Select **Moved** to purge hosts that you manually moved to the recycling bin and select **Migrated** to purge hosts that have failed to migrate to an upgraded CSA MC.

Step 4 Click **Purge**.

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.



Note

See [Viewing Host Details, page 3-28](#) 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 3-12](#)):

- 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 member 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**

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.

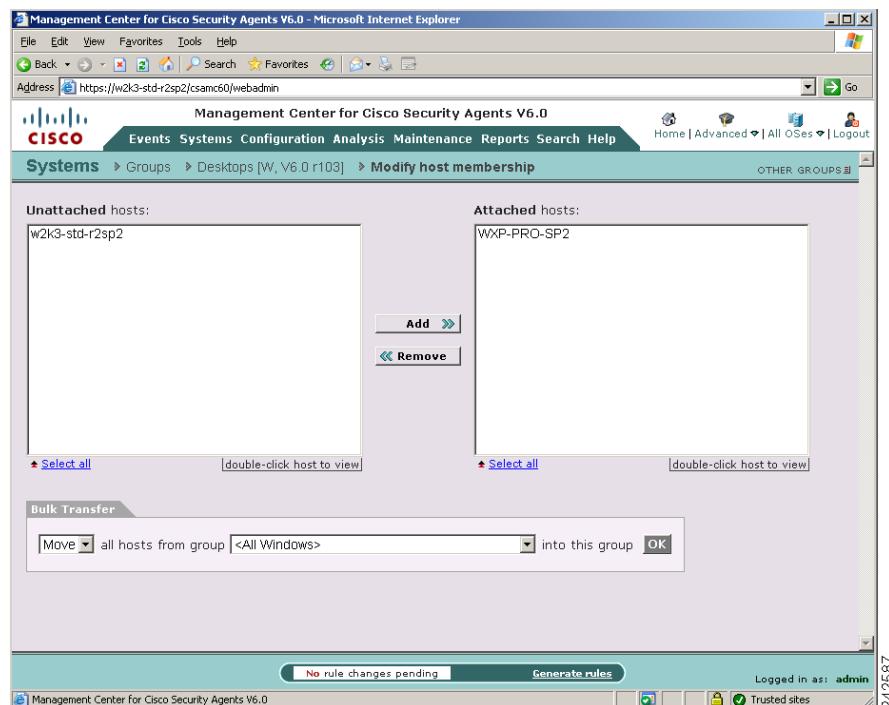
The bulk transfer operations are at the bottom of this page. (See [Figure 3-12](#).)

- 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 you 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.

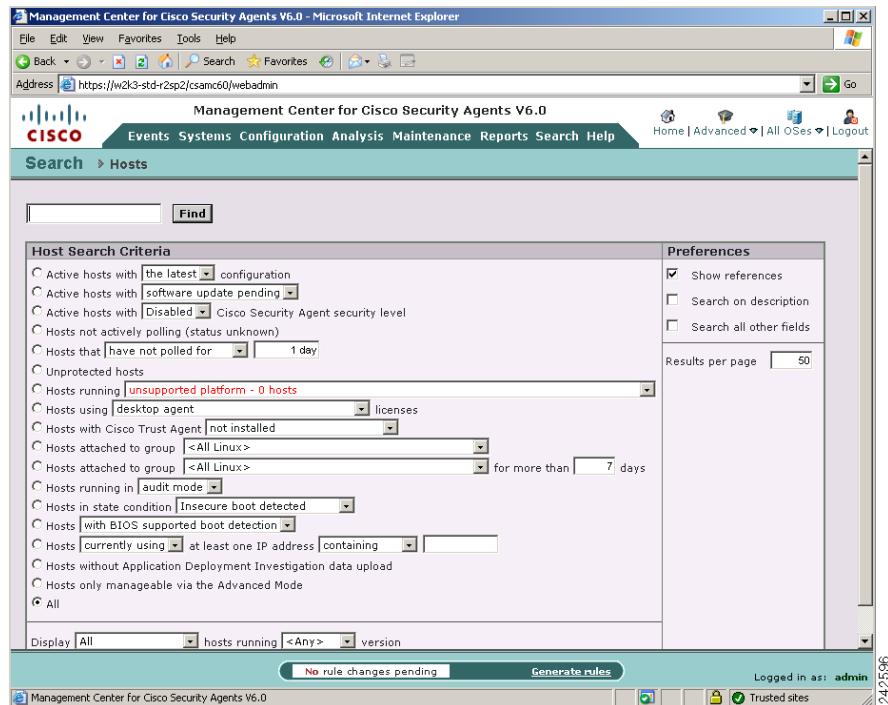
When you next click the **Generate** button, policies associated with this group will no longer be applied to the removed hosts. (The host is not deleted from the database, it is just no longer part of the group.)

Figure 3-12 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](#)” section on page 3-36 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 3-14](#).) The Host Operations Box opens. (See [Figure 3-15](#))
- Step 4** In the Available Operations drop-down list box, select one of the following options:
- **Move to Recycle Bin.** This function allows you to move hosts to the Recycle bin for the purpose of deleting those hosts from the local database. In the Move to Recycle Bin 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 3-13 Hosts Search Page

■ Managing Hosts Using CSA MC

Figure 3-14 Hosts Search Results Page

Management Center for Cisco Security Agents V6.0 - Microsoft Internet Explorer

Management Center for Cisco Security Agents V6.0

Events Systems Configuration Analysis Maintenance Reports Search Help

Search > Hosts

Host Search Criteria [change]
All hosts

1 result

#	Name	Description	Reference list
1	XP-PRO-SP2 [W]	WindowsNT 5.1.2600 Service Pack 2 [W] (English) [x86 fam 6 model 15 step 8] 511MB Tag: VMware-56 4d 31 59 4d cd 1e 78-5d f8 4d 20 8c e9 a7 (Cisco Systems, Inc.)	Groups

Operations No rule changes pending Generate rules Logged in as: admin

Management Center for Cisco Security Agents V6.0

Figure 3-15 Host Operations Box

Host Managing Tasks

The configuration options on the Host Managing Tasks page let you add, move, and remove hosts from selected groups at set times so that the action occurs automatically. Using a configured, automatic, management task could be useful in various recommended scenarios. For example, you’re conducting a pilot of the product and you want all newly registered hosts to remain in a group that has audit mode (see [Using Audit Mode, page 5-44](#)) enabled for certain period of time before those hosts move to a group that is not in audit mode. Having this group movement occur automatically can reduce the administrative burden of having to manually do this. Especially, if it is your policy to have all new hosts start off in audit mode.

This same scenario can be applied to using learn mode (see [Using Learn Mode, page 5-48](#)). Rather than having to remember to move hosts out of a group with learn mode enabled or having to remember to turn learn mode off, you can use a host managing task to do this automatically when scheduled.

Configure a host managing task to automatically add, move, or remove hosts as follows:

-
- Step 1** Move the mouse over **Systems** in the menu bar and select **Host Managing Tasks** from the drop-down list that appears. The list of existing tasks (if any) is displayed.
- Step 2** Click the **New** button to create a new task. The host managing tasks configuration page appears. See [Figure 3-16](#).
- Step 3** In the available fields, enter the following information:
- **Name**—This is a unique name for this task. 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 description appears in the list view to help you identify this particular task.
- Step 4** In the **Configuration** section of the page, select a combination of the following options:
- **Run this task every**

Select one or more days of the week to run this task. You can also specify a certain time to run the task. If you do not specify a time (note that it's a 24 hour clock), the default time is midnight.

- **Add** hosts from group <group name> to group <group name> if they have been part of the source group for more than <number> of days.

Use the **Add** checkbox option to put all hosts in an additional group without removing them from their current group. This addition to the selected group occurs only if the hosts have been part of the original group for longer than the time frame specified. This time frame can be between 1 and 365 days.

- **Move** hosts from group <group name> to group <group name> if they have been part of the source group for more than <number> of days.

Use the **Move** checkbox option to migrate all hosts from the current specified group to another specified group. This moving of hosts from the selected group and the addition of those hosts to another group occurs only if the hosts have been part of the original group for longer than the time frame specified. This time frame can be between 1 and 365 days.

- **Remove** hosts from group <group name> if they have been part of this group for more than <number> of days.

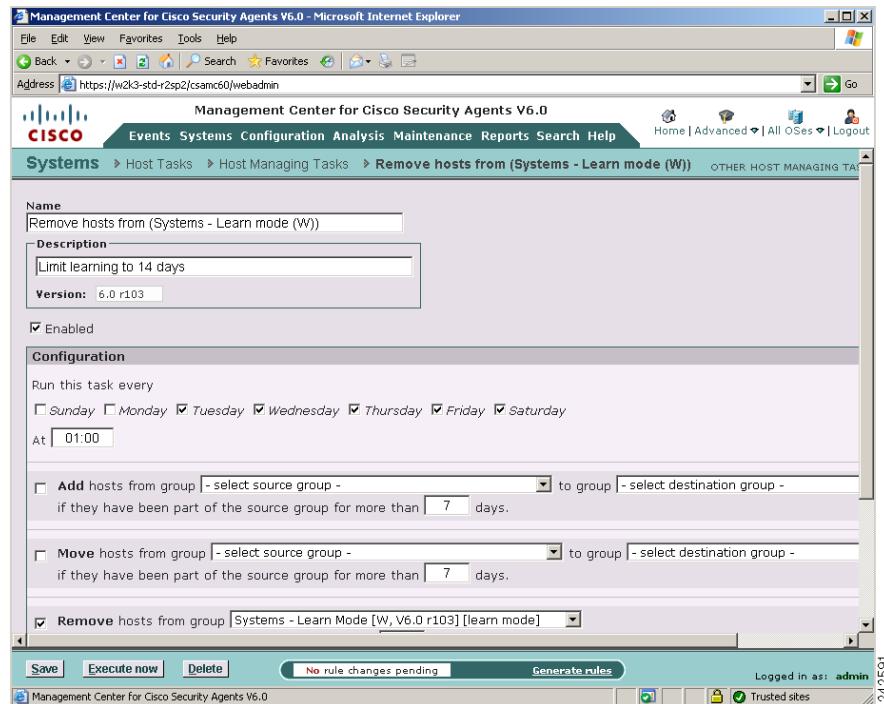
Use the **Remove** checkbox option to take all hosts from the current specified group out of that group. This removal of hosts from the selected group occurs only if the hosts have been part of that group for longer than the time frame specified. This time frame can be between 1 and 365 days.

- **Regenerate** rule programs.

Agents do not receive most CSA MC configuration changes unless rules are generated after the changes are made. Therefore, if you configure a task to occur at a certain day and time and you want agents to pull the group configuration changes down when they occur, you must select this checkbox to generate rules as part of the task. If you do not select this checkbox, configuration changes that require a rule generation are only made on the MC and are not received by agents until a manual rule generation is performed.

Step 5 Click the **Save** button.

Click the **Execute now** button to immediately run the configured task.

Figure 3-16 Host Managing Tasks

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 [Scheduling Software Updates, page 3-56](#) 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 3-17](#)):

- Name of the software update, for example SP 5.2.0.102
- Description of the software update, for example Service Pack for agent on Win2K, Windows XP, Windows 2003
- 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 3-17 Available Software Updates Page

The screenshot shows a Microsoft Internet Explorer window titled "Management Center for Cisco Security Agents V6.0 - Microsoft Internet Explorer". The address bar shows the URL: <https://w2k3-std-r2sp2/csanc60/webadmin>. The page header includes the Cisco logo and navigation links: Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, Help, Home, Advanced, All OSes, and Logout.

The main content area displays a table for "Update V6.0.0.103". The table rows are:

Name	Update V6.0.0.103
Description	Service pack for agent on Windows 2000, Windows XP, Windows 2003, and Windows Vista
Target systems	Cisco Security Agent (versions 6.0.0.1 - 6.0.0.102)
Version	6.0.0.103
Operating system	Windows 2000 , Windows 2003 , Windows Vista , Windows XP
Operating system version(s)	Windows 2000 (5.0.4.2195 , 5.0.3.2195 , 5.0.2.2195 , 5.0.1.2195 , 5.0.0.2195) , Windows 2003 (5.2.2.3790 , 5.2.1.3790 , 5.2.0.3790) , Windows Vista (6.0.0.6000 , 6.0.1.6000 , 6.0.1.6001) , Windows XP (5.0.1.2600 , 5.1.0.2600 , 5.1.1.2600 , 5.1.2.2600 , 5.1.3.2600)

At the bottom of the page, there are buttons for Delete, No rule changes pending, Generate rules, and a status message: Logged in as: admin. The status bar at the bottom of the browser window shows the URL: Management Center for Cisco Security Agents V6.0 and the number 242584.

Scheduling Software Updates

Create a **Scheduled Software Update** to distribute a software update listed on the Available Software Updates page to selected groups.

To schedule a software update follow this procedure:

-
- Step 1** Log on to the CSA MC as a user with configure or deploy privileges. You can perform this task in either Advanced Mode or Simple Mode.
 - Step 2** From the **Systems** menu, navigate **Software Updates > Scheduled Software Updates** (see [Figure 3-18](#)).
 - Step 3** Click the **New** button to create a new entry. This takes you to the update configuration page.
 - Step 4** Enter a **Name** for the update that makes it easily identifiable.
 - Step 5** 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 6** 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 7** From the **Software update** pulldown list, select the Solaris, Linux, or Windows update you want to distribute.
 - Step 8** **Enable update for hosts in selected groups** From the available list of groups, select one or more to distribute this update to.

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.

**Note**

If a software update has been scheduled, and rules have been generated, changing the update time to another time and saving those changes will not require you to generate rules again. The new scheduled update time will take effect without generating rules.

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 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 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 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 If you are using the Cisco Trust Agent (CTA) in your enterprise, you can use this page to configure a CTA software update in combination with a CSA update or on its own. Refer to your CTA documentation for particular software update information.

Step 12 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 3-18 Scheduled Software Updates Page

The screenshot shows the 'Management Center for Cisco Security Agents V6.0 - Microsoft Internet Explorer' window. The URL in the address bar is `https://w2k3-std-72sp2/csanc60/webadmin`. The page title is 'Management Center for Cisco Security Agents V6.0'. The navigation menu includes Events, Systems, Configuration, Analysis, Maintenance, Reports, Search Help, Home, Advanced, All OSes, and Logout. The current path is Systems > Software Updates > Scheduled Software Updates > Update to V6.0.0.103 (Windows). A link to OTHER SCHEDULED SOFTWARE is visible. The main content area displays configuration settings for a scheduled update:

- Name:** Update to V6.0.0.103 (Windows)
- Description:** Windows update scheduled via the Software Update Wizard
- Configuration:**
 - OS:** Windows
 - Software update:** Update V6.0.0.103
 - Enable update for hosts in selected groups:** A dropdown menu shows '<All Windows>' selected, with other options like 'All Windows [V6.0 r103]', 'Desktops [V6.0 r100]', 'Desktops [V6.0 r103]', and 'Servers - CSA Management Center [V6.0 r100]' listed.
 - Update time (hh:mm):** from 00:00 to 23:59
 - Checkboxes:** Force reboot after install (unchecked), Quiet install (unchecked)

At the bottom of the page, there are Save, Delete, and Generate rules buttons. The status bar indicates 'No rule changes pending' and 'Logged in as: admin'. The timestamp '24/2/05' is also present.

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 service on one MC before you install the software update on the other MC. Then restart the services.



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.

- [Preparing a Security Policy, page 4-2](#)
 - [Configuring Rule Modules and Policies, page 4-2](#)
 - [Developing a Security Policy, page 4-3](#)
- [Combining Policies, page 4-6](#)
- [Making a Policy Mandatory, page 4-7](#)
- [Building Policies and Rule Modules, page 4-8](#)
 - [Configure a Policy, page 4-8](#)
- [Attaching Rule Modules to Policies, page 4-11](#)
- [Attaching Policies to Groups, page 4-12](#)

- Overall Policy Methodology, page 4-14
 - Analyzing Applications, page 4-14
- Configuring Policies —The Methodology, page 4-16
 - General Server Policy, page 4-17
 - Sample Web Server Policy, page 4-18
 - Combined General Server and Sample Web Server Policies, page 4-19

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 Audit Mode (from the Group or Rule Module pages). In Audit 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.

Developing a Security Policy

If you are crafting your own policies, please refer to [Overall Policy Methodology, page 4-14](#) 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.

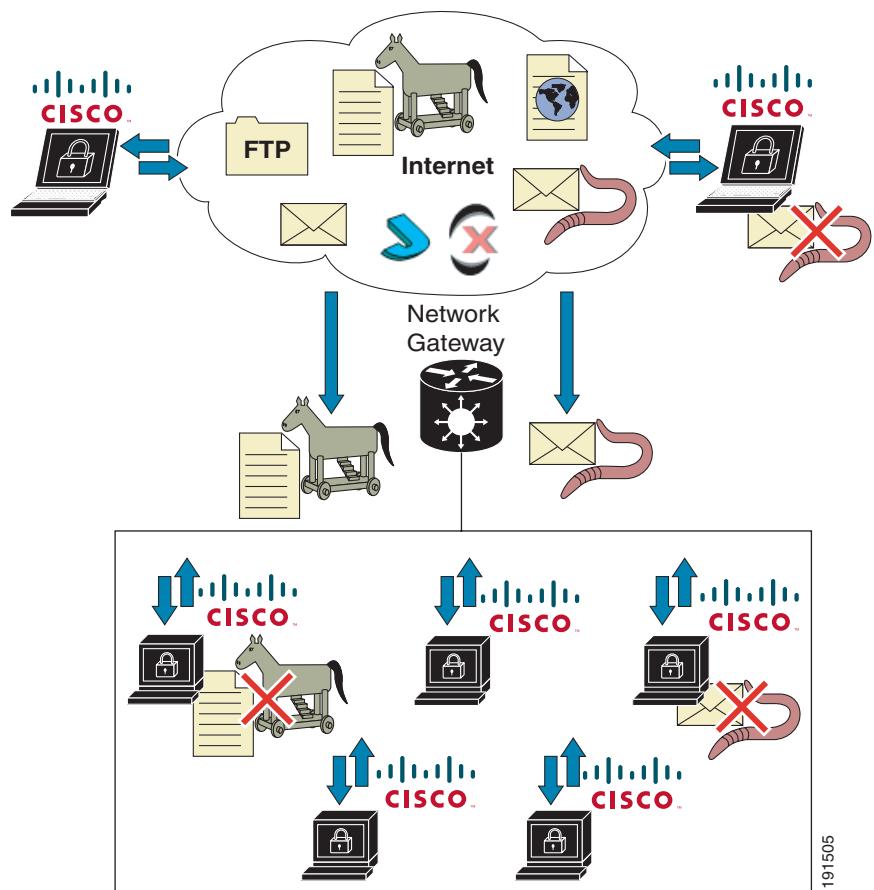
Providing Safe Access to Required Resources

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.

Combining Policies

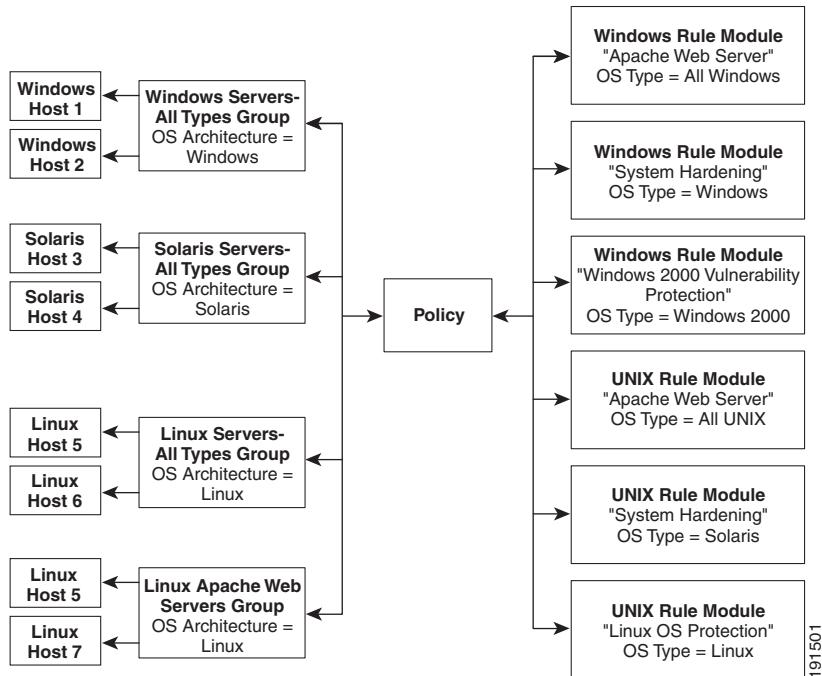
You can attach multiple rule modules to single policies and you can attach multiple policies to a single group. Moreover, a host can belong to multiple groups and inherit policies from all of them. For example, a desktop can belong to the Desktop-All types group and inherit the Systems-Audit Mode policy. 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 5-18](#) 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

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.

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 the group 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** Log on to the CSA MC as a user with configure privileges and switch to Advanced Mode.
- Step 2** 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 3** Click the **New** button to create a new policy entry. This takes you to the policy configuration page.
- Step 4** 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 5** In the Properties area, 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 6** Click the **Simple Mode Settings** link to configure this policy's availability on the Host Security Page.
- By selecting **Expose this policy also in Simple Mode (on the Host Security page)** this policy will be displayed to both Simple Mode and Advanced Mode users. If this feature is not selected, neither Simple Mode nor Advanced Mode users will be able to see this policy on the Host Security Page. Next, select the **desktop** checkbox, the **server** checkbox, or both checkboxes, to indicate the kind of hosts for which this policy is recommended.
- Through the Host Security page, users can add or delete his policy to a group so that it may be included in an agent kit for the group, view the host membership in a group, view the agent kits created for the group, and move the group in and out of Audit Mode.
- Step 7** Click the **Save** button.
- This policy is empty until you attach configured rule modules to it.

Figure 4-3 New Policy

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 5-4](#).

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** Log on to the CSA MC as a user with configure privileges and switch to Advanced Mode.
 - Step 2** 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 3** 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 4** From the edit view, click the **Modify policy associations** link. This takes you to a page containing swap boxes. See [Figure 4-4](#). 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 5** 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.

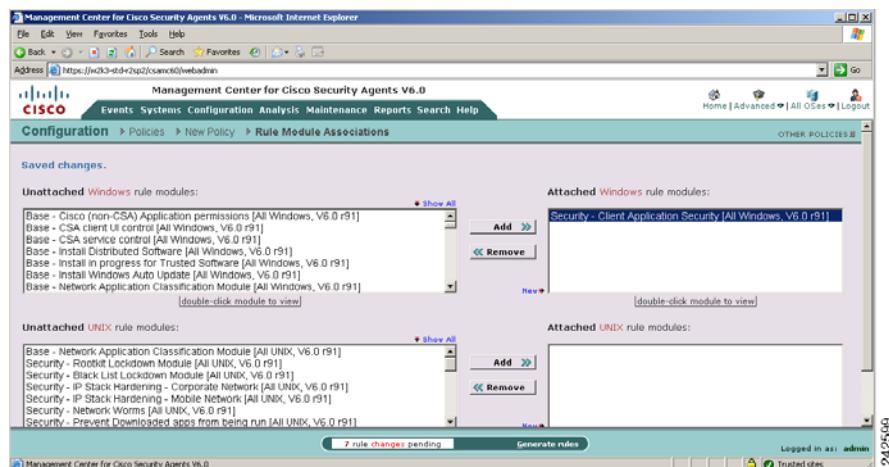
■ Attaching Policies to Groups



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 4-4 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 5-4](#).

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.)

This procedure is for Advanced Mode users. For an alternative procedure for use in Simple mode, see [Host Security Page, page 2-24](#).

To attach a policy or policies to an existing group using the **Modify policy associations** link in the Group configuration page, do the following.

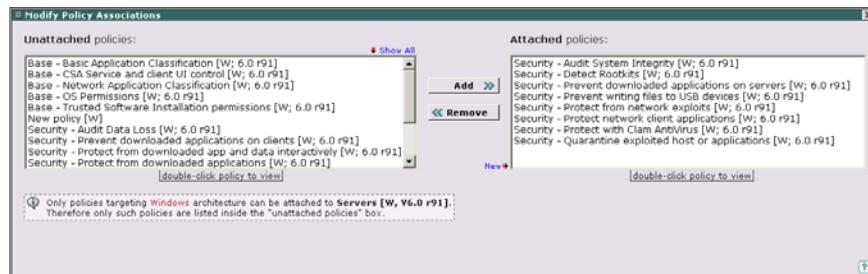
-
- Step 1** Log on to the CSA MC as a user with configure privileges and switch to Advanced Mode.
 - Step 2** Attach a policy to a particular group by accessing that group's edit view. From **Systems** in the menu bar, click on **Groups** to access the group's list view.
 - Step 3** From the group list view, click the link for the group you want to attach a policy to. This brings you to that group's edit view.
 - Step 4** From the edit view, click the **Modify policy associations** link. This takes you to a page containing swap boxes (see Figure 4-5). The left box contains the policies not attached to this group. The right box contains policies that are attached to this group.
 - Step 5** 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 4-5 Attaching Policies



242597

**Note**

You can try out policies on host systems by selecting Audit Mode for a group or for a particular rule module. Selecting Audit Mode and enabling logging on rules attached to “audit mode” groups causes the agent to log designated denied events triggered by policies but not take any actions on those events.

Overall Policy Methodology

The policies created 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.

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 section 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 4-1 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 4-2 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 4-3 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

Rule Type	Description
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 5

Rule Module Configuration

Overview

Rule modules consist of one or more rules. One or more rule modules are meant to be attached to a policy. This module of rules is generally configured for a particular “modular” purpose. It is in this manner that several rules can be moved together from one policy to another or exist as part of several policies.

Rule module are generally OS specific while policies are not. This way, you can scale a great many rule modules to a lesser number of policies to simplify your basic product configuration view. For example, you could have one policy for all Apache servers, but that policy would consist of several OS specific rule modules containing hundreds of rules. As an administrator, you may only be interested in your Apache policy which you can attach to a general servers groups and deploy in this manner.

This section contains the following topics.

- [About Rule Modules and Rules, page 5-3](#)
- [Rule Module Components, page 5-4](#)
 - [Configuring Rule Modules, page 5-4](#)
 - [Adding Rules to a Rule Module, page 5-6](#)
 - [Filtering the Rules Display, page 5-9](#)
 - [Copying Rules between Modules, page 5-9](#)
 - [Comparing Configurations, page 5-10](#)
 - [Merging or Copying Rule Modules, page 5-12](#)

- View Change History, page 5-12
- Explanation of Rules, page 5-13
- Consistency Check, page 5-14
- Attaching Rule Modules to Policies, page 5-14
- Generating Rule Programs, page 5-16
- Common Rule Page Configuration Items, page 5-17
 - Rules: Action Definitions, page 5-19
 - Rules: Manipulating Precedence, page 5-22
 - The Monitor Action, page 5-24
 - The Notify User Action, page 5-24
 - Using the Set Action, page 5-25
- Querying the User, page 5-39
 - Caching Responses, page 5-43
- Rule Overrides, page 5-44
 - Using Audit Mode, page 5-44
 - Using Learn Mode, page 5-48

About Rule Modules and 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 7, “Using Global Settings”](#) 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,

Rule Module Components

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

Configuring Rule Modules

Rule modules are the building blocks for your policies. Modules are made of several different types of rules. See [Chapter 6, “Available Rule Types”](#) for information on rule types.



Note

Carefully read [Rules: Action Options and Precedence, page 5-18](#) so that you will understand how rule precedence works once policies are deployed. You should also refer to the chapter on configuration Variables ([Chapter 9, “Configuring Variables and State Conditions”](#)) 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** Log on to the CSA MC as a user with configure privileges and switch to Advanced Mode.
 - Step 2** Move the mouse over **Configuration>Rule Modules** in the menu bar. The list of existing rule modules is displayed in the rule module list page. CSA MC ships with several pre-configured modules.
 - Step 3** Click the **New** button to create a new rule module
 - Step 4** If you have not set an operating system admin preference, select whether this is a Windows or a UNIX rule module from the pop-up box that appears.

**Note**

UNIX generically refers to both Solaris and Linux operating systems.

-
- Step 5** 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 6** 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 7** In the **OS** field, optionally, you can select to target this module for a specific operating system within your Windows or UNIX classification.
 - Step 8** Optionally, available under **Rule overrides**, you can put this rule module into **Audit mode**. This way, you can have the rules within the audit mode module operating in audit 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 audit mode on the group level. See [Using Audit Mode, page 5-44](#) for details.

- Step 9** Optionally, available under **Rule overrides**, you can put this rule module into **Learn mode**. This way, you can localize policy rules on the agent and prevent the flurry of query pop-ups that can appear to a user when the agent is first installed. Learn mode works in a specific manner, in combination with deployed query user rules. See [Using Learn Mode, page 5-48](#) for details.
- Step 10** Optionally, you can impose configured **State Conditions** on rule modules. Click the **change** link next to **System state** or **User state** to specify a state condition for the rule. See [Setting State Conditions, page 9-40](#).
- Step 11** Click the **Save** button.
- Step 12** Now you add rules to your module. Click the **Add** button in the Rules area and select the kind of rule you want to add to the module.
- Refer to the descriptions of rule types in [Chapter 6, “Available Rule Types”](#) for details on creating the rule you selected.

Figure 5-1 New Rule Module

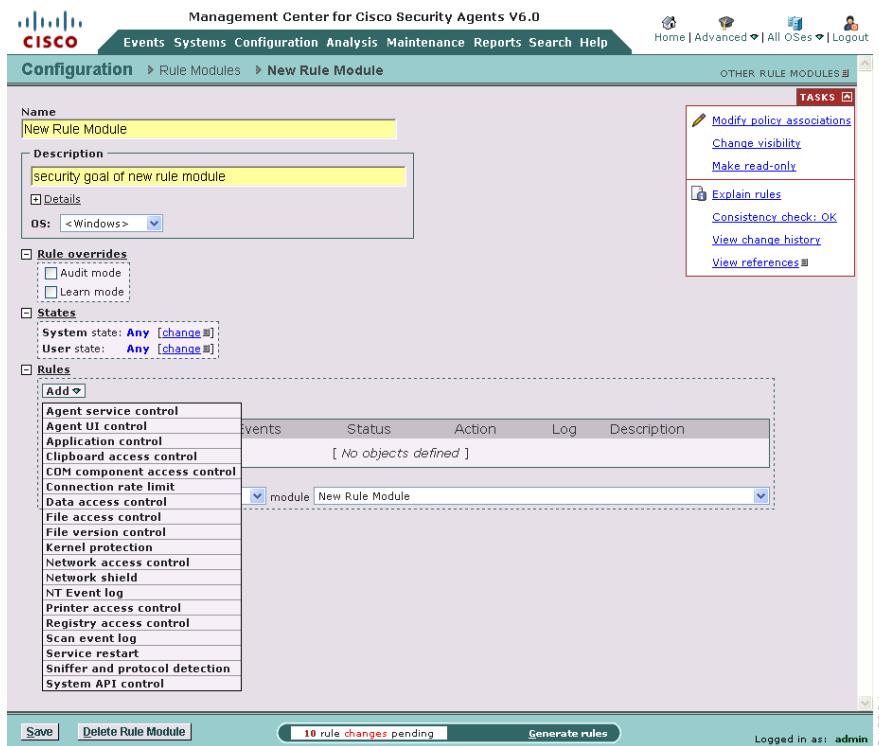


- Note** After the agent is initially installed, there is a non-configurable, automatic, normalization learning period of 72 hours of running time. This learning is for both running applications and unusual system calls. You can use the Reset Cisco Security Agent, Learned Information checkbox to clear all the initial learning and to start the automatic 72 hour learning period again.

Adding Rules to a Rule Module

-
- Step 1** Log on to the CSA MC as a user with configure priveleges and switch to Advanced Mode.
- Step 2** In the menu bar, mouse-over **Configuration** and select **Rule Modules** from the menu. The list of existing rule modules is displayed in the rule module list page. CSA MC ships with several pre-configured modules.
- Step 3** Click the link for the Rule Module to which you want to add rules.

- Step 4** Expand the Rules area of the rules module and click the **Add**. A list of rule types is displayed in a drop down menu.
- Step 5** Select the kind of rule you want to add to the rule module. A configuration page for the rule type you specified opens.
- Step 6** Configure the rule according to the procedures in Chapter 6, “Available Rule Types” and click **Save**.

Figure 5-2 Rule Module, Modify 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 5-3](#).

Rule Module Components

The **ID** column in the Rules section shows 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 5-3](#)) 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 5-3 Rules List in Rule Module

The screenshot shows the Management Center for Cisco Security Agents V6.0 interface. The top navigation bar includes Home, Advanced, All OSes, and Logout. The main menu has options like Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, and Help. Below the menu, the path Configuration > Rule Modules > Base - CSA service control is displayed. On the right, there's a 'TASKS' panel with links like Modify policy associations, Change visibility, Make writable, Explain rules, Consistency check: OK, View change history, and View references. The main content area shows a form for a rule module with fields for Name (Base - CSA service control), Description (Module to protect Cisco Security Agent), OS (<Windows>), and Version (6.0 r152). Under 'Rule overrides', there are Audit mode and Learn mode checkboxes. The 'States' section is collapsed. The 'Rules' section is expanded, showing a table with four entries:

ID	Type	Events	Status	Action	Log	Description
168	Agent service control		Enabled	Black list applications, modify agent configuration		Black list applications, modify agent configuration
169	Agent service control		Enabled	Untrusted Applications (not White List, Backup, Inventory, System, Virus scanner), modify agent configuration		Untrusted Applications (not White List, Backup, Inventory, System, Virus scanner), modify agent configuration
170	Agent service control		Enabled	All Applications, disable the agent security		All Applications, disable the agent security
167	Agent service control		Enabled	Timer to restore Security to 4 hours, All Applications, disable the agent security		Timer to restore Security to 4 hours, All Applications, disable the agent security

At the bottom, there are buttons for Delete, Enable, Disable, Copy, Save, Delete Rule Module, 11 rule changes pending, Generate rules, and Logged in as: admin. A status bar at the bottom right shows 242806.

Filtering the Rules Display

The Groups configuration page, Policy configuration page, and the Rule Module configuration page each display a table listing either the rules attached to the group or the rules included in the module. 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** Log on to the CSA MC as a user with configure privileges and switch to Advanced Mode.
 - Step 2** Move the mouse over **Configuration>Rule Modules** in the menu bar. The list of existing rule modules is displayed in the rule module list page. CSA MC ships with several pre-configured modules.

- Step 3** Click the link for the Rule Module from which you want to copy the rule.
- Step 4** In the Rule Module page (see [Figure 5-3](#)), select the checkbox for the rule or rules you want to copy to another module.
- Step 5** 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 6** Click the **Copy** button.
All checked rules are copied to the selected module.
To clone rules within a module, repeat steps 1-4 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.

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 5-4](#)). 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 module and no corresponding similar rule in the second module, 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 5-4 Compare Rule Modules

The screenshot shows a Microsoft Internet Explorer window displaying the Management Center for Cisco Security Agents V6.0. The URL in the address bar is <https://w2k3-std-r2sp2/csmc60/webadmin>. The page title is "Management Center for Cisco Security Agents V6.0". The navigation menu includes Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, Help, Home, Advanced, All OSes, and Logout. The main content area shows a comparison between two rule modules:

Name	Security - Web and Email run downloaded apps (Medium Security)	Security - Web and Email run downloaded apps (High Security)
Version	6.0 r103	6.0 r103
Description	Module to control web and email applications when security level is Medium	Module to control web and email applications when security level is High
Detailed description	This rule module applies a Medium level of security to web browsers and email clients. Don't allow possibly exploited web browsers and email clients to start suspicious executables. User may be queried if necessary. This is the default security level.	This rule module applies a High level of security to web browsers and email clients. Those processes will not be able to start any suspicious processes.
OS	<All OS types>	<All OS types>
Read-only	Yes	Yes
Exception	No	No
Display only in Show All mode	No	No
Audit mode	No	No
Learn mode	No	No
Included system state sets	\$Security Level Medium [V6.0 r103]	\$Security Level High [V6.0 r103]
Excluded system state sets		
User state sets		
Rules	6 items	7 items

At the bottom of the comparison table, there is a note: "» Use the checkboxes to merge or copy rules to a new rule module or to existing rule modules. » All rules displayed (show only similar rules with detailed differences)". Below the table, there are buttons for Copy, Delete, 4 rule changes pending, Generate rules, and a status bar indicating Logged in as: admin and Trusted sites. The status bar also shows the date 24/26/00.

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 5-5 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 5-6](#).

Figure 5-6 Rule Module Explanation Page

The screenshot shows a Microsoft Internet Explorer window titled "Management Center for Cisco Security Agents V6.0 - Microsoft Internet Explorer". The address bar shows the URL: https://w2k3-std-2sp2/csmc6fl/webadmin. The main content area is titled "Explanation of rule module Security - Web and Email run downloaded apps (Medium Security) [V6.0 r103]".

Detect Rules:

- The detect rules are always evaluated after the enforce rules.
- The following rules are applied only if the following conditions are met:
 - the system state matches system state set [Security Level Medium \[V6.0 r103\]](#).

Control execution of applications:

- Irrespective of any other rules,** Attempts to invoke processes in any of application classes [Applications to configure system settings \[V6.0 r103\]](#), [Command Shell \[V6.0 r103\]](#), [NT Virtual DOS Machine \[V6.0 r103\]](#), [Applications to configure network settings \[V6.0 r103\]](#) by processes in any of application classes [Web browser applications \[V6.0 r103\]](#), [Email applications - All clients \[V6.0 r103\]](#), [Applications using email protocols \[V6.0 r103\]](#), [Instant Messenger applications \[V6.0 r103\]](#), [Applications using web protocols \[V6.0 r103\]](#), but not in application class [Desktop shell applications \[V6.0 r103\]](#), will notify the user if the attempt causes the process to be terminated or is denied. No events will be logged when the rule is triggered.
247
- In the absence of any applicable 'priority deny', 'priority terminate process' or 'allow' rules,** Attempts to invoke processes in all of application classes [Administrator defined - Applications considered Untrusted \[V6.0 r103\]](#), [<First Time Application Execute>](#) but not in any of application classes [Applications to configure system settings \[V6.0 r103\]](#), [Command Shell \[V6.0 r103\]](#), [NT Virtual DOS Machine \[V6.0 r103\]](#), [Applications to configure network settings \[V6.0 r103\]](#), by processes in application class [Desktop shell applications \[V6.0 r103\]](#) will be denied, unless overridden by the user. An event will be logged when the rule is triggered.
248

At the bottom of the page, there are buttons for Print, 4 rule changes pending, Generate rules, and a status bar indicating Logged in as: admin, Trusted sites, and the date 24/2/05.

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.

Attaching Rule Modules to Policies



Note This is the same procedure provided in [Chapter 4, “Building Policies”](#). It is included here as well for your convenience.

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 5-4](#).

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** Log on to the CSA MC as a user with configure privileges and switch to Advanced Mode.
 - Step 2** Move the mouse over **Configuration>Rule Modules** in the menu bar. The list of existing rule modules is displayed in the rule module list page. CSA MC ships with several pre-configured modules.

- Step 3** 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 4** From the edit view, expand the Tasks menu and click the **Modify policy associations** link. This takes you to a page containing swap boxes. See [Figure 5-7](#). 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 5** 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**

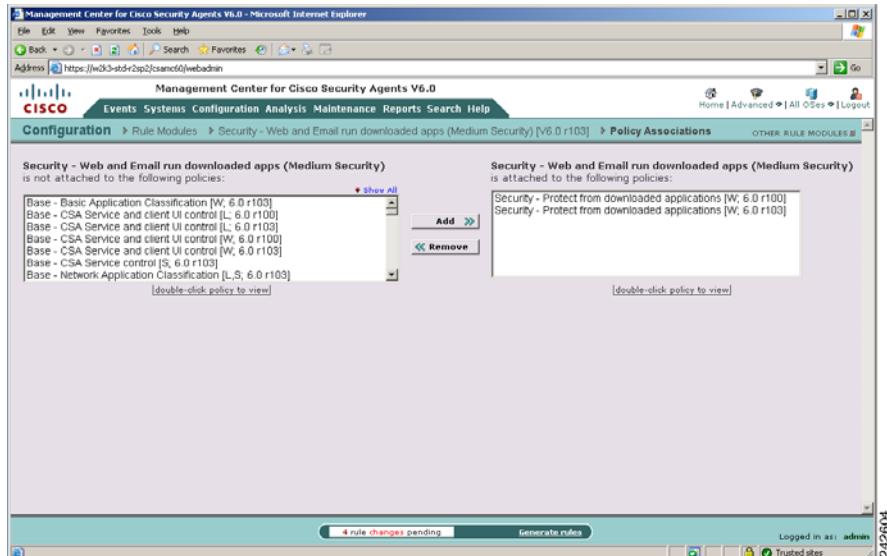
You can attach rule modules of differing architectures to the same policy. This way, you can configure task-specific, self-contained, inclusive policies across all supported architectures for software that is supported on all platforms. For example, Apache is a web server software product that supports 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.

■ Generating Rule Programs

Figure 5-7 Rule Module Associations



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.)

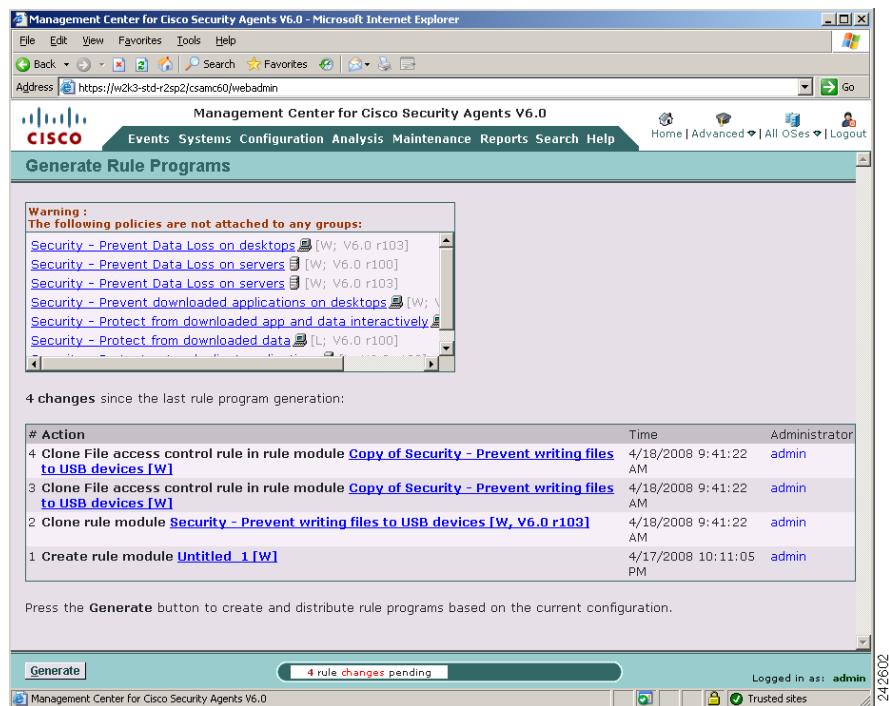
The Generate rule programs view displays the status of all non-distributed database items with the name of the administrator who made the configuration changes. A **Details** link appears beside each edited configuration item. Click this link to view what modifications were made to the configuration in question.

Once you've checked these modifications, you can either go back and change or delete configurations or you can click the **Generate** button (in the bottom frame) to distribute all updates.

**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 made them by accessing the **Audit Trail** view from the Reports drop-down list. See [Using Audit Trail, page 2-32](#) for information.

Figure 5-8 Generate Configuration



Common Rule Page Configuration Items

The following sections provide information on the common fields found on most rule type pages. These include the action options that determine rule precedence as well as a description of how query rules work. The unique rule types themselves are described in the next chapter.

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	Priority Terminate Process
Priority 2	Priority Deny
Priority 3	Priority 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/Not applicable	Monitor
Priority/Not applicable	Notify User
Priority/Not applicable	Set
Priority/Not applicable	Add process to application class
Priority/Not applicable	Remove process from application class

The priority listings beside each item indicate the manner in which CSA processes rules. All priority 1 enforcement rules (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 Monitor rules, are always checked, even in the presence of a 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

- **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.
- **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.
- **Priority 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 are always checked, even in the presence of a priority enforcement rule which governs the same resources triggering first.



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. Additionally, you can configure

monitor rules to trigger only when an enforcement action of a certain type occurs. This way, you are only monitoring “deny actions on a file resource”, for example. See [The Monitor Action, page 5-24](#) for more information,

- **Set**—Use the “Set” action in a rule to cause a particular configuration action to occur when the criteria configured in the rule occurs on a system. See [Using the Set Action, page 5-25](#).

- **Notify User**—You can select to notify the user when an action triggers the rule in question. The user can then acknowledge the notification and enter a justification for the action in question. The Notification Settings configuration window lets you choose an OK button or a combination of Yes and No radio buttons to add to the notification pop-up window.

See [Log, page 5-44](#) and [Notification Settings, page 9-27](#) for more information.

- **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 if the action specifying access to the resource matches any of the parameters in this rule (i.e., allow, deny, terminate). See [Building Classes as Rule Consequences, page 8-12](#) 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 if the action specifying access to the resource matches any of the parameters in this rule (i.e., allow, deny, terminate). See [Building Classes as Rule Consequences, page 8-12](#) for details.

**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.

For every rule 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 [The Monitor Action, page 5-24](#)). 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.

**Note**

Audit Mode and Learn Mode do not affect rule precedence. For example, if you have two rules that are exactly the same, except one is in Audit Mode and one is not, the manner in which CSA MC orders those rules in the list dictates which rule will fire first. That order can be as simple as - the rule that was created by the administrator first fires first.

The Monitor Action

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.

Additionally, you can configure monitor rules to trigger only when an enforcement action of a certain type occurs. This way, you are only monitoring “deny actions on a file resource”, for example.

The Notify User Action

When you configure various rule types, you can select to notify the user when an action triggers the rule in question. The user can then acknowledge the notification and enter a justification for the action in question. The Notification Settings configuration window (see [Notification Settings, page 9-27](#)) lets you choose an OK button or a combination of Yes and No radio buttons to add to the notification pop-up window.

When you select Notify User as the action type for a rule, a Notification Settings pulldown menu appears. You must select one of the preconfigured Notification Setting as part of the rule. You configure a Notification Setting from the **Notification Settings** configuration page, accessible from the **Configuration>Variables** menu. There you configure the notification text and the buttons that appear in the pop-up notification box the end user will see. You can also select to have a justification free form text field appear on the pop-up window. See [Notification Settings, page 9-27](#) for configuration information.

Presenting the user with a notification pop-up with various buttons and a justification edit field can serve the following purposes:

- Warn the end user that he/she may be performing an action that goes against corporate policy. You are not disallowing the action, you are simply notifying the user and requesting that a free-form text justification for the action be

entered into the pop-up. This text then appears in the MC event log. In this case, you may simply present a Yes button on the pop-up as an acknowledgement of the notification.

- As another example, you can notify the user when their system is quarantined due to a rootkit. This could be a simple notify pop-up with an OK button, explaining the quarantined state and asking the user to contact IT.

In addition to querying the user, you can require the user to type in a user justification statement in a pop-up window edit field. This free-form justification text typed in by the end user appears in the event log message on the MC. The presence of this field requires the user to explain why a resource is being accessed or an action is being performed.

Using the Set Action

Set is a singular configuration action that causes a particular, one-time, configuration item to occur when the criteria configured in the rule triggers on a system. For example, when a rule with “Set” configured triggers, a specific action occurs, such as the security level being set to low. This is different from Add and Remove process tagging. Add and Remove process tagging cause a tag to be bound to a process for the life of that process or until the tag is removed. Set causes a one-time action to occur.

**Note**

Set is similar to Add and Remove process tagging in one respect. You can configure the Set to occur based on a user query response. However, the only valid query response for Set is “Allow”. If the connection were to be denied, there would be nothing to mark.

**Note**

In some cases the resulting Set action may configure a global system state (Set Host Address as Untrusted). In other cases, the output of the Set action is to simply generate an event (such as Set Rule Module protection.)

When you select Set as the action type for a rule, an Attribute pulldown menu and a Value pulldown menu appear. For every attribute you can set, there are corresponding values that must also be set. There are several attribute and value pairs you can set for a rule.

**Note**

Not all attributes are available for every rule type. For example, Differentiated Service options are only available for Network access control rules. The applicable set attributes for the rule type in question will be the only types you can select for that rule.

The rest of this section describes possible attribute and value pairs.

Untrusted vs. Unchanged Trust Status

Several set attributes define the trust status of an object, such as an application or a file, as being either “unchanged” or “untrusted.” An object is designated as “untrusted” if CSA detects malicious behavior and a rule tags the object as “untrusted.” If CSA detects benign behavior that might be misinterpreted as malicious behavior, a rule tags the object’s trust status as “unchanged.” If an object is tagged as both untrusted and unchanged, the unchanged tag takes precedence and the action is not prevented based on the object’s trust status.

Attribute: Current Application Virus Classification

The **set current application Virus Classification** attribute assigns a static behavior-based AntiVirus tag to an application.

After specifying the **current application Virus Classification** attribute, select one of these values:

- Include no static tag
- Include the Tag <Virus:Behavior.Excessive Policy Violation>
- Include the Tag <Virus:Behavior.Malicious Activity>
- Include the Tag <Virus:Behavior.Dangerous Activity>
- Include the Tag <Virus:Behavior.Suspicious Activity>
- Include the Tag <Virus:Behavior.Potential Unwanted Application>

Many types of rules can assign a behavior-based antivirus tag to an application when the application interacts with another application and attempts a certain activity. Behavior antivirus tags are “static.” The tags can be assigned to an application and they can be configured by the administrator but their names cannot be changed.

If there are two rules with the same tagging requirements and one rule applies a “no static tag” and one rule applies one of the behavior static tags, the rule with the “no static tag” classification takes precedence and the application does not receive a static tag.

For more information about how these tags are used and how behavior-based antivirus works, see [AntiVirus Basics, page 15-2](#).

Attribute: Custom-made state condition

This set action allow you to define custom system states to suit your enterprise’s individual needs. After specifying the **Custom-made state condition** set attribute, select one of the values, **Custom 1** through **Custom 10**.

The custom-made state conditions can be created using many different rule types. This allows administrators to define custom states using a wide variety conditions.

A benefit of custom states is protecting resources without having a host enter a High, Medium, or Low security level system state. If users change the security level on their agent, this will have no affect on the rules that enforce security based on your custom system state.

Hosts can only be in one custom state at a time. If different rules, defining different custom states are triggered for the host, the host moves to the custom state that was triggered last. The host remains in that custom state until system states are reset on the agent. See [Resetting Cisco Security Agents, page 3-9](#) the procedure to reset an agent from the CSA MC. The **Detailed status and diagnostics** link on the Host Details page lists the system state(s) that the host is in. See the [“Host Status” section on page 3-31](#) for more information.

After you create a custom state, you will need to create a system state set that references the custom state. You can also configure the system state set to include additional factors like scanning data tags or static data tags. In order to protect a resource, you will then need to create a protection rule that specifies the new system state set.

Custom states can be defined by these rule types.

- Agent service control rule
- Application control rule
- Clipboard access control

Common Rule Page Configuration Items

- COM component access control
- Connection rate limit
- Data access control
- File access control
- File version control
- Kernel protection
- Network access control
- Network interface control
- Network shield
- Printer access control
- Registry access control
- Rootkit / Kernel protection
- Scan event log
- System API control

Attribute: Data Payload trust status

Values: After specifying the Data Payload trust status attribute, select one of these values:

- unchanged for any protocol
- unchanged if MSRPC
- unchanged if LPC
- untrusted if MSRPC (locally and globally)
- untrusted if MSRPC (locally)
- untrusted if LPC (locally and globally)
- untrusted if LPC (locally)
- untrusted for any protocol (locally and globally)
- untrusted for any protocol (local)

By using a rule that sets Data Payload trust status to Untrusted, you are configuring the system to try to create a signature when a specific type of action is detected by a rule. When this detection occurs, the payload is retrieved by the agent and signature generation is attempted. If a signature is generated by a rule that includes a global setting, the agent sends the signature to the MC for global distribution. Agents with rules that enforce restrictions based on global signatures then receive the newly created signature and are protected against that particular attack.

Locally and Globally Explanation

If a data payload is classified as unchanged or untrusted locally, it causes a generated signature to be temporarily added (for one hour) to the @signatures or @highrisk_signature lists on the local machine. Additionally, if the unchanged or untrusted global attribute is used, an event is sent to CSA MC to make the generated signature a candidate for global event correlation. If the signature is centrally correlated, it is added to the global signature list on all similar hosts, if the configured event correlation threshold is reached.

Attribute: Data scan on CLOSE

After specifying the Data scan on CLOSE attribute, select one of these **values**:

- being required for this file
- NOT being required for this file

The Data scan on CLOSE attribute is available for File Access Control rules (FACLs).

If a FACL **requires** a data scan on CLOSE, CSA compares the content of the file to the scanning data tag patterns when the file is closed. (These tags, and their definitions, may be found by navigating from the **Configuration** menu, **Global Settings > Scanning Data Tags**.) If the content in the file matches the pattern of a scanning data tag, the file is given the tag. A file may have more than one scanning data tag. (See [Scanning Data Tags and Static Data Tags, page 16-4](#) for more information on these types of tags.)

If a FACL does **NOT require a data scan**, the data scan does not occur.



Note

If a file gets marked as both **requiring** and **NOT requiring** a scan, a scan will not be performed.

Attribute: Data scan on OPEN

After specifying the Data scan on OPEN attribute, select one of these values:

- being required for this file
- NOT being required for this file

The Data scan on OPEN attribute is available for File Access Control rules (FACLs).

If a FACL **requires** a data scan on OPEN, CSA compares the content of the file to the patterns defined by scanning data tags, when the file is opened. (These tags, and their definitions, may be found by navigating from the **Configuration** menu, **Global Settings > Scanning Data Tags**.) If the content in the file matches the pattern of a scanning data tag, the file is given the tag. A file may have more than one scanning data tag. (See [Scanning Data Tags and Static Data Tags, page 16-4](#) for more information on these types of tags.)

If a FACL does **NOT require a data scan**, the data scan does not occur.



Note

If a file gets marked as both **requiring** and **NOT requiring** a scan, a scan will not be performed.

Attribute: detected access

Values: Protected, Unprotected

This attribute is intended to notify you (via the event log) and optionally take action (via a system state) when an application or service, or other system component that is marked as Unprotected does not have a corresponding Protected rule and is therefore not being protected by the agent.

To use this as a protection auditing tool, you would include a rule that is configured with “Set-detected access-Protected” for the resource that you are protecting in a policy. This rule marks the resource as being protected by the agent.

Subsequently, if you want to make sure that certain resources are being protected on systems, you would configure a “Set-detected access-Unprotected” rule for the resource in question and include it, for example, in a policy attached to the <All OS type> groups. This way, if a resource that requires protection is accessed on a

system and there a “Set-detected access-Unprotected” rule without a corresponding “Set-detected access-Protected” rule for that resource, a message is sent to the event log informing you that the resource is not protected.

For example, you could use this feature to ensure that hosts running Web servers are properly protected. To accomplish this, you would write a set rule in the All Windows Group that said “Set-detected access-Unprotected” when any application acts as a server for TCP/80. Another rule would be added to the Microsoft IIS Web Server module specifying to “Set-detected access-Protected” when IIS accepts a connection for TCP/80. (A similar rule could be added for Apache in the corresponding module.) Hosts running an IIS Web Server that have both policies attached would meet the protection criteria and no event would be logged. Hosts with policies that specify the requirement for protection (Unprotected) with no corresponding protection provided (Protected) would have a policy mismatch and would generate an event as a result.

You can configure a System State to apply if a corresponding Set rule of this type triggers. See [System State Sets, page 9-40](#).

Attribute: detected boot

Values: Insecure, Secure

This attribute is intended to detect when a previous system boot occurred in a non-standard manner. For example, the system was booted from a peripheral device (CD ROM) rather than from the hard drive. This type of boot can be considered non-standard and therefore possibly suspicious. (This is one way of introducing a Trojan to a system.) This type of peripheral device insecure boot detection works in conjunction with a particular type of compatible BIOS on compliant systems. The compatible BIOS detects a non-standard boot and on the next normal boot, if you have an appropriately configured Kernel Protection rule (see [Kernel Protection, page 6-53](#)), a message is sent to the MC which logs this insecure boot detection. This, in turn, causes the system state (if configured) to trigger. A Safe Mode boot also falls into this insecure boot category. Compatible BIOS is not required for a Safe Mode boot detection.

You can configure a System State to apply if a corresponding Set rule of this type triggers. See [System State Sets, page 9-40](#).

Attribute: detected rootkit trust status

After specifying the detected rootkit trust status attribute, select one of these values:

- Unchanged
- Untrusted

The set attribute is available for kernel protection rules.

A rootkit may be detected when module loads after boot time or a module attempts to modify kernel functionality. Note that if the trust status of a rootkit gets marked as both unchanged and untrusted, the unchanged rootkit trust status gets precedence over an untrusted rootkit trust status.

You can configure a System State to apply if a corresponding Set rule of this type triggers. See [System State Sets, page 9-40](#).

Attribute: Differentiated Service (Trusted QoS)

Values: priority Best Effort (0,0), priority Scavenger (8, CS1), application specified, IP routing (48, CS6), Voice (46, EF), Interactive Video (34, AF41), Streaming Video (32, CS4), Mission Critical Data (26, AF31), Call Signaling (24, CS3), Transactional Data (18, AF21), Network Management (16, CS2), Bulk Data (10, AF11), Best Effort (0,0). Scavenger (8, CS1)

You specify Differentiated Service for a certain traffic flow by setting a QoS marking which is a recognizable value in an IP packet. This allows routers and switches to identify and take action on QoS-marked traffic, providing finer granularity of control in forwarding traffic.

The available markings provide a DSCP (Differentiated Services Code Point) setting and a PHB (Per Hop Behavior) setting. The DSCP value matches the service field in the IP header. The PHB value matches the way routers and switches handle traffic on a hop by hop basis. These values appear in parenthesis beside each value option in the following order (DSCP,PHB).



Note

While all provided value markings are not described here, you should note that by default, applications transfer with a Best Effort value. The provided Scavenger value is lower than Best Effort. You would use a Scavenger marking to

significantly downgrade a certain type of traffic flow. The **priority** Best Effort and **priority** Scavenger values are provided to allow you set a prioritization between multiple rules that may be using multiple types of markings.

Important Details about CSA Differentiated Service Functionality

In the absence of any rules on the agent that provision QoS markings, the general default of all systems is to mark traffic flows as “application specified”. In the presence of rules on the agent that provision QoS markings, the agent will select and provision DSCP markings accordingly. If there is a Differentiated Service rule conflict on the agent (i.e. more than one applicable Differentiated Service set rule for a traffic flow), the agent picks the highest marking to provision. (The precedence order of markings is the available pulldown list, top to bottom.)

Note that the agent is only marking packets that it transmits. The agent cannot mark packets that it receives. It is the responsibility of the remote host to mark those packets appropriately.

When the agent is disabled, stopped, or turned to Off using the security slide bar, existing sessions are no longer QoS provisioned by the agent. The agent stops marking existing flows. Existing flows then revert to “application specified”. If the agent is re-enabled, authorized flows resume the previous marking provisioned by the agent. If a new session is created during the time the agent is disabled, the new flow is not interfered with when the agent is back in the picture. That flow is automatically given the general system default of allow with an application specified marking and it retains that marking for the life of the connection.

Note that we only authorize at the beginning of a connection.

Note that Audit Mode has no bearing on Differentiated Service functionality. The agent provisions the specified markings even if Audit Mode is enabled.

Refer to RFC 2475 for general information on Differentiated Services.

You can configure a System State to apply if a corresponding Set rule of this type triggers. See [System State Sets, page 9-40](#). For example, if your network is under attack (i.e. “virus detected”) you can configure a system state to trigger that uses rules to downgrade all traffic flows.

Attribute: Discovery of other CSA nodes

Values: Disabled, Enabled

This set attribute is available for the following rule types; Buffer Overflow, Connection rate limit, Data access control, Network access control, Network Shield, and System API. It is intended to determine if a host IP address has an active Cisco Security Agent associated with it. If so, a list of active agent systems is maintained and can be used in rules, via a cookie (@csanode) to restrict or allow communication and resource availability based on the presence of an active agent. For example, if an agent is detected on a system, allow the system in question to communicate with “n” systems. Using this set rule type, you can enable/disable csa node detection on a per connection basis.

Attribute: file Data Classification

Values: Static data tags

The set attribute is available for file access control (FACL) protection rules. This attribute allows a file to be tagged with a static data tag without having to scan its contents.

After specifying the file Data Classification attribute you select a static data tag from the values list. Static data tags are distributed with this release of CSA and are available for you to configure and use. See [Scanning Data Tags and Static Data Tags, page 16-4](#) for more information on these types of tags.

You cannot change the names of these tags and you cannot create new static data tags. Static data tags are assigned to files based on what group of applications attempt to access them. You define the parameters for static data tags based on your enterprise's needs. This tagging method may be useful if, for example, you have a specialized application. For example, you may know in advance that any file that your specialized application reads should be considered a <HIPAA Controlled> file.

Attribute: File deletion

After specifying the **File deletion** attribute, select one of these values:

- being required for this file
- NOT being required for this file

The File deletion attribute is available for Scan Event Log rules.

This attribute allows you to mark a file with a scanning data tag, static data tag, or virus scanning tag for deletion by the Security Agent.

Note that if a file gets marked as both **requiring** and **NOT requiring** deletion, the delete will not be performed.

Attribute: file trust status

After specifying the detected rootkit trust status attribute, select one of these **values**:

- Unchanged
- Untrusted

The set attribute is available for file access control (FACL) protection rules.

A file may be marked as Untrusted if the Cisco Security Agent considers the file type to have executable or interpretable content. Thus, with the default Windows handling for file extensions, a .txt file would not be considered executable, and would not trigger the Set-File-Untrusted rule.

Executable files that are persistently tracked in the agent UI Untrusted Applications window (see [The Agent User Interface, page A-8](#)) are localized to each system. Applications that appear in that localized list are automatically added to the built-in application class <*Processes Executing Untrusted Content> (see [Built-in Application Classes, page 8-4](#)) and, in turn, that populated built-in application class can be used in rules.

Note that if a file gets marked as both unchanged and untrusted, a unchanged file tag gets precedence over an untrusted file tag.

Attribute: Host address trust status

After specifying the Host address trust status attribute, select one of these **values**:

- Unchanged
- Untrusted (locally)
- Untrusted (locally and globally)

The set attribute is available for network access control rules on Windows platforms and connection rate limit rules on Unix platforms.

This Host address attribute is intended to mark the IP addresses of hosts as untrusted when they violate security policies or exhibit malicious behavior. Being classified as an untrusted host (locally) causes that host to be temporarily added (for one hour) to the @dynamic list on the local machine. Additionally, if the

untrusted global attribute is used, an event is sent to CSA MC to make the host address a candidate for global event correlation. If this address is centrally correlated, it's permanently added to the global quarantine list on all hosts (if the configured event correlation threshold is reached).

**Tip**

You may want to use the local untrusted value for an external web server that is continually hit by external hosts. This way, those hosts that appear malicious wouldn't become globally quarantined for your entire internal network, but they would be temporarily prevented from communicating with the web server.

You can configure a System State to apply if a corresponding Set rule of this type triggers. See [System State Sets, page 9-40](#).

Attribute: Security level

Values: High, Medium, Low

Set the Security Level attribute 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 be applied when the state has been moved to high. On a high setting, you may enforce a rule that denies the virus-infected system from making outgoing network connections.

You can configure a System State to apply if a corresponding Set rule of this type triggers. See [System State Sets, page 9-40](#).

Attribute: Stack

Values: recovery

If you are using the Set Stack Recovery action, you are configuring the system to try to recover and unwind the stack back to a safe place when an unhandled exception has occurred. Stack recovery is intended for vital services only. You may simply want to let non-vital services fail.

Attribute: Sensitive Data Scan

Values: being required for this file, NOT being required for this file

A file may be marked as requiring or not requiring a scan for sensitive data.

Attribute: Timer to restore Security

After specifying the Timer to restore security, select a **time value** or specify that restoring security is **NOT being required**.

The time value indicates how long after CSA security has been set to “Off” or a after a “net stop csagent” has been performed will CSA security be turned back on automatically.

The Timer to restore security attribute is available for Agent Service Control rules.

If a host is affected by several Agent Service Control rules with differing time values for restoring security, and one of those values is **NOT being required** then restoring security as **NOT being required** takes precedence over all other time settings. In this case, CSA will not be restarted automatically.

If there are more than one required time setting specified by various Agent Service Control rules and there are no rules specifying that restoring security is NOT being required, the shortest time configuration required to restart security takes precedence over all others.



Note

This set attribute is not available for Solaris agents.

Attribute: Virus scan

After specifying the Virus scan attribute, select one of these **values:**

- being required for new application
- NOT being required for new application

The set attribute is available for Application control rules.

When the virus scan is required, an application control rule using this set attribute, causes CSA to perform a virus scan, with Clam AntiVirus, when an application from one application class attempts to run an application from another application class.

When a virus scan is not required, the virus scan does not occur. If a file is affected by a rule which does not require a virus scan and a rule that does require a virus scan, the virus scan does not occur.

When CSA detects a Application control rule on the host with this set attribute, the AntiVirus window, in the agent interface, becomes available to the user. See “[AntiVirus Protection](#)” section on page [A-17](#) for a description of the AntiVirus screen in the agent interfaces.

Attribute: Virus scan on CLOSE

After specifying the Virus scan on CLOSE attribute, select one of these **values**:

- being required for this file
- NOT being required for this file

The Virus scan on CLOSE attribute is available for File Access Control rules (FACLS).

When the virus scan is required, A FACL using this set attribute causes CSA to perform a virus scan, with Clam AntiVirus, when an application attempts to write a file, or when an application attempts to create, rename, or delete a directory. The virus scan occurs when the user closes the file. If a virus has infected a file, the infection will be caught immediately after the file has been modified.

When a virus scan is not required, the scan does not occur. If a file is affected by a rule which does not require a virus scan, and a rule that does require a virus scan, the virus scan does not occur.



Note

When CSA detects a FACL on the host with this set attribute, the AntiVirus window, in the agent interface, becomes available to the user. See “[AntiVirus Protection](#)” section on page [A-17](#) for a description of the AntiVirus screen in the agent interface.

Attribute: Virus scan on OPEN

After specifying the Virus scan on OPEN attribute, select one of these **values**:

- being required for this file
- NOT being required for this file

The Virus scan on OPEN attribute is available for File Access Control rules (FACLs).

When the virus scan is required, a FACL using this set attribute, causes CSA to perform a virus scan, with Clam AntiVirus, when an application from an application class attempts to Read or Write a file, or when an application from an application class attempts to create, rename, or delete a directory. The virus scan occurs when the file is opened.

When a virus scan is not required, the scan does not occur. If a file is affected by a rule which does not require a virus scan and a rule that does require a virus scan, the virus scan does not occur.



Note

When CSA detects a FACL on the host with this set attribute, the AntiVirus window, in the agent interface, becomes available to the user. See “[AntiVirus Protection](#)” section on page A-17 for a description of the AntiVirus screen in the agent interface.

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 9-29](#) for configuration details.

**Caution**

For Solaris rules, Query user actions are selectable on the MC but query pop-ups are not displayed on Solaris agent host systems. Instead, if you configure a Query user rule for a Solaris system, the default action is immediately taken on the system if the rule is triggered.

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 policies.

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 5-9 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.

Logged query responses—In addition to deciding which query actions (Allow, Deny, Terminate) are available to the user for the query pop-up, you can also configure the query response to log only when a particular query action is selected by the user. Using the multi-select box available from the

Logged query responses section, you can select one or more response types to produce a log message. For example, if all query actions are being made available for the query, you can configure only a Terminate response to produce a log message. (By default, all query responses are logged.)

Don't ask me again—In addition to the buttons 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 9-29](#).)



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.

Justification—In addition to simply querying the user, you can require the user to type in a user justification statement in a pop-up window edit field. This justification text typed in by the end user appears in the event log message on the MC. The presence of this field requires the user to explain why a resource is being accessed or an action is being performed.

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.

Notes about Query Caching

- Permanent responses are remembered across reboots.
- Temporarily cached responses are not remembered across reboots.
- When a query response is cached temporarily for one hour, if during that one hour time frame, the cached response is used by a subsequent rule request, the window is extended by an hour.
- 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

Rule Overrides

Audit Mode and Learn Mode are useful tools during piloting or initial deployment of CSA.

Using Audit Mode

Audit 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 audit mode, the agent will not deny any action or operation even if an associated rule indicates that 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 or rule module on a host before enforcing it. If examining the logs shows you that the policy or rule module is working as intended on a group, you can then remove the audit mode designation.

When using Group audit mode (available from the Rule Overrides area), you may 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 audit mode sends events to CSA MC, event log messages are preceded with the word “Audit”. 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 word “Audit.” Event detection (not prevention) messages appear the same in the event log regardless if audit mode is on or off.

Group Audit Mode

If audit mode is enabled on the group level, all rules on hosts within audit mode groups are in audit mode.

If a host belongs to a group with audit mode selected, all policies associated with that host are in audit mode (even if the host is part of another group that does not have audit mode selected), not just the policies applied to the audit group. Therefore, audit mode applies to the host as a whole, not to specific policies.

You can determine if a group is in audit mode in one of these ways:

- In the groups list page, the row that identifies a group will display an **A** among the group’s attributes. You can reach the groups list page by navigating **Systems > Groups** from the CSA MC menu bar.
- When displaying the group’s details page, the Audit mode check box, in the Rule Overrides area, will be selected. You can see a group’s details page by clicking on a group in the groups list page.
- On the Host Security page, the Audit Mode checkbox in the row that describes the group is checked. You can reach the Host Security page by navigating **Configuration > Host Security** from the CSA MC menu bar.



Note

Using the Hosts Managing Tasks page, you can configure “timed” audit mode. Basically, you can configure a task that causes hosts to move in and out of selected groups at timed intervals. This way, you can have all new hosts move out of a group in audit mode and into a group in live mode after a 30 day pilot, for example. Refer to [Host Managing Tasks, page 3-51](#) for configuration information.

Rule Module Audit Mode

You can also use audit mode on the rule module level. If a rule module attached to a policy is in audit mode, only the rules associated with that rule module are run in audit mode. The rules in the other rule modules of the policy continue to be run in whatever mode they are configured for. 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.

If a rule module is in audit mode, and it is used in more than one policy, the rule module will be in audit mode in every policy to which it is assigned.



Caution

You should be aware that putting a deployed “live” rule module into audit mode turns off all security that the rule module in question had been providing. Keep this in mind when using audit mode to analyze how rule modules are working.

You can determine if a rule module is in audit mode by looking in one of these locations:

- In the rule module list page, the row that identifies the rule module will display an A in the Attributes column. You can reach the rule module list page by navigating **Configuration > Rule Modules** from the CSA MC menu bar.
- In the policies details page, the row that identifies the rule module will display an A in the Attributes column. You can reach the policy details list page by navigating **Configuration > Policies** from the CSA MC menu bar and then clicking the name of a policy.
- In the group details page, expand the combined policy rules. The rules are displayed in rows and the rule’s rule module is referenced. If the rule module is in audit mode, the rule module will display an A next to its name. You can view the group details page by navigating **Systems > Groups** from the CSA MC menu bar and then clicking the name of a group.

Policy Audit Mode

A policy can only be put in test mode in the context of a group. This means that if a policy is in more than one group, the policy could be in audit mode in one group and in live mode in another group. For a group that uses the policy in audit mode, all of the rules in that policy are in audit mode.

If a host uses two identical rules and one is in audit mode and one is in live mode, both rules will trigger. The audit mode rule will have no effect. The live mode rule will enforce whatever action it is designed to enforce.

You can determine if a policy is in audit mode by looking in one of these locations:

- From the group details page, in the row that identifies the policy, the Audit Mode check box will be selected. You can view the group details page by navigating **Systems > Groups** from the CSA MC menu bar and then clicking the name of a group.
- In the Host Security page, click a group name to see the policies that it uses. The Audit Mode check box will be selected if the policy is in audit mode for that particular group. You can reach the Host Security page by navigating **Configuration > Host Security** from the CSA MC menu bar.

Identifying Hosts in Audit Mode

A host is considered to be in audit mode if any group to which it belongs is in audit mode. Individual rules on a host may be in audit mode if a rule module, or a policy for a group to which the user belongs, is in audit mode. Hosts, themselves, cannot be configured to be in audit mode.

If you want to determine the extent to which a host is auditing rules or enforcing rules, look at these locations:

- On the hosts details page, click **Host Settings** in the Status area. If audit mode is marked “on” then at least one group to which the hosts belongs is in audit mode. You can reach the host details page by navigating **Systems > Hosts** from the CSA MC menu bar, and then clicking the name of the host you are investigating.
- In the host details page, look at the **Group Membership and Policy Inheritance** table. A group or a policy in audit mode will be marked with an **A** in their attributes column. Expand the group name to look at the rule modules associated with the group. Rule modules in audit mode will also be marked with an **A** in their attributes column.

Using Learn Mode

Learn mode is intended to localize policies on individual systems, eliminating the initial flurry of pop-up queries that users may experience when the agent is first installed on a system. This flurry of queries is a result of query rules that are deployed to let end users decide when an unknown system action is normal or abnormal. When the agent is first deployed, these pop-up queries can be numerous since the agent is seeing system actions for the first time. Unfortunately, this initial bombardment of queries for actions that are likely benign (in most cases) can train the user to respond Yes to the majority of queries they see.

To solve this problem without removing useful query rules from your deployment, you can enable Learn mode for a temporary period of time. Learn mode directs the agent not to display query pop-ups, and to instead take an immediate *Allow* query response when a query rule is triggered, and to persistently save the allow response.

If you intend to use Learn mode, the queries that qualify for learning must have certain options enabled. While Learn mode is enabled from either the Group page or the Rule module page, queries are defined from the Configuration>Variables>Query Settings menu. There are several pre-configured queries listed on the query settings page. In order for Learn mode to work, you must do the following:

- Enable **Learn mode**, located in the Rule overrides section, on either the Group page or on a specific Rule module page.
Like Audit mode, Learn mode can be enabled for all persistent queries in all policies running on hosts (Group Learn mode) or enabled for specific persistent queries located in a particular Rule module (Rule module Learn mode).
- Access the Query Setting configuration page (see [Query Settings, page 9-29](#)) for the query you want to deploy for learning. A query qualifies for learning if:
 - The **Enable “Don’t ask again” option** is selected
 - **Allow** is selected as one of the Allowed query actions

Once query responses are taken, and Learn mode is turned off, the majority of queries no longer appear and system security provided by the agent is normalized to the individual system. At this point, users should only see query pop-ups for unusual or suspicious system behavior.

Additional Notes on Learn Mode

- All qualifying queries will be answered with an automatic and persistent Yes for the time frame that Learn mode is enabled. (You must remember to turn Learn mode off after a reasonable amount of time.)
- An event is logged to the MC Event Log when a query is triggered and learned. This event is formatted similar to most events, but it explains that a query response was taken and that learn mode was turned on for the query in question.
- The learned allow responses are displayed in the agent User Query Responses window as they occur.
- If both Audit mode and Learn mode are enabled for a query rule, learning does not occur.
- Using the Hosts Managing Tasks page, you can configure “timed” Learn Mode. Basically, you can configure a task that causes hosts to move in and out of selected groups at timed intervals. This way, you can have all new hosts move out of a Learn Mode group after a set time. Refer to [Host Managing Tasks, page 3-51](#) for configuration information.
- When in Learn Mode, the agent learns the various applications that are running on the local machine. It also learns any unusual systems calls that are typically exhibited by the machine. Consequently, any applications that have been seen running on the system during the Learn Mode period will not trigger or be classified as a “first time execute” application when it is first run after the learning period. And any unusual systems calls that were observed during learning will not trigger the unusual system calls detection in the System API rule.

■ Rule Overrides



CHAPTER 6

Available Rule Types

Overview

Rule modules contain various types of rules. Each rule type is intended to control a different set of system resources. For example, there is a rule type that controls access to files and directories and another rule type that controls network accesses. It is through the combining of the many available rule types that a rule module provides overall security to the entire system. This chapter provides information on each rule type.

This section contains the following topics.

- [Rules Common to Windows and UNIX, page 6-3](#)
 - [Agent Service Control, page 6-3](#)
 - [Agent UI Control, page 6-6](#)
 - [Application Control, page 6-11](#)
 - [Connection Rate Limit, page 6-15](#)
 - [Data Access Control, page 6-19](#)
 - [File Access Control, page 6-23](#)
 - [Network Access Control, page 6-29](#)
 - [Network Shield Rule, page 6-34](#)
- [Windows Only Rules, page 6-42](#)
 - [Clipboard Access Control, page 6-42](#)
 - [COM Component Access Control, page 6-45](#)

- File Version Control, page 6-49
- Kernel Protection, page 6-53
- NT Event Log, page 6-57
- Printer access control, page 6-59
- Registry Access Control, page 6-61
- Scan Event Log, page 6-64
- Service Restart Rule, page 6-67
- Sniffer and Protocol Detection, page 6-69
- System API Control Rule, page 6-71
- UNIX Only Rules, page 6-78
 - Network Interface Control, page 6-81
 - Resource Access Control, page 6-84
 - Rootkit / kernel Protection, page 6-86
 - Syslog Control, page 6-90

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 12, “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 5-4.](#)

-
- Step 1** To add rules to your module, expand the rules area of the rule module and click the **Add** button. 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 6-1](#)).

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 5-18](#).

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 5-22](#) 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 8, “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 sidebar 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 6-6](#) 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 Audit 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 6-1 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 Audit 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 6-2](#). 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** 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 sidebar 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 6-3](#)). You must both provide this sidebar 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 sidebar 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.)

- **Suppress taskbar notifications**—Selecting this check box in the Agent UI control rule, greatly reduces CSA notifications to the user. If the option is selected, user interaction with CSA is changed in these ways:
 - The user no longer receives balloon messages.
 - The flag icon in the system tray on longer pulses.
 - The user no longer receives tool-tip text in the task bar icon.
 - The user will no longer hear sounds for security events.

**Note**

Users also have control over suppressing taskbar notifications. On the agent shortcut menu, users can select “Suppress Taskbar Notifications.” If users choose to suppress taskbar notifications, then they gain control over turning this function on or off in the future. If an administrator changes the Suppress taskbar notifications check box in this rule after a user changes the setting, the administrator’s action will have no affect on that user.

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 policies. (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

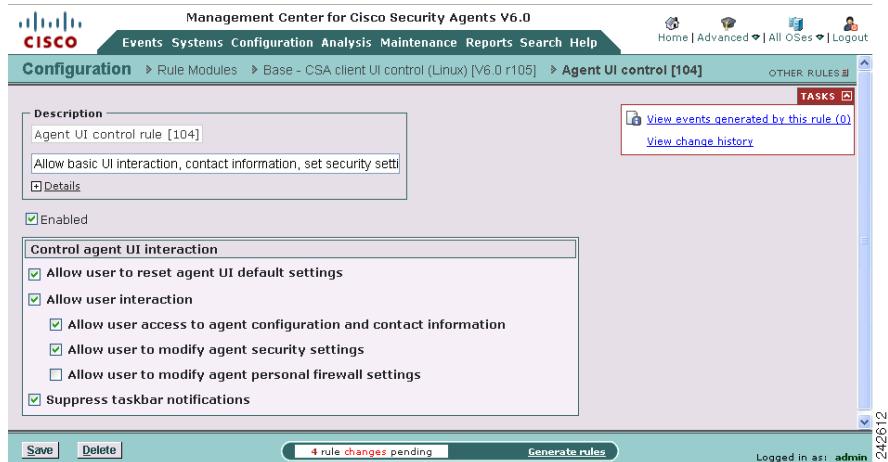
If a host belongs to multiple groups with multiple policies, having a visible agent UI setting, if present in any group for which the host is a member, takes precedence over a no user interaction agent UI setting.

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, page 3-26](#)).

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 policies.

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.

■ Rules Common to Windows and UNIX

Figure 6-2 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.

**Note**

These instructions are a continuation of [Configuring Rule Modules, page 5-4](#).

-
- Step 1** To add rules to your module, expand the rules area of the rule module and click the **Add** button. 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 6-3](#)).
- 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 5-18](#).

**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**—For enforcement 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 5-22](#) for details.

Step 6 when

- **Current applications in any (or all) of the following selected classes**—If you want to control an application (allow or deny) running on a system no matter how it is 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).

If you choose **Applications in any of the following selected classes**, the rule will affect an application that is a member of one of the selected application classes.

If you choose **Applications in all of the following selected classes**, the rule will affect an application that is a member of every application class you select.

You may also create a new application class by clicking the blue **New** link next to the application class list box. For application class configuration details, see [Chapter 8, “Using Application Classes”](#)

(When your rule is configured, currently selected application classes appear at the top of the list. See [Configuring Static Application Classes, page 8-8](#) 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.

Step 7 attempt to run

- **New applications in any (or all) of the following selected classes**—Select the application you want to control if an attempt is being made to run it by the application defined by the **Applications in any (or all) of the following selected classes** field.

If you choose **New applications in any of the following selected classes** the rule will control an application that is a member of one of the selected application classes.

If you choose **New applications in all of the following selected classes**, the rule will affect an application that is a member of every application class you select.

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 8 And —

For detection rules, in this area, specify the enforcement action taken by CSA.

Specifying Allow by default or Allow if triggered by a rule indicates applications that have been allowed to run by other rules. Specifying, Terminated or Denied by rule indicates applications that have been prevented from running by other rules.

Step 9 When you are finished configuring your Application control rule, click the **Save** button. This rule is now part of your rule module. It takes effect when the rule module is attached to a policy, the policy is attached to a group and then downloaded by an agent on the network.

Rules Common to Windows and UNIX

Figure 6-3 Application Control Rule

The screenshot shows the 'Management Center for Cisco Security Agents V6.0' interface. The title bar includes the Cisco logo and navigation links: Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, Help, Home, Advanced, All OSes, and Logout. The main menu path is Configuration > Rule Modules > Security - Prevent Downloaded apps from being run [V6.0 r105] > Application control [9]. A 'TASKS' button is visible in the top right.

Description: Application control rule [9]
 Details

Enabled:

Take the following action:

- Priority Deny
- Log
- Take precedence over other Priority Deny rules

when:
 Current applications in the following class:
 <[All Applications](#)>

But not in the following class:
[Administrator defined - White List Applications \[V6.0 r105\]](#)

attempt to run:
 New applications in the following class:
[Administrator defined - Applications considered Untrusted \[V6.0 r105\]](#)

But not in the following class:
 <[none](#)>

Buttons at the bottom: Save, Delete, 4 rule changes pending, Generate rules, Logged in as: admin, 2:426 13

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. For example: 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 5-4](#).

Step 1 To add rules to your module, expand the rules area of the rule module and click the **Add** button. 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 5-18](#). (Note that you cannot configure Query User Connection rate limit rules. Also note that if you select the Set action for marking a host as untrusted, you can only configure the rule for servers and for specific hosts.)

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 8, “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, different 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. Selecting the “different” hosts option would be beneficial for controlling outgoing connections. For example, if a system on your network has been infected by a network worm, you could control the worm replication by tracking how many different hosts the infected system is trying to connect to and setting a limit to those connections. If you only tracked all host connections in this case, you may cut the system off from legitimate server access, for example.

Step 8 hosts having addresses - Type in a literal network address or a reference to a network address set variable (preceded by a dollar sign). See [Using the Correct Syntax, page 2-41](#) for a full description of proper IPv4 and IPv6 address syntax.

You can also click the **Insert Network Address Set** link to access a list of pre-configured network address sets. From the Insert Network Address Set link, click the New “**shortcut**” item to create a new network address set variable without leaving the rule page.

**Note**

IPv6 addresses can only be used by a rule associated with a Vista rule module.

**Note**

You can use the “short hand” symbol **@local** to indicate all local addresses on the agent system. Use **@remote** to indicate all address that are not on the local agent system. Refer to [Using the Correct Syntax, page 2-41](#) for more information and additional shorthand symbols.

Step 9 Using these local interfaces - The default entry here is <all>, indicating all addresses. Generally, you should not have to change this. Note that you cannot enter a “literal” in this field. You must select a preconfigured variable from the Insert Network Interfaces Set link if you want to change the default here. If you want to define a local interface using a combination of interface type and network address, create a network interface set that specifies that combination.

**Note**

<All> is the only valid setting for UNIX, Solaris, or Linux platforms.

Step 10 Over/Under a limit <100> network connections in <5> minutes

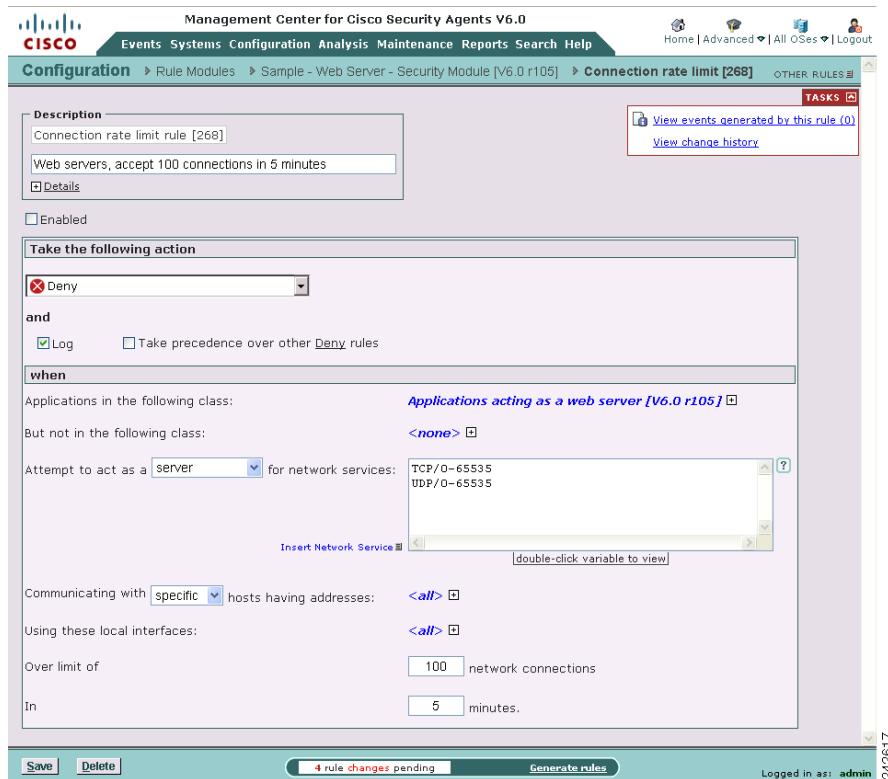
Reasonable values are entered into these fields by default. They define the number of connections that can normally be expected during a time frame from either specific hosts or all hosts.

- 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.

Rules Common to Windows and UNIX

Step 11 When you are finished configuring your connection rate limit rule, click the **Save** button.

Figure 6-4 Connection Rate Limit Rule



Data Access Control

Data access control rules are used for these purposes:

- Protecting web servers
- Protecting MSRPC and LPC interfaces

See also, [Creating Data Access Control Rules, page 6-21](#).

Protecting web servers

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.



Note

Data access control rules specifying HTTP protocol data sets are not supported for desktop versions of Windows operating systems.

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 9-7](#)) 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, versions 1.3, 2.0)

**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.

For Windows Vista, if you want to install Internet Information Services (IIS), you need to make sure that the **IIS Metabase and IIS 6 configuration compatibility** and **ISAPI Filters** features are included in the installation.

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 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 12-11](#) for instructions.

Protecting MSRPC and LPC interfaces

Once the CSA MC has collected and correlated enough malicious payloads from attacks on MSRPC or LPC interfaces, it creates a signature representing the attack. The signature is associated with the @signatures token. After the signature has been distributed to the agent on a host, if a payload matches the attack signature, a data access control rule prevents the application from processing it and the attack fails.

If an MSRPC or LPC interface has been attacked numerous times and a signature can not be generated, the payloads associated with the interface under attack are associated with the @highrisk_signatures token. If a new payload is received and

it is matched to the payload tags associated with the @highrisk_signatures token, a data access control rule prevents the application from processing the payload and the attack fails.

See [Chapter 14, “Automatic Signature Generation”](#) for a detailed discussion of the automatic signature generation feature.

Creating Data Access Control Rules

**Note**

These instructions are a continuation of [Configuring Rule Modules, page 5-4](#).

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, expand the rules area of the rule module and click the **Add** button. 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 5-18](#).
- 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 5-22](#) 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 8, “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.

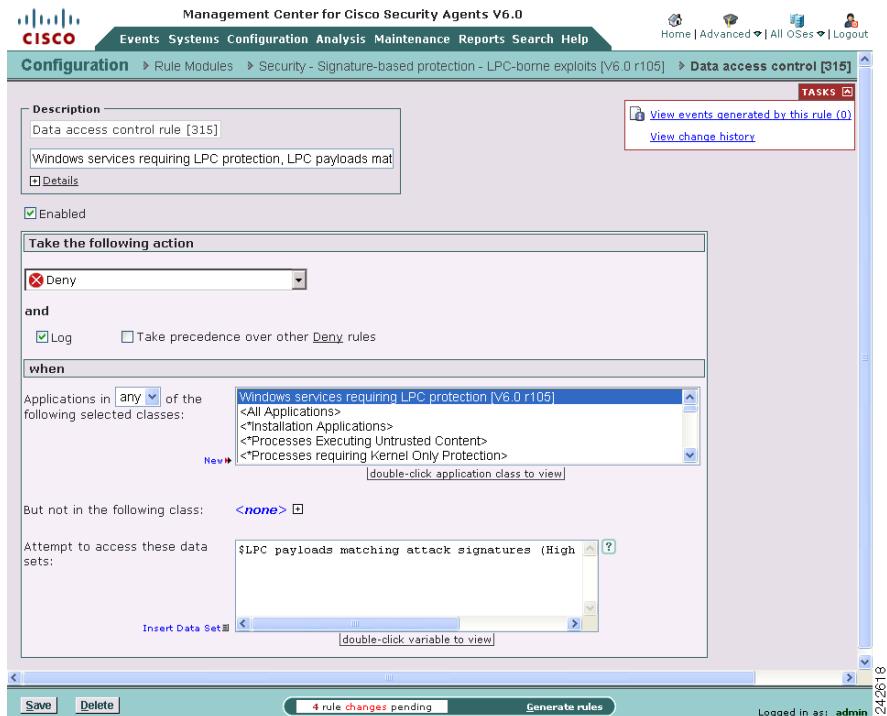
Step 7 Attempt to access these data sets

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. See [Data Set Pattern Matching Syntax, page 2-55](#) for a complete discussion of valid syntax.

For information on configuring Data Sets, see [page 9-7](#).

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

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

Figure 6-5 Data Access Control Rule

File Access Control

Use file access control rules to limit allowable system file actions to named files or directories based on these factors:

- The action itself (Deny, Allow)
- The application performing the action (Web Browser, Mail Client)
- The operation performed (Read, Write)

Whereas file protection enforces read and write access, directory protection encompasses directory deletes, renames, and new directory creation.



Note

These instructions are a continuation of [Configuring Rule Modules, page 5-4](#).

Step 1 To add rules to your module, expand the rules area of the rule module and click the **Add** button. 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 5-18](#) and [Rules: Action Definitions, page 5-19](#).

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 5-22](#) for details.

Step 6 **When**—

- **Applications in any (or all) 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. You may also create a new application class by clicking the blue **New** link next to the application class list box.

If you choose **Applications in *any* of the following selected classes** the rule will affect an application that is a member of one of the selected application classes.

If you choose **Applications in *all* of the following selected classes**, the rule will affect an application that is a member of every application class you select.

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 by clicking the blue **New** link next to the application class box. For application class configuration details, see [Chapter 8, “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. You may also create a new application class by clicking the blue **New** link next to the application class list box.



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

Step 7 Attempt the following operations —

Select either or both the **Read File** or **Write File** operations you are allowing or denying on the files named in the **On any of these files box**. If you want to prevent an application from opening a file for reading, select Read file. If you want to prevent an application from opening a file for writing, select Write file.

For directory protection, the “Write” actions you are allowing or denying are **Create**, **Delete**, and **Rename**. Refer to File and Directory protection in [Using the Correct Syntax, page 2-41](#).



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 [Directory and Filename Syntax Requirements, page 2-43](#).

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>\<i><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 9-12](#).

You can enter more than one file path, but each entry must appear on its own line. You can use File Set variables here. See File Sets for configuration details. By default, this field has a <none> entry indicating no files. When you click inside this field, the <none> disappears so that you can enter your own file restrictions.



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.

**Caution**

If you are using file path literals, you should refer to Using the Correct Syntax. When entering file path literals in File access control rules, the entry `c:\winnt` will allow actions on files in that directory, but it will not allow new files to be saved in the `winnt` directory and it will not allow file deletions. You must enter `c:\winnt*` to include the protection of existing files within that directory in rule restrictions.

**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 **dynamically quarantined files** link on the Event Correlation page. See [Manage Dynamically Quarantined Files and IP Addresses, page 7-10](#) for more information.

Step 9

And — In this area, specify the enforcement action CSA took when the application attempted to access the file.

Indicating **Allow by default** or **Allow if triggered by a rule** indicates that CSA allowed the application to access the file. Indicating **Terminated** or **Denied by rule** indicates that CSA prevented the application from accessing the file.

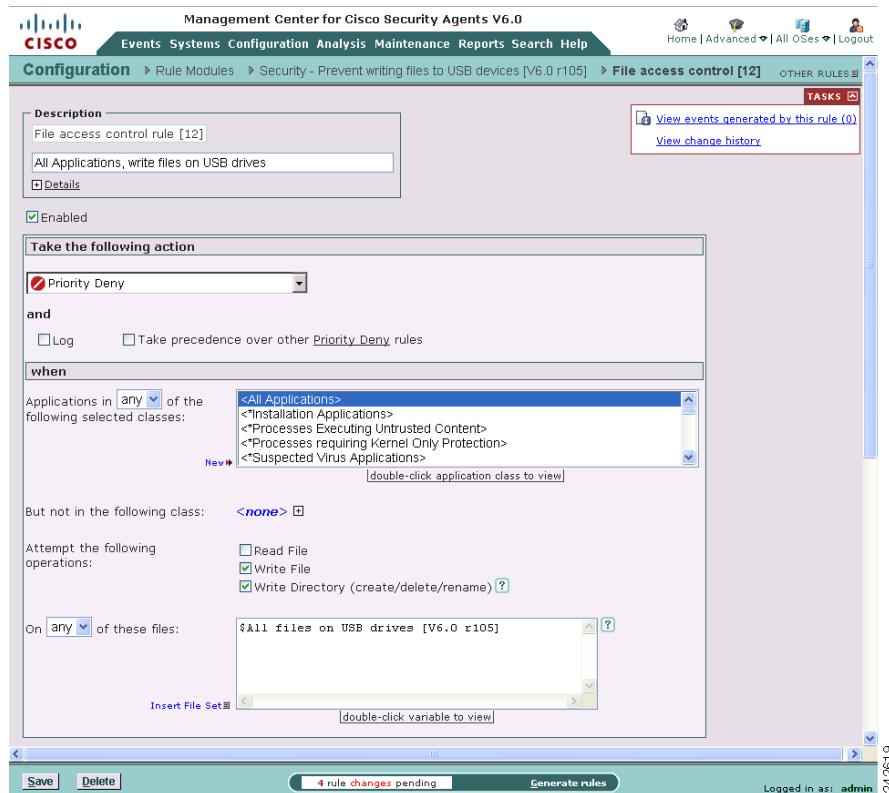
Step 10

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.

**Note**

In order to distribute rules to the correct hosts, you must associate policies with groups and then Generate rules. See [page 5-16](#) for instructions.

Rules Common to Windows and UNIX

Figure 6-6 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 5-4](#).

Step 1 To add rules to your module, expand the rules area of the rule module and click the **Add** button. 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 5-18](#).

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 5-22](#) 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 8, “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 6-32](#) 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. See [Network Services Syntax, page 2-53](#) for more information about entering protocol/port number combinations.

This field refers to either a server providing this service or a client accessing this service. For Network Service configuration details, see [page 9-24](#).

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. See [Network Address Set Syntax Requirements, page 2-50](#) for a full description of proper IPv4 and IPv6 address syntax.

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.



Note A NACL rule must be associated with a Vista rule module to accept IPv6 address literals and network address sets including IPv6 addresses.

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 [Short hand notation for network address sets, page 2-52](#) for more valid tokens that can be used in this rule type.

Step 10 Using these local interfaces

The default entry here is <all>, indicating all addresses. Generally, you should not have to change this. Note that you cannot enter a “literal” in this field. You must select a preconfigured variable from the Insert Network Interfaces Set link if you want to change the default here. If you want to define a local interface using a combination of interface type and network address, create a network interface set that specifies that combination.



Note <All> is the only valid setting for UNIX, Solaris, or Linux platforms.

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 8-8](#) for details.



Caution

In order to distribute rules to the correct hosts, you must associate policies with groups and then Generate rules. See [page 5-16](#) for instructions.

**Note**

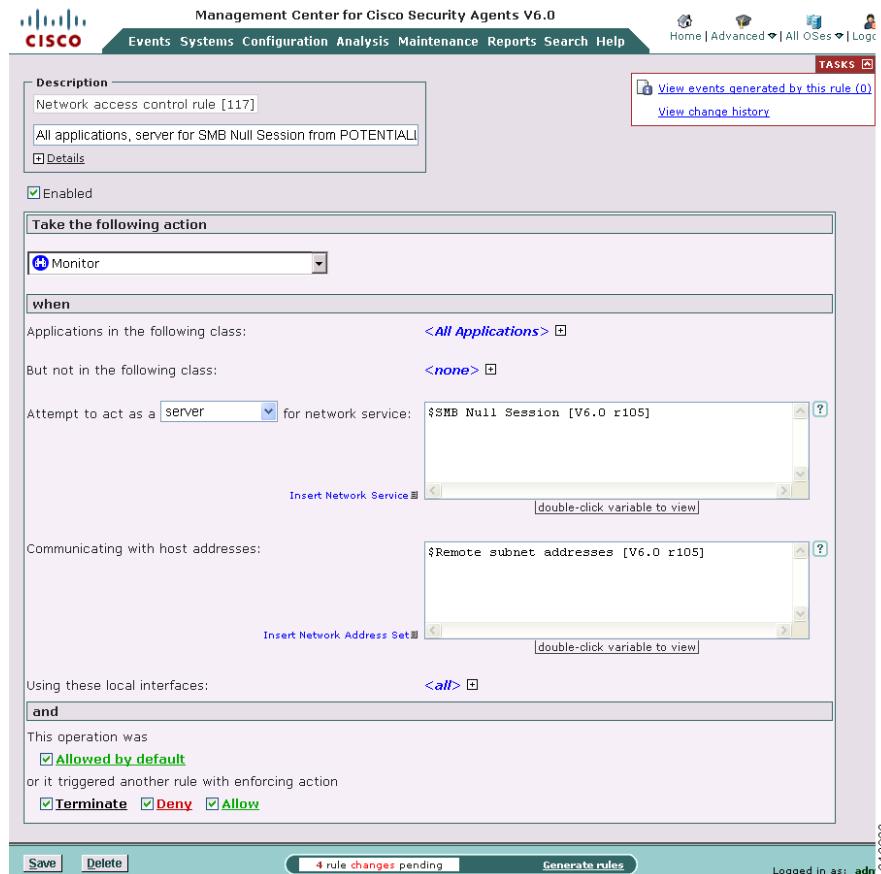
No network access control rule denial events are logged for any UDP port resulting from multicast packet signals. (If a collection of hosts have the same network access control rule and a broadcast such as UDP/138 were denied, then event messages would inundate CSA MC.)

**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 6-7 Network Access Control Rule

Network Shield Rule

The Network shield rule provides network protocol stack hardening capabilities.

**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.

**Note**

Network shield rules are not enforced for agents using IPv6 addresses.

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 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. Also see [Correlation, page 7-7](#) 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 5-18](#).

**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 5-22](#) 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.

- IPv6 packets on platforms without IPv6 support

Starting with CSA 6.0, CSA provides IPv6 support for Network access control rules on Solaris and Vista. We do not support IPv6 Network Access Control rules for Windows 2000, Windows XP, Windows 2003, and Linux platforms. Until these platforms do support IPv6 Network Access Control rules, this feature provides an administrator with a control to prevent end users from using IPv6.

If you configure this rule as a Deny, IPv6 traffic to Windows 2000, Windows XP, Windows 2003, and Linux platforms is dropped.

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.

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.

**Note**

This rule option is not available for UNIX policies as the UNIX OS already provides this protection.

**Note**

This rule option is not available for Windows Vista.

**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 7-7](#)), 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).

- TCP Chimney Offload

Disables the Microsoft TCP Chimney Offload feature if it is in use. This allows CSA to enforce the following network shield options.

- IP Security Checks
- Invalid TCP Header
- TCP blind session spoofing attempt
- Malicious packet



Note If you make any changes to the “TCP Chimney Offload” feature, these changes are not enforced until after the agent system(s) is rebooted.

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 - Type in a literal network address or a reference to a network address set variable (preceded by a dollar sign). See [Network Address Set Syntax Requirements, page 2-50](#) for a full description of proper IPv4 and IPv6 address syntax.

You can also click the **Insert Network Address Set** link to access a list of pre-configured network address sets. From the Insert Network Address Set link, click the **New** “shortcut” item to create a new network address set variable without leaving the rule page.

**Note**

IPv6 addresses can only be used by a rule associated with a Vista rule module.

**Note**

You can use the “short hand” symbol **@local** to indicate all local addresses on the agent system. Use **@remote** to indicate all address that are not on the local agent system. Refer to [Short hand notation for network address sets, page 2-52](#) for more information and additional shorthand symbols.

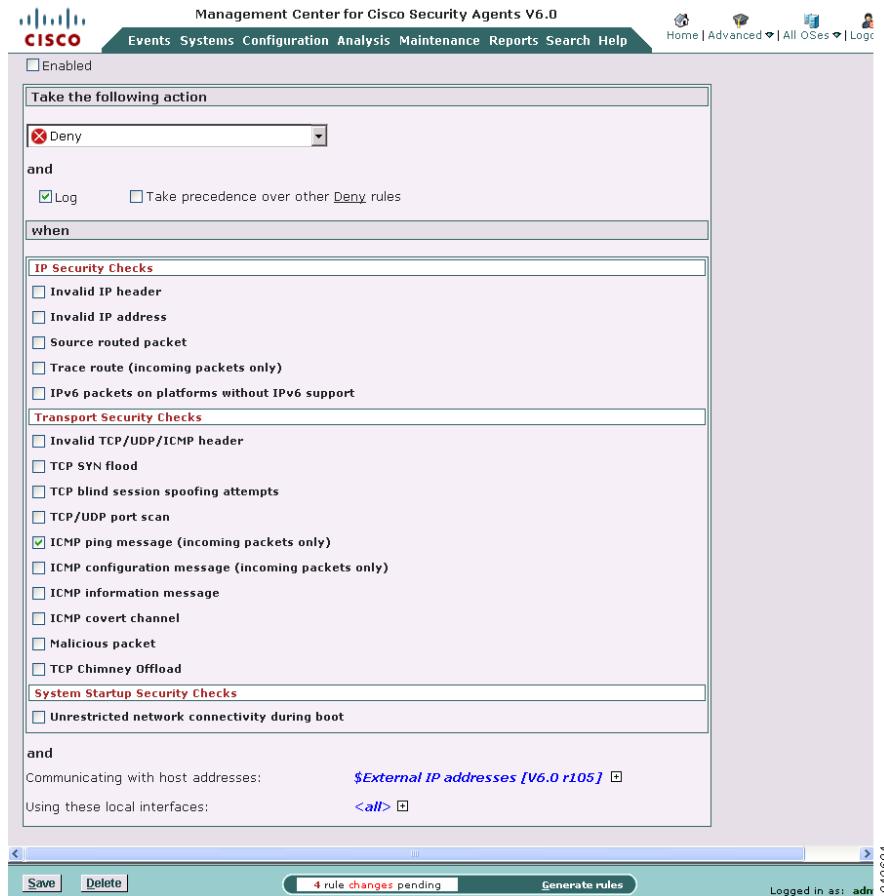
Step 6 Using these local interfaces

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. Note that you cannot enter a “literal” in this field. You must select a preconfigured variable from the Insert Network Interfaces Set link if you want to change the default here. If you want to define a local interface using a combination of interface type and network address, create a network interface set that specifies that combination.

**Note**

<All> is the only valid setting for UNIX, Solaris, or Linux platforms.

Step 7 Click Save when finished.

Figure 6-8 Network Shield Rule

Windows Only Rules

The following rules are only available for Windows Rule Modules.

Clipboard Access Control

Use the clipboard access control rule to configure permissions for which applications can access information that is written to the clipboard by other applications. When writing security policies, you may want to protect clipboard 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, only processes which match the second specified application classes are allowed to read that data from the clipboard.

**Note**

You should note that when you're writing clipboard rules for applications, if a process writes to the clipboard and then exits, the clipboard data written by that process becomes inaccessible to all applications. The initial process writing to the clipboard must not exit for the clipboard data to be accessible to other applications per the clipboard access control rule. This rule type is implemented in this way to prevent certain types of data loss from occurring.

One scenario in which you may want to use this rule is as follows. You could prevent applications from accessing clipboard data that is written by applications which are categorized as “sensitive data applications.”

These instructions are a continuation of [Configuring Rule Modules, page 5-4](#).

-
- Step 1** To add rules to your module, expand the rules area of the rule module and click the **Add** button. 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 6-9](#).
 - 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 **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 5-18](#).

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 5-22](#) 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 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. For example, if you only want a subset of applications in the selected application class to apply to this rule (i.e. dynamic or behavioral based tags that may get widely applied via a dynamic application class builder rules) you would use the But not field to select those application exclusions. Note that the entry <None> is selected by default.

Step 7 **attempt to read clipboard data written by:**

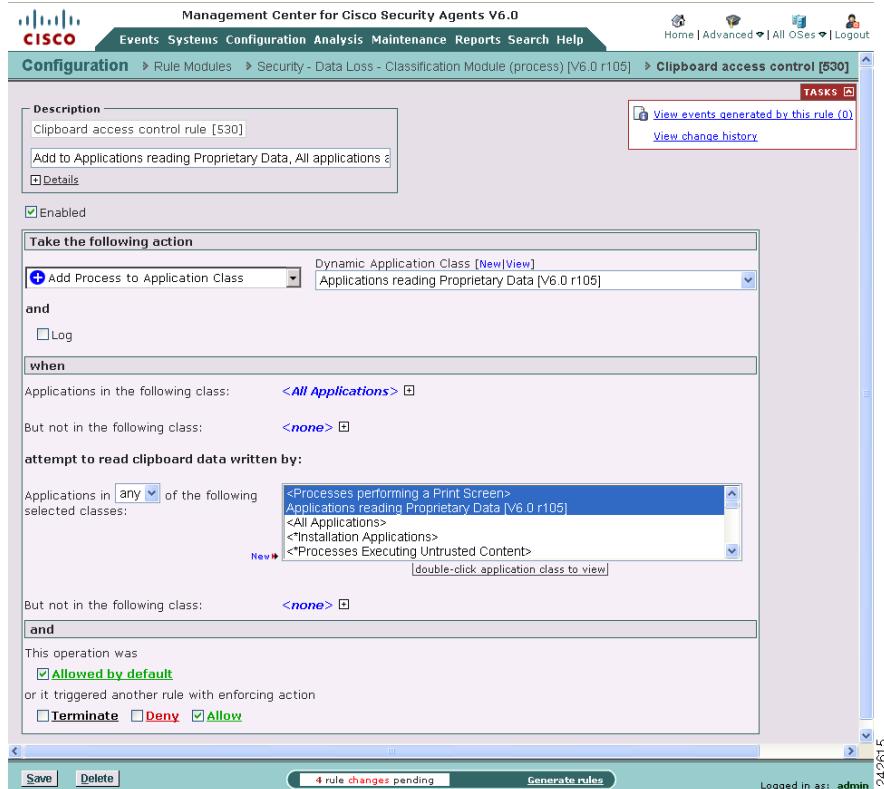
- **Applications in any of the following selected classes**—This second applications field indicates the application classes that you do not want to read clipboard data which has been written by selected applications above. If you selected “All Applications” in the top application field, you cannot select All Applications in this second field.
- **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 8 When you are finished configuring your Clipboard access control rule, click the **Save** button.



Note

There is a built-in application class that accessible to only the Clipboard access control rule. **Processes performing a Print Screen** is a pre-configured application class intended to identify processes performing screen captures. You could use this application class to include print screen applications in a rule preventing clipboard access of print screen data. Or you could require users to enter a justification for using the print screen option as part of a clipboard access rule with a notify action. (See [The Notify User Action, page 5-24](#) for more information.)

Figure 6-9 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 12-11](#) for information.

These instructions are a continuation of [Configuring Rule Modules, page 5-4](#).

-
- Step 1** To add rules to your module, expand the rules area of the rule module and click the **Add** button. 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 6-14](#)).
- 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 5-18](#).
- 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 5-22](#) 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 8, “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 12-11](#) for instructions.

PROGID’s, use the following syntax:

Outlook.Application

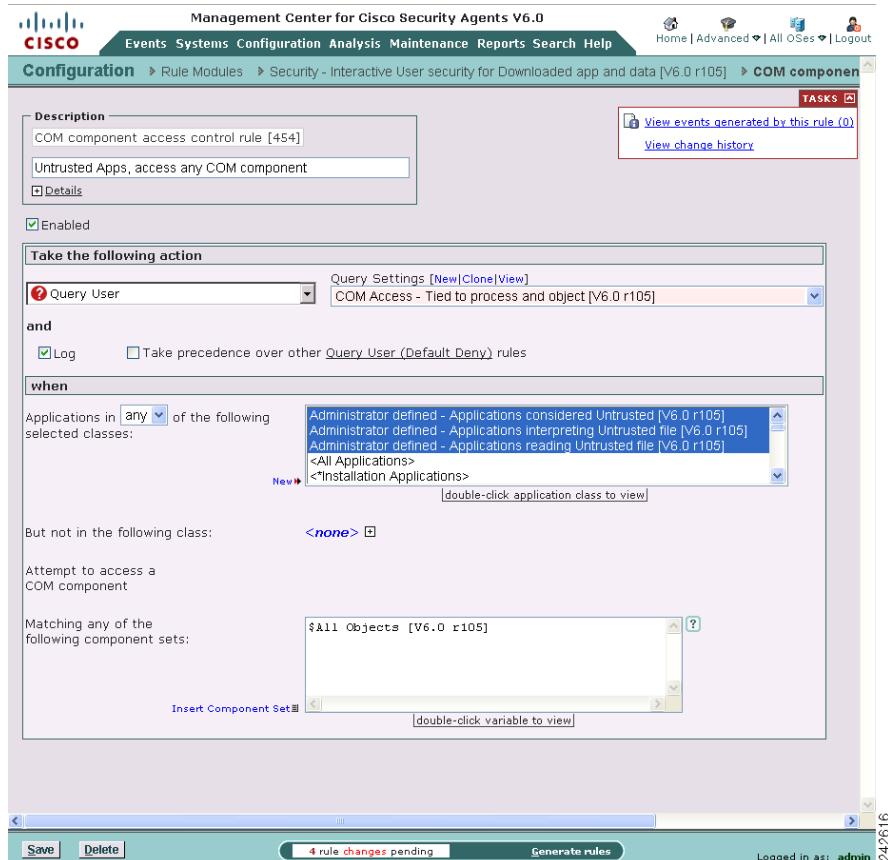
When entering CLSID’s (uppercase hexadecimals) using the following syntax, you must include the brackets shown here:

{000209FF-0000-0000-C000-000000000046}

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

Windows Only Rules

Figure 6-10 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 5-4](#).

Step 1

To add rules to your module, expand the rules area of the rule module and click the **Add** button. 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 5-18](#).

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 5-22](#) 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 file(s) 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 8, “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 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 8 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.



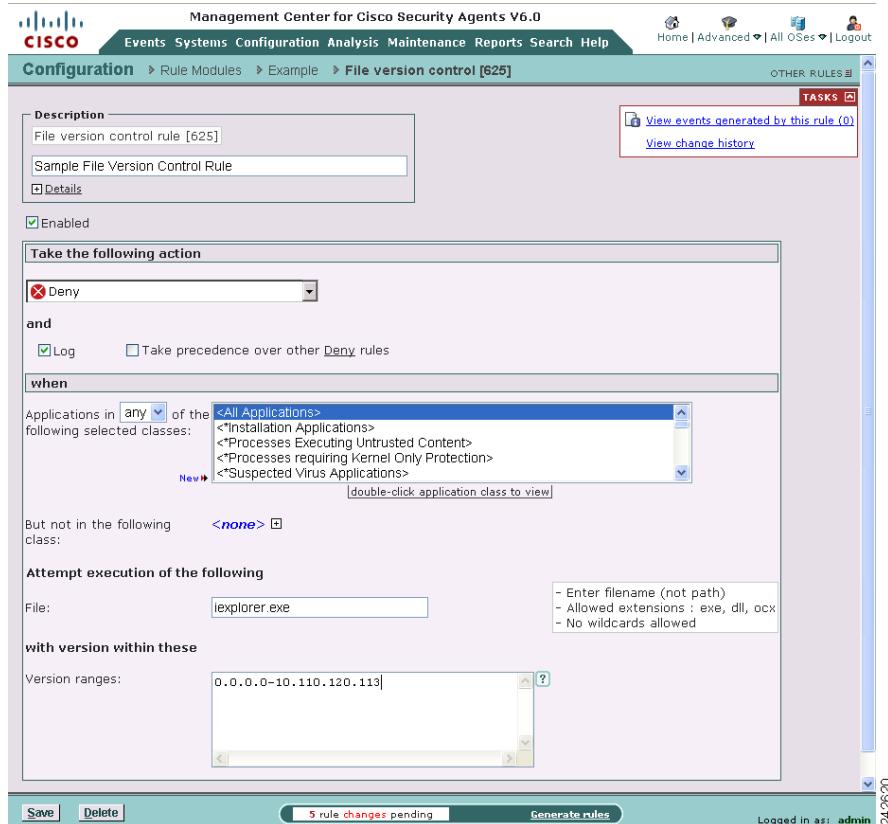
Note

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 9 Click the **Save** button when you are finished.

Windows Only Rules

Figure 6-11 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. This rule also detects if a system was booted in a non-standard, insecure manner.



Note These instructions are a continuation of [Configuring Rule Modules, page 5-4](#).

Step 1 To add rules to your module, expand the rules area of the rule module and click the **Add** button. 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 5-18](#). Note that 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 5-22](#) 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. Enter module data in the following edit fields:

- **Module hashes to be included**

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  
ae45e23b45093dfffa899\**  
ae45e23b45093dfffa899\*\*\uphcleanhlp.sys
```

- **Code patterns to be included**

By default, this field contains <all> . The wizard enters code patterns (not inside any module) into this field.

- **The previous detected boot was insecure**

When a system has previously booted in a non-standard manner, selecting this checkbox causes a message to be sent to the event log. A boot is considered standard if the system was booted from the primary hard disk. Any other boot type, for example, booting from a peripheral device (CD ROM) or a hard disk that is not the primary, is considered non-standard. A non-standard boot may be considered suspicious. (e.g., This is one way of circumventing the Cisco Security Agent and introducing a Trojan to a system.)

The insecure boot detection this checkbox enables works in conjunction with a particular type of compatible BIOS on compliant systems. The compatible BIOS detects a non-standard boot and on the next normal boot, if you have this checkbox selected, a message is sent to the MC which logs this insecure boot detection. (If a Host is running a BIOS that supports this insecure boot detection feature, the individual Host details page will indicate this. From the CSA MC menu bar, click Systems>Hosts. Then click on the link for an individual host. The Host Status section includes a category named “BIOS supported boot detection”.)



Note

A Safe Mode boot also falls into this insecure boot category since the Cisco Security Agent provides no security in Safe Mode. Compatible BIOS is *not* required for a Safe Mode boot detection.

- **Included boot patterns**

By default, this field contains <all> . You can use provided tokens here to only detect certain boot types as insecure or to exclude a particular boot type from the detection. Available tokens are:

@fixed - This indicates a fixed hard disk that is not the primary disk. (Compatible BIOS is required to detect this.)

@network - This indicates all network shares. (Compatible BIOS is required to detect this.)

@removable - This indicates all removable media. That includes, floppies, CDs, zip drives, etc. (Compatible BIOS is required to detect this.)

Windows Only Rules

@safemode - This indicates the detection of a system having booted in any debug mode in which the agent does not load. (Detecting this is not BIOS dependent.)

- Step 7** Click **Save** when finished.



Note

Certain types of keystroke loggers deploy kernel level drivers. When this is the case, the Kernel protection rule will catch this type of keystroke logger. Additionally, you should use the [System API Control Rule](#), page 6-71 to catch other types of keystroke loggers.

Figure 6-12 Kernel Protection Rule

The screenshot displays the 'Kernel protection [427]' configuration page in the Management Center. The 'Description' field contains 'Kernel protection rule [427]'. The 'Action' section is set to 'Deny' and includes an option to 'Log'. The 'When' condition is 'Modules load after system startup'. Under 'Included modules', there is a link to '\$Administrator defined - Black List files [V6.0 r105]'. There are also sections for 'Included module hashes' and 'Included code patterns', each with an 'all' button. A note at the bottom of the 'when' section states: 'Note: The edit fields in this rule section are maintained by the Event Management Wizard.' Below the main configuration area are buttons for 'Save', 'Delete', 'Generate rules', and status information ('5 rule changes pending'). The bottom right corner shows the user is logged in as 'admin' on '24/26/21'.

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 5-4](#).

Step 1 To add rules to your module, expand the rules area of the rule module and click the **Add** button. 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 6-13](#)).

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.

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.

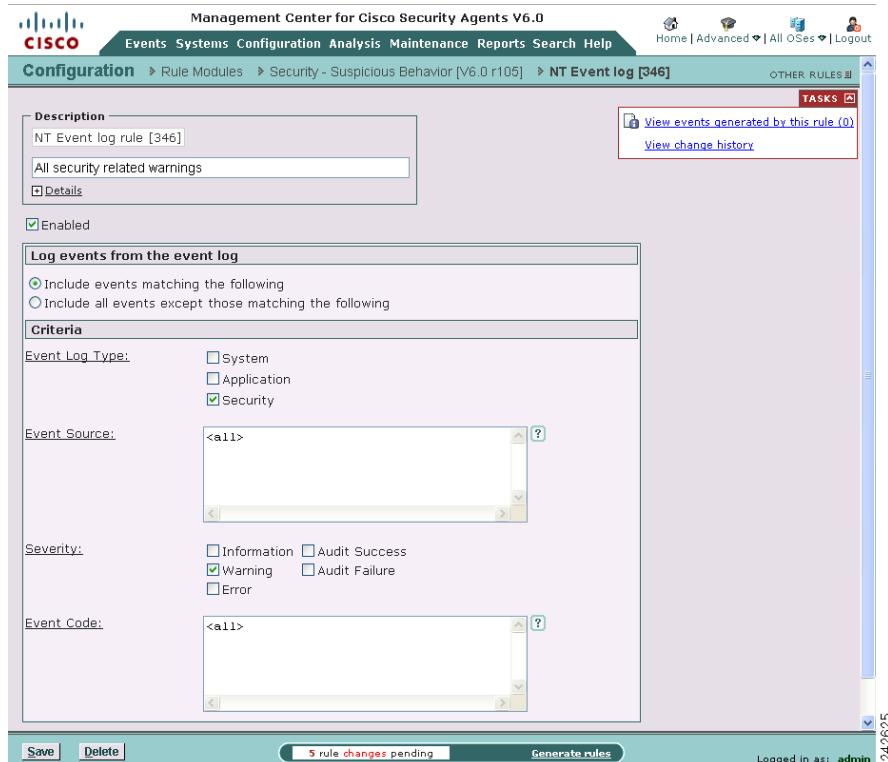
The event code is the number identifying the particular event type. For example, 6005 is the ID of the event that occurs when the Event log service is started. You can find the event IDs for Windows security events by searching for the following articles on the Microsoft web site: Q174074, Q299475, Q301677, and Q947226.

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.

Figure 6-13 NT Event Log Rule

Printer access control

Use this rule type to control which applications are allowed to send data to the printer. For example, you can use this rule to prevent applications categorized as “sensitive data applications” from printing.



Note These instructions are a continuation of [Configuring Rule Modules, page 5-4](#).

Step 1 To add rules to your module, expand the rules area of the rule module and click the **Add** button. A pop-up list of the available rule types appears.

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

Step 3 Enter the following information for this 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 **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 5-18](#).

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 5-22](#) 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 file(s) 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.

- **But not in any of the following 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.

Attempt to print.

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 5-4](#).

-
- Step 1** To add rules to your module, expand the rules area of the rule module and click the **Add** button. 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 5-18](#).
- 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 5-22](#) 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 8, “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 9-38](#) for details on included operating system registry values.

**Note**

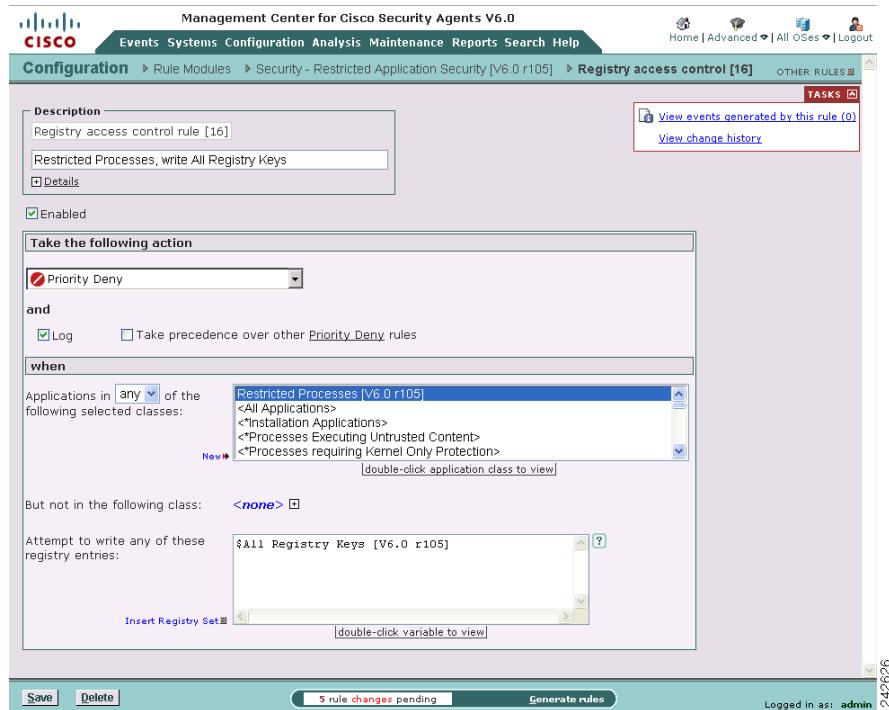
You cannot enter registry literals here. You must create a registry set variable if you are not using pre-configured registry sets.

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 5-16](#) for instructions.

Figure 6-14 Registry Access Control Rule

Scan Event Log

Generally, think of a scan event log rule as taking an action if these conditions have been met:

1. An application has performed some action that triggered a virus scan or data scan; for example, an application has opened or closed a file.
2. As a result of the virus or data scan, a file was tagged and is represented by the file set that you specify.
3. As a result of gaining a data tag or virus tag, the application's action that triggered the scan was allowed or denied.

The scan event log rule then takes action. Here are some of the actions that the scan event log rule could take and an example of how that action could be used. There are many other uses for the actions listed here.

- A **Monitoring** action will send an event to the CSA MC. You could use a monitor to ensure that there is an event to include in a report.
- A **Notify User** action sends a message to users. The message could be used to inform users that they are working with sensitive data. It may also be used to require them to justify their actions.
- A **Set** action could be used to delete a file infected with a virus.
- The **Add or Remove an Application from an Application Class** action could be used to identify an application that has read proprietary information.



Note

These instructions are a continuation of [Configuring Rule Modules, page 5-4](#).

Step 1 To add rules to your module, expand the rules area of the rule module and click the **Add** button. A pop-up list of the available rule types appears.

Step 2 Select the **Scan Event Log 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 5-18](#) and [Rules: Action Definitions, page 5-19](#).

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 5-22](#) for details.

Step 6 When —

- **Applications in any (or all) of the following selected classes**

Select one or more application classes here to indicate the application(s) that perform some action that causes a data scan or antivirus scan.

If you choose **Applications in any of the following selected classes** the rule will affect an application that is a member of one of the selected application classes.

If you choose **Applications in all of the following selected classes**, the rule will affect an application that is a member of every application class you select.

Note that the entry, <All Applications>, is selected by default. You can use this default or you can create your own application classes by clicking the blue **New** link next to the application class box. For application class configuration details, see [Chapter 8, “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. You may also create a new application class by clicking the blue **New** link next to the application class list box.



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

Step 7 **Perform an operation causing a Data Scan or Virus Scan.** You can select either the Data Scan or Virus Scan checkbox, or both Data and Virus scan checkboxes for this rule.

Step 8 Where the scan results match any of these file sets:

As a result of the virus or data scan, a file was tagged and represented by the file set that you specify here.

Click the **Insert File Set** link to specify one or more pre-configured file sets from the menu that appears. You can also click the blue **New** link, in the Insert File Set list box, in order to create a new File set for this rule.

The file sets you select or create should specify a particular data scanning tag or virus scanning tag, or specify <all> tags in the Content Matching field of the file set.

Step 9 And —

In this area, specify the enforcement action CSA took on the operation that triggered the data scan or virus scan.

Indicating **Allow by default** or **Allow if triggered by a rule** indicates that CSA allowed the operation that triggered the scan. Indicating **Terminated** or **Denied by rule** indicates that CSA prevented the operation that caused the scan.



Note Though the action that triggered the scan could have been allowed or denied, the scan itself is performed.

Step 10 When you are finished configuring your scan event log rule, click the **Save** button. This rule is now part of your new rule module.

In order to distribute rules to the correct hosts, you must associate the rule module with a policy, associate the policy with a group, and then Generate rules. See [page 5-16](#) for instructions.

Service Restart Rule

Use the Service restart rule to have the agent restart Windows 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 5-4](#).

**Note**

System Restart rules ignore system states. They are triggered regardless of system state or change in system state.

Step 1 To add rules to your module, expand the rules area of the rule module and click the **Add** button. 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 6-15](#)).

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 Vista, Windows XP, Windows 2003 and 2000:
Start>Settings>Control Panel>Administrative Tools>Services “Name” 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 service specified in this rule.

Step 6 Click **Save** when finished.**Note**

The Service Restart rule is different from the Windows configurable restart service. Windows only restarts processes that have gone away. The agent restarts a process that experiences a failure of any kind.

Figure 6-15 Service Restart Rule

The screenshot shows the Management Center for Cisco Security Agents V6.0 interface. The top navigation bar includes links for Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, Help, Home, Advanced, All OSes, and Logout. The main window title is "Configuration > Rule Modules > Sample - Web Server - Security Module [V6.0 r105] > Service restart [277]". The left sidebar has a "TASKS" section with "View events generated by this rule (0)" and "View change history". The main configuration area has a "Description" field containing "Service restart rule [277]" and "World Wide Web Publishing Service (HTTP) - Windows XP". Below this, there are checkboxes for "Enabled" (unchecked) and "Log" (checked). The "Restart" section contains a field "The following service :" with "World Wide Web Publishing" selected. The "when" section contains two checked checkboxes: "Not responding to Service Control Manager" and "Not responding to network requests for service :" with "HTTP" selected. At the bottom, there are "Save" and "Delete" buttons, a status message "5 rule changes pending", and a "Generate rules" button. The bottom right corner shows the user is logged in as "admin" with ID "242629".

Sniffer and Protocol Detection

**Note**

Sniffer and protocol detection is not supported for agents running on Windows Vista systems.

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 5-4](#).

Step 1

To add rules to your module, expand the rules area of the rule module and click the **Add** button. 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 6-14](#)).

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.

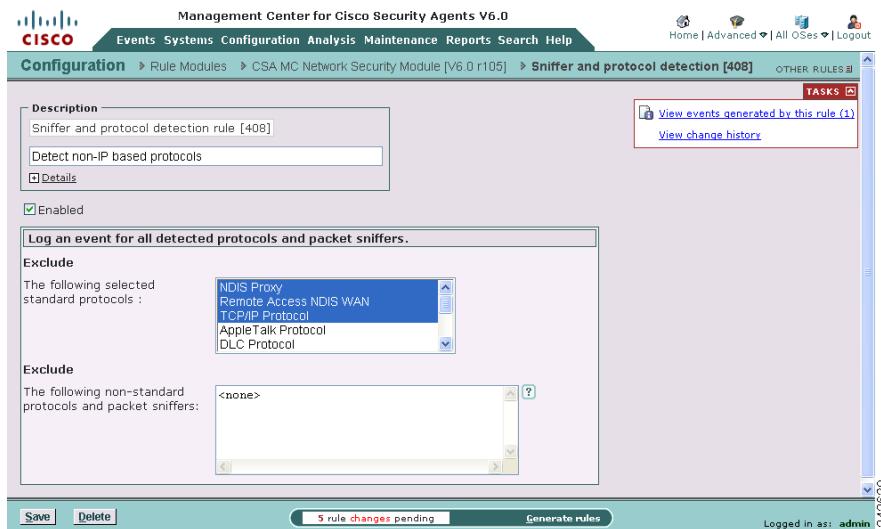
This is also where you should enter any packet sniffer programs you want to exclude from this rule. (Find the names for these programs in Cisco Security Agent log files or in system registries.) For example, enter:

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 6-16 Sniffer and Protocol Detection Rule

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. See [Figure 6-17](#).



This rule type is not available for UNIX policies. Refer to the Buffer overflow rule information on [page 6-78](#) 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. See [Service Restart Rule, page 6-67](#) for more information.

These instructions are a continuation of [Configuring Rule Modules, page 5-4](#).

To configure a System API rule, do the following:

-
- Step 1** Log in to the CSA MC as an administrator with configure privileges and switch to advanced mode.
- Step 2** Open the rule module to which you want to add this System API rule.
- Step 3** To add rules to your module, expand the rules area of the rule module and click the **Add** button. A pop-up list of the available rule types appears.
- Step 4** Select the **System API** rule. This takes you to the configuration view for this rule type.
- Step 5** 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 6** **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 5-18](#).
- Step 7** 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 5-22](#) for details.
- Step 8** **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 8, “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.

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.

Note that the entry <None> is selected by default

targeting (where applicable)

The “targeting” application class selections are only applicable to following checkbox items on this page: *Inject code into other applications*; *Write memory owned by other applications*. A targeting option is available for these items because these actions (injecting code and writing memory) involve two or more parties. These parties include the one that is initiating the action and the process(es) being affected. Providing an optional targeting selection in these cases for choosing particular application classes allows for further configuration granularity.

- Step 9** In the **Attempt the following operations** area, select the checkbox next to action you want to regulate.

System Information Checks

- Access local configuration information
Detect applications that attempt to read system registry settings.
- Access Security Account Manager
Detect applications that attempt to steal local system passwords.

System Monitoring Checks

- Trap keystrokes
Detect applications that attempt to capture system keystrokes.

See [Kernel Protection, page 6-53](#) for additional information.

- 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 for parallel port media devices on any operating system.



Note

A System API Control rule that allows or denies applications from monitoring media devices is supported for Windows Vista. The Vista operating system passes all audio device access through one process: `audiodg.exe`. Therefore, any System API Control rule, written to control media device access becomes a blanket allow or a blanket deny for all audio processes because CSA is only able to enforce the rule on “`audiodg.exe`.”

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.

Additionally, you can use this Access system functions checkbox in combination with a “Set - Data Payload” action type to generate signatures to catch buffer overflow based attacks.

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.

Additionally, you can use this Handle exceptions checkbox in combination with a “Set - Data Payload” action type to catch MSRPC or LPC attacks and generating a signature from that attack type.

Patterns to be included: Use the Wizard from the Event log message in question to create an exception to exclude a particular pattern in a System API “allow” rule when you are seeing exception handling events that you think are benign. Entering patterns here for exclusion will prevent CSA MC from logging further messages for this pattern.

- 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.

Step 10 Click **Save**.



Tip

There is a red **Tasks menu** in the upper right corner of the page. Clicking the down arrow, expands the menu. This menu provides quick links to common tasks that are relevant to the item being configured.

Figure 6-17 System API Control Rule

The screenshot shows the Management Center for Cisco Security Agents V6.0 interface. The title bar reads "Management Center for Cisco Security Agents V6.0". The main menu includes Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, Help, Home, Advanced, All OSes, and Logon.

The current view is under Configuration > Rule Modules > Security - Suspicious Behavior [V6.0 r105] > System API control [345].

Description: System API control rule [345]
Active Network, First Time Applications (not White List), Inject code into other applications

Enabled:

Take the following action: Monitor

when: Applications in any of the following selected classes:
 <First Time Application Execute>
 Active Network Applications [V6.0 r105]
 <All Applications>
 <Installation Applications>
 <Processes Executing Untrusted Content>
New > double-click application class to view

But not in the following class:
 Administrator defined - White List Applications [V6.0 r105]

targeting (where applicable):
Applications in the following <All Applications> class:
But not in the following <none> class:

attempt the following operations:

- System Information Checks:**
 Access local configuration information
 Access Security Account Manager
- System Monitoring Checks:**
 Monitor media devices
Included patterns: <all>
 Trap keystrokes
- System Modification Checks:**
 Access physical memory
 Download and invoke ActiveX controls
 Inject code into other applications
 Write memory owned by other applications
- Atypical System Behavior Checks:**
 Access system functions from code executing in data or stack space
Included patterns: <all>
 Handle exceptions
Included patterns: <all>
 Invoke unusual system calls
Included patterns: <all>

and:
This operation was
 Allowed by default
or it triggered another rule with enforcing action
 Terminate Deny Allow

32

UNIX Only Rules

The following rules are only available for UNIX Rule Modules.

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 module, expand the rules area of the rule module and click the **Add** button. 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 6-18).
- 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 5-18](#). (Note that 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 5-22](#) 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 8, “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 8-7](#) for details. This checkbox monitors the execution of instructions from stack memory. This only provides logging.

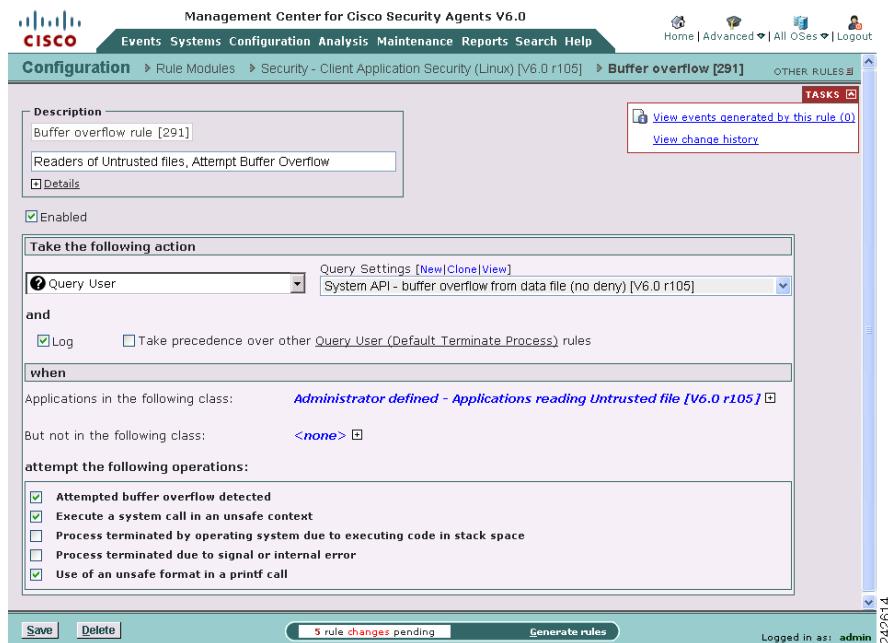
- Process terminated due to signal or internal error

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.

Figure 6-18 Buffer Overflow Rule

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 5-4](#).

-
- Step 1** To add rules to your module, expand the rules area of the rule module and click the **Add** button. 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 6-19](#)).

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 5-18](#).

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 5-22](#) 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 8, “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

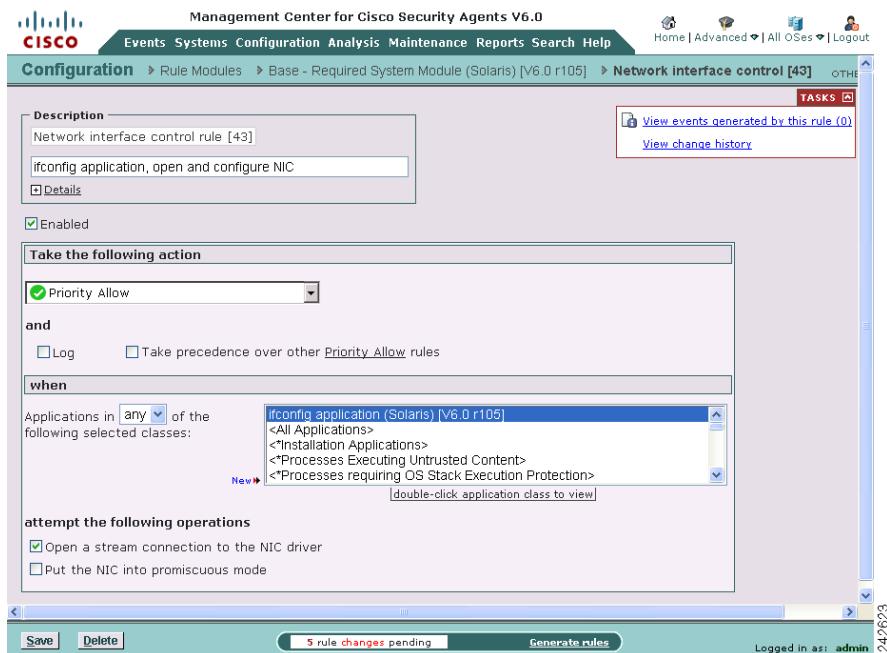
**Note**

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 6-19 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 5-4](#).

Step 1 To add rules to your module, expand the rules area of the rule module and click the **Add** button. 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 6-21](#)).

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.

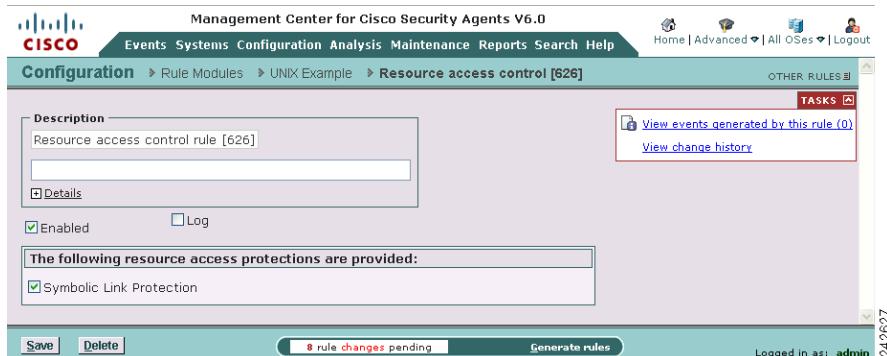
Step 4 Select the **Symbolic Link Protection** checkbox to turn on that functionality.

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 6-20 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 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 5-4](#).

Step 1 To add rules to your module, expand the rules area of the rule module and click the **Add** button. 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 6-21](#)).

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 5-18](#).

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 5-22](#) 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 8, “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.

- **The previous detected boot was insecure**

When a system has previously booted in a non-standard manner, selecting this checkbox causes a message to be sent to the event log. A boot is considered standard if the system was booted from the primary hard disk. Any other boot type, for example, booting from a peripheral device (CD ROM) or a hard disk that is not the primary, is considered non-standard. A non-standard boot may be considered suspicious. (e.g., This is one way of circumventing the Cisco Security Agent and introducing a Trojan to a system.)

The insecure boot detection this checkbox enables works in conjunction with a particular type of compatible BIOS on compliant systems. The compatible BIOS detects a non-standard boot and on the next normal boot, if you have this checkbox selected, a message is sent to the MC which logs this insecure boot detection. (If a Host is running a BIOS that supports this insecure boot detection feature, the individual Host details page will indicate this. From the CSA MC menu bar, click Systems>Hosts. Then click on the link for an individual host. The Host Status section includes a category named “BIOS supported boot detection”.)

– Included boot patterns

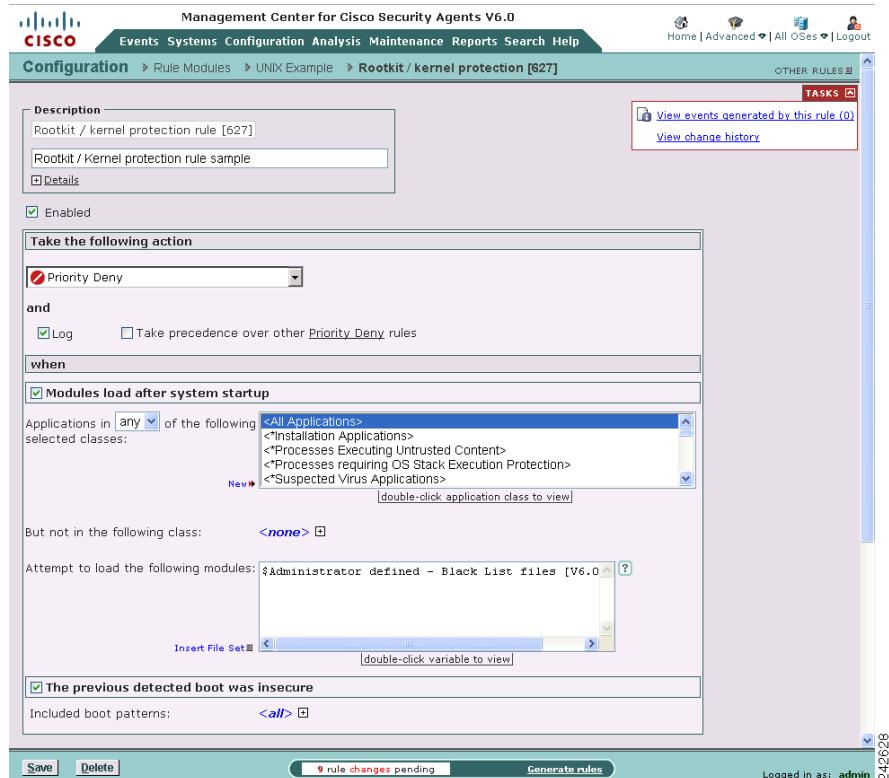
By default, this field contains <all>. You can use provided tokens here to only detect certain boot types as insecure or to exclude a particular boot type from the detection. Available tokens are:

@fixed - This indicates a fixed hard disk that is not the primary disk. (Compatible BIOS is required to detect this.)

@network - This indicates all network shares. (Compatible BIOS is required to detect this.)

@removable - This indicates all removable media. That includes, floppies, CDs, zip drives, etc. (Compatible BIOS is required to detect this.)

Step 8 Click the **Save** button.

Figure 6-21 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 5-4](#).

Step 1 To add rules to your module, expand the rules area of the rule module and click the **Add** button. 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 6-22](#)).

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.

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 or 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
eth0
```

To get every message of category “warning” from the /sbin/dhcpagent daemon, you would configure your syslog rule in the following manner (See [Figure 6-22](#)):

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 6-22 Syslog Control Rule

The screenshot shows the 'Configuration' section of the Management Center for Cisco Security Agents V6.0. The title bar includes the Cisco logo and the URL 'Events Systems Configuration Analysis Maintenance Reports Search Help'. The main menu shows 'Configuration' selected. The page title is 'Syslog control [556]'. A red box highlights the 'Log events from Syslog' section.

Description: Syslog control rule [556]
Super User password failures

Criteria

- Event Source:** su
- Facility:** auth, cron, daemon, kern, local0
- Priority:** Debug, Warning, Information, Error, Notice, Alert and above
- Message Pattern:** **authentication failure**user=root**

TASKS

- View events generated by this rule (0)
- View change history

Buttons at the bottom: Save, Delete, 9 rule changes pending, Generate rules, Logged in as: admin, 24263!

■ UNIX Only Rules



CHAPTER 7

Using Global Settings

Overview

Management Center for Cisco Security Agents provides configuration tools from the Global Settings section that are used to categorize and apply tags to processes, files, and IP addresses and to correlate events across multiple systems. When tags are applied and certain correlation rules are triggered, 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 based on noticing the action taking place on a small number of systems. The Cisco Security Agent also scans agent systems for applied tags and can apply rules informing users of data loss possibilities on that basis. This chapter contains these sections:

- [Application Trust Levels, page 7-2](#)
 - [Setting Application Trust Levels, page 7-2](#)
 - [Using the Event Management Wizard to Set Trust Levels, page 7-3](#)
 - [Identifying Members of the White List, Grey List, and Black List, page 7-4](#)
- [Scanning Data Tags, page 7-15](#)
- [AntiVirus Exemptions, page 7-5](#)
- [Event Correlation, page 7-7](#)
- [Signature Settings, page 7-13](#)
- [Scanning Data Tags, page 7-15](#)

- Static Data Tags, page 7-15
- Report Configuration, page 7-16

Application Trust Levels

Application trust levels refer to an application's placement on a "White List," "Grey List," or "Black List." After an application is placed on one of these lists, there are different rules provided in this release that permit or restrict the application from acting.

Applications in the White List are generally trusted and allowed to run, however, they are continuously monitored and if they commit a severe violation, they are immediately restricted.

Applications in the Black List are not trusted and are prevented from running. If they are running, they are terminated. If a user needs to use a black-listed application, then the application must be added to the white list. In such a case, it is recommended that the user adds rules that restrict the application to the minimum set of privileges required.

Applications are placed on the white list, grey list, or black list in one of these ways:

- Administrators place the applications on a list by using the global **Application Trust Levels** page.
- Some members of a list are static. We have already classified some applications and placed them on one of these lists.

You do not need to ensure that every application on a host is placed on one of these lists.

Setting Application Trust Levels

CSA MC Administrators can add files to the White List, Grey List, and Black List through the global Application Trust Level page.

Step 1 Log on to the CSA MC as a user with configure privileges. This procedure can be performed by users in Advanced Mode or Simple Mode.

Step 2 From the **Configuration** menu, navigate **Global Settings > Application Trust Levels**.

Step 3 On the global **Application Trust Levels** page, click **New**.

Step 4 In the **File Name** field, provide the path and filename for the application you are listing. You can use wildcards (**) to generalize the location of the file. For example:

C:\Program Files\Cisco\CSAgent\bin***

Indicates every file in every subdirectory of C:\Program Files\Cisco\CSAgent\bin.

\Program Files\Cisco\CSAgent\bin*

Indicates every file in every subdirectory of CSAgent\bin no matter what drive it is installed on.

See [Using the Correct Syntax, page 2-41](#) for more information about how to properly use wildcards.

Step 5 In the **Trust Level** field, select **White List**, **Grey List**, or **Black List** from the pull-down menu.

Step 6 In the **OS** field, specify the type of operating system this trust specification applies to. Windows indicates any supported Windows platform. UNIX indicates any supported UNIX or Linux platform.

Step 7 In the **Justification** field, explain why you are creating setting the trust for the application.

Step 8 Click **Save**. The new trust level designation is displayed on the **Application Trust Level** page.

Step 9 Generate rules when you are ready to deploy this configuration to hosts.

Using the Event Management Wizard to Set Trust Levels

Step 1 Log on to the CSA MC as a user with configure privileges. This procedure can be performed by users in Advanced Mode or Simple Mode.

Step 2 From the **Events** menu, select **Event Log**.

Step 3 Find the event which identifies the process for which you want to set a trust level.

Step 4 Click the **Wizard** link.

- Step 5** In the **Classify Application** area, note that the **Application that triggered this event** field is already populated with the directory path and file name of the application.
- Step 6** In the Action field, select **I trust this application**, **I am not sure I trust this application**, or **I do not trust this application**. These choices place the application on the White List, Grey List, or Black List, respectively.
- Step 7** In the **Justification** field, explain why you are creating setting the trust for the application.
- Step 8** Click **Finish**. The new trust level designation is displayed on the **Application Trust Level** page.
- Step 9** Generate rules when you are ready to deploy this configuration item.

Identifying Members of the White List, Grey List, and Black List

Applications are assigned to the White List, Grey List, and Black List; they are not added dynamically if a rule triggers.

The White List, Grey List, and Black List are defined by the contents of these application classes: **Administrator defined - White List Applications**, **Administrator defined - Grey List Applications**, and **Administrator defined - Black List Applications**.

Each application class is made up of file sets and has at least one file set that references its own list's token, such as @whitelist, @greylist, and @blacklist. For example, the **Administrator defined - White List Applications** application class contains the **Administrator defined - White List files** file set. One component of this file set is defined as any file associated with the @whitelist token. The @whitelist token is defined as any file on the global **Application Trust Level** page that is described as being on the white list. The Grey List and Black List applications are defined in similar ways.

In order to identify which applications are part of which trust level list, you need to look in two places: in the application class for the trust level and on the Application Trust Level page.

To view the contents of an application class, follow this procedure:

-
- Step 1** Log on to the CSA MC as any user type and switch to **Advanced Mode**.

- Step 2** From the **Configuration** menu, navigate **Applications > Application Classes** and search for the **Administrator defined - White List Applications**, **Administrator defined - Grey List Applications**, or **Administrator defined - Black List Applications** application classes.
- Step 3** Click the link for the application class. The applications that define this class are listed in the file sets listed in the **when created from one of the following executables** file sets.
- Step 4** Double click a file set to view the applications that belong to it.

To view the applications administrators have assigned to trust lists, follow this procedure:

-
- Step 1** Log on to the CSA MC as a user with any level of privileges and view the CSA MC interface in either Advanced Mode or Simple Mode.
- Step 2** From the **Configuration** menu, navigate **Global settings > Application Trust Level**. Applications' memberships in trust level lists are clearly identified on the Application Trust Level page.

AntiVirus Exemptions

AntiVirus exemptions can be created for signature-based AntiVirus tags that you have determined to be false positives. Creating an exemption for a tag prevents any files, that have been given the tag, from being restricted by AntiVirus rules that pertain to that tag. Creating an exemption for an individual file, with a particular AntiVirus tag, prevents that file from being restricted by AntiVirus rules that pertain to that tag.

You can create an exception for a virus tag through the **Event Management Wizard** or through the **AntiVirus Exemptions** page. See [Creating AntiVirus Exemptions Using the Event Management Wizard, page 15-14](#) and [Creating AntiVirus Exemptions Using the Global AntiVirus Exemptions Page, page 15-15](#) for these procedures.

Here is an example of how an end-user and a CSA MC administrator would be affected by an AntiVirus exemption: Assume that files have been quarantined on various hosts because they have been tagged with an AntiVirus tag. The CSA MC administrator determines that the tag represents a false positive and then creates

an exemption for that tag either using the wizard or by hand. The exemption is then listed on the AntiVirus Exemptions page on the CSA MC. When the administrator is ready, he or she generates rules.

The next time the host's CSA polls in to the CSA MC, it receives the AntiVirus exemption information. Within the next minute, any files with that AntiVirus tag that have already been quarantined are removed from the Quarantined files tab of the agent. The files are not put in the Restored tab. The AntiVirus exemption is global and individual users are not given the opportunity to re-classify the file as Quarantined.

To open the AntiVirus Exemptions list page, mouse-over the **Configuration** menu on the CSA MC and navigate **Global Settings > AntiVirus Exemptions**. The list page provides these columns of information to describe an AntiVirus exemption:

- **Virus:** This is the name of the virus as reported in an event or as determined by the Event Management Wizard. It is also the AntiVirus tag name for the virus. The name of the AntiVirus tag specified in the AntiVirus Exemptions page must match the tag attached to a file exactly in order for the file to be exempted from AntiVirus rule restrictions.
- **Target:** This indicates <All files> if the AntiVirus tag has been exempted, and therefore any file with the tag will be exempted from AntiVirus rule restrictions that pertain to that tag. The Target may also indicate a path to a particular file in order to exempt only that file from AntiVirus rule restrictions. Two wildcards (**) may be specified at the beginning of the directory path to generalize where this file might be found. For example:

**\Documents and Settings\Administrator\Desktop\Temp\virus.doc indicates the virus.doc file on Administrator's desktop.

**\Desktop\Temp\virus.doc indicates virus.doc on any desktop.

- **Justification:** The field displays the explanation the Administrator provided for creating the exemption.
- **Creation time:** Indicates the time the exemption was made.
- **Source:** Indicates the user name that created the exemption and if the exemption was created using the wizard.
- **OS:** Indicates the operating system for which the exemption pertains.

Event Correlation

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 **Global Event Correlation** page, accessible from the menu bar as follows **Configuration>Global Settings>Global Event Correlation** (see [Figure 7-1](#)), 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 8-7](#)) 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 6-23](#) 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 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 6-23](#) 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 6-57](#) 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 the “Set” action is used in a rule to mark a host address as Untrusted (globally) (see [Using the Set Action, page 5-25](#)) 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 6-23](#) 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 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 where they are available in rules 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 7-2](#). 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 7-3](#). 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 3-4](#) for poll hint details.

Confidence Ratings

When you click the Manage dynamically quarantined files and IP addresses links, items that are not added manually by the administrator, but are added automatically through event correlation will have a “high” or a “low” confidence rating. This rating indicates the “danger” likelihood of the item that has been quarantined. This rating is based on the detected file type and the network protocol involved.

**Note**

The events to quarantine a specific file or address are subject to event suppression like other components on the system. Duplicate correlation events are suppressed for one hour. This means that a given object can be quarantined, at most, once an hour.

Figure 7-1 Global Event Correlation Page

Management Center for Cisco Security Agents V6.0 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address https://w2k3-std-rsp2/csmc60/websm

Management Center for Cisco Security Agents V6.0

CISCO Events Systems Configuration Analysis Maintenance Reports Search Help

Home | Advanced | All OSes | Logout

Configuration > Global Settings > Event Correlation

Warning: At least one of the system count parameters is greater than the number of active hosts (2). Please adjust the parameter to a lower value if you wish to see correlation events.

Correlate network scans [Events : none]
Log a message if 5 systems report this event within 60 minutes

Correlate events received from operating system event logs and generate a summary event [Events : none]
 Log individual events in addition to summary event
Log a message if 2 systems report this event within 30 minutes

Correlate suspected virus application events and add contaminated files to list of [dynamically quarantined files](#) [Events : none]
Log a message if 2 systems report this event within 60 minutes

Correlate events received from virus scanners and add contaminated files to list of [dynamically quarantined files](#) [Events : none]
Log a message if 2 systems report this event within 60 minutes

Correlate communications with untrusted hosts and add peer addresses to list of [dynamically quarantined IP addresses](#) [Events : none]
Log a message if 5 systems report this event within 60 minutes

Save 4 rule changes pending Generate rules Logged in as: admin 24/6/07

Management Center for Cisco Security Agents V6.0

Trusted sites

Event Correlation**Figure 7-2 Quarantine Files Window**

<input type="checkbox"/> File Name	Quarantine Time	Source	Events
<input type="checkbox"/> bo.exe	2004-10-11 14:45:48	global correlation of a suspected virus (low fidelity)	view
<input type="checkbox"/> iloveyou.vbs	2004-10-11 14:40:32	entered by administrator	

191543

Figure 7-3 Quarantine IP Addresses Window

<input type="checkbox"/> IP Address	Quarantine Time	Source	Events
<input type="checkbox"/> 10.172.196.1	2008-06-12 15:18:54	entered by administrator admin	

242807

Signature Settings

The **Signature Settings** page is accessible from the CSA MC menu bar by navigating **Configuration>Global Settings>Signature Settings**. You can use this page to set the values for global and local signature correlation, thresholds to prevent denial of service attacks, globally enable new signatures and other managerial tasks related to signature correlation. The following sections are currently included in the Global Signature Settings page:

- **Common** - This section contains common signature settings. This includes an expiration time for global and local signatures and a check box to control whether new global signatures are immediately distributed to all agents. The default setting is that the **Enable new signatures** check box is not selected and signatures expire in 30 days.

When the **Enable new signatures** check box is not selected, signatures are automatically generated after the MSRPC or LPC correlation thresholds are met but they are not automatically distributed to agents. You must individually enable signatures in the **Manage global signatures** page when the **Enable new signatures** checkbox is not selected.

If the **Enable new signatures** checkbox is selected, signatures are automatically generated after the MSRPC or LPC correlation thresholds are met and the signatures are distributed to all hosts when they next poll in.



Note If you want new signatures enabled automatically, select the **Enable new signatures** checkbox and generate rules on the CSA MC.

- **MSRPC** - The **Correlate untrusted MSRPC payloads received by Cisco Security Agent systems** checkbox, turns on untrusted MSRPC payload signature generation. The checkbox is selected by default. The next section determines how many agents within a specific time frame, with similar events for receiving untrusted MSRPC payloads, are required to trigger a global signature correlation. The default is two systems reporting two similar MSRPC payloads within 1440 minutes (24 hours).

The next section for MSRPC signature generation deals only with local payloads associated with Denial of Service (DoS) attacks. Administrators define DoS attacks as a specified number of attacks on an interface, over a specified period of time, without a signature being correlated. Once that

threshold is met, future payloads attacking the interface are associated with the @highrisk_signatures token. After a configurable amount of time, the payloads are no longer associated with the @highrisk_signatures token.

By default, an interface is considered receiving a DoS attack if ten payloads are received within 30 minutes and a signature could not be created for the attack; after 60 minutes, the payloads are disassociated with the @highrisk_signatures token.

- **LPC** - The **Correlate untrusted LPC payloads received by Cisco Security Agent systems** checkbox, turns on untrusted LPC payload signature generation. The checkbox is selected by default. The next section determines how many agents within a specific time frame, with similar events for receiving untrusted LPC payloads, are required to trigger a global signature correlation for all agents. The default is two systems reporting two similar LPC payloads within 1440 minutes (24 hours).

The next section for LPC signature generation deals only with local payloads associated with Denial of Service (DoS) attacks. Administrators define DoS attacks as a specified number of attacks on an interface, over a specified period of time, without a signature being correlated. Once that threshold is met, future payloads attacking the interface are associated with the @highrisk_signatures token. After a configurable amount of time, the payloads are no longer associated with the @highrisk_signatures token.

By default, an interface is considered receiving a DoS attack if ten payloads are received within 30 minutes and a signature could not be created for the attack, and after 60 minutes, the payloads are disassociated with the @highrisk_signatures token.

- The links labeled **Expand all** and **Collapse all** allow you to display or hide all the settings for the <Common>, <MSRPC>, and <LPC> areas of this page.
- The Tasks menu has one menu item. Clicking **Manage Global Signatures** allows you to see the list of globally correlated signatures and manage them.

For more information about how to manage global signatures and local signatures, and how these settings are used when administering the automatic signature generation feature, see [Chapter 14, “Automatic Signature Generation”](#).

Scanning Data Tags

Scanning Data Tags represent text-matching patterns and built-in number patterns. If a rule triggers file scanning, CSA searches the file for all of the enabled scanning data tag patterns visible in the **Data Classification - Scanning Tags** page. If the pattern is found often enough in the file, the scanning data tag is attached to the file. Once the tag is attached to the file, other rules can control access to that file.

From the Configuration menu navigate Global Settings > Scanning Data Tags to reach the **Data Classification - Scanning Tags** page. See [Managing Scanning Data Tags, page 16-9](#) for a full description of that page and the administrative tasks associated with it.

Static Data Tags

A **static data tag** can be assigned to a file if a particular application accesses the file. **Static data tags** are built-in data tags distributed with this release and are listed on the **Data Classification - Static Data Tags** page on the CSA MC. You cannot change the names of these tags and you cannot create new static data tags.

You define the rules, based on your enterprise's needs, that assign static data tags to files. There are no Data Loss Prevention policies that come pre-configured to assign static data tags to files.

Static data tagging can be useful if, for example, you have a specialized application. Perhaps your enterprise is a hospital and you know in advance that any file that your specialized application reads falls under HIPAA guidelines. There is a <HIPAA Controlled> static data tag that you can apply to the file. This type of tagging method may also be useful when a file type is not scannable for a text-matching pattern, such as an audio file or a graphics file.

From the Configuration menu, navigate Global Settings > Static Data Tags to reach the **Data Classification - Static Tags** page. See [Managing Static Data Tags, page 16-14](#) for a full description of that page and the administrative tasks associated with it.

Report Configuration

Using the Report Configuration page, you can customize the look of all of your reports. For reports you generate as PDF, you can specify a font and an image for a watermark. For both PDF and HTML reports, you can specify an image for a logo. These customizations will be reflected on every report you generate.

The customizations are all optional. If you do not choose to customize your reports, they will be created using the default settings on the **Report Configuration** page.

The Report Configuration page is available in advanced mode only.

Configuring Reports

Follow this procedure to configure your reports:

-
- Step 1** From the Configuration menu, navigate Global Settings > Report Configuration.
 - Step 2** For PDF output report types, you can specify a font in the **Font Name** field. Only true type fonts (.ttf), true type collections (.ttc), and open type fonts (.otf) may be used.
 - a. Fonts can not be imported directly from the \Windows\Fonts directory. If the font you want is in the \Windows\Fonts directory, copy it from that directory and place it on your desktop or in some other location.
 - b. Click the **Add** button next to the Font Name field.
 - c. Browse to the new location of your desired font.
 - d. Select the font and click **Open**.
 - e. Click **Upload**.
 - Step 3** If you specified a font in the previous step, you must define its font type in the **Font Type** field. In the **Font Type** field select **Non-unicode Font** or **Unicode Font** depending on the font you chose in the previous step.

Step 4 For PDF output report types, you can specify an image to be used as a watermark. The optimum size for the watermark images is 600 x 400 pixels. You may upload image files with .bmp, .gif, .jpeg, and .jpg file extensions. To add an image to serve as your watermark:

- a. Click the **Add** link next to the **Watermark** field.
- b. Browse to the image you are going to use for your watermark.
- c. Select the image and click **Open**.
- d. Click **Upload**.

Step 5 For both PDF and HTML output types, you can specify an image to be used as a logo. The optimum size for the logo image is 920 x 520 pixels. You may upload image files with .bmp, .gif, .jpeg, and .jpg file extensions. To add an image to serve as your logo:

- a. Click the **Add** link next to the **PDF Logo** or **HTML Logo** field.
- b. Browse to the image you are going to use for your logo.
- c. Select the image and click **Open**.
- d. Click **Upload**.



Note The logo is displayed in the top right corner of the report and it replaces the default Cisco logo.

Step 6 Click **Save**. Rules do not need to be generated for these configuration settings to take affect.

Deleting Report Configurations

You can delete any fonts, watermark, or logo images that you have added to the Report Configuration page. This removes these fonts and images as a choice on the Report Configuration page but does not delete the font or image from your disk.



Note You cannot delete the default font or logo image nor can you delete fonts and images that are being used by a report.

Follow this procedure to delete an image or font:

-
- Step 1** Make sure the image or font you want to delete is not in use:
- From the Configuration menu, navigate **Global Settings > Report Configuration**.
 - Assume that the fonts and images displayed in the list boxes is in use by the reports.
 - If the font or image that you want to display is in use, change the font or image to another choice from the list box.
 - Click **Save**.
- Step 2** Go back and select the font or image you want to delete from the list box.
- Step 3** Click the blue **Delete** link next to the list box. The font or image is deleted.



CHAPTER 8

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 8-2](#)
 - [Processes Created by Application Classes, page 8-2](#)
 - [Removing Processes from Application Classes, page 8-2](#)
 - [Shell Scripts and Application Classes, page 8-3](#)
 - [Built-in Application Classes, page 8-4](#)
 - [Built-in Configurable Application Classes, page 8-7](#)
 - [Configuring Static Application Classes, page 8-8](#)
- [Dynamic Application Classes, page 8-12](#)
 - [Defining Dynamic Classes, page 8-13](#)
 - [Configuring Dynamic Application Classes, page 8-14](#)
 - [Configure an Application-Builder Rule, page 8-17](#)
 - [Configure a Rule Using a Dynamic Application Class, page 8-21](#)

- [Create New Application Classes from Rule Pages, page 8-22](#)
- [Application Class Management, page 8-23](#)

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 9-12](#). 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 8-8](#) 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.

**Note**

In general, with scripts such as perl scripts, the agent's ability to place the script in a configured application class depends upon whether the interpreter executes the script (via exec) or simply reads it. In the first case, the agent does recognize the script. In the latter case, it cannot.

**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 8-1](#)) 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 8-7](#). 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 8-1 Built-in Application Classes

The screenshot shows the 'Application Classes' section of the Cisco Management Center. The table lists 21 built-in application classes:

Name	Version	OS	Description	Attributes
Active Network Applications	6.0 r146	UNIX	Applications which have recently initiated or accepted a TCP/UDP connection	DR
Administrator defined - Applications considered Untrusted	6.0 r146	UNIX	This application class includes processes which untrusted and not in the globally defined White List	R
Administrator defined - Applications interpreting Untrusted file	6.0 r146	UNIX	Applications interpreting untrusted files	DR
Administrator defined - Applications reading Untrusted file	6.0 r146	UNIX	Applications reading untrusted files	DR
Administrator defined - White List Applications	6.0 r146	UNIX	This application class includes processes which are defined as White List files in the Global File Trust Settings.	R
Applications using email protocols	6.0 r146	UNIX	Processes which have attempted to use email related network protocols (e.g. SMTP)	DR
Applications using web protocols	6.0 r146	UNIX	Processes which have attempted to use web related network protocols (e.g. HTTP)	DR
Editor applications (Linux)	6.0 r146	Linux	UNIX Text Editing tools	R
Editor applications (Solaris)	6.0 r146	Solaris	UNIX Text Editing tools	R
Quarantined Processes - Local	6.0 r146	UNIX	Processes operating under quarantine due to local policy violation	DR
System Management Applications and descendants	6.0 r146	UNIX	Applications currently in use administrators to manage the system	DR
TTY applications	6.0 r146	UNIX	TTY login applications	R
Web browser clients (Linux)	6.0 r146	Linux	Web browser client executable files	R
<*Processes Executing Untrusted Content>			Built in application class	
<*Suspected Virus Applications>			Built in application class	
<All Applications>			Built in application class	
<First Time Application Execute>			Built in application class	
<Network Applications>			Built in application class	

Buttons at the bottom include New, Delete, Clone, Compare, 1 rule change pending, Generate rules, and Logged in as: amallio. A timestamp 242810 is also visible.

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.
- Processes performing a Print Screen—This includes all processes that access the print screen function. This class is available in the Clipboard access control rule to provide further protections to clipboard data by including print screen captured data.
- 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 (*) in the rule application class selection list boxes (see [Figure 8-1](#)). 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.

- Installation Applications—This includes processes installing software.
- 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 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.

- Third Party Security Applications:—This application class is used to mark other security products which may attempt to control similar resources as CSA. This application class provides certain built-in permissions to facilitate interoperability and system stability.

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 descendants 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 8-4](#).

To create an application class, do the following:

-
- Step 1** Log in to the CSA MC as a user with configure privileges and switch to Advanced Mode.
- Step 2** 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 3** Click the **New** button to create a new application class.

- Step 4** If you have not set an operating system admin preference, select whether this is a Windows or a UNIX rule module from the pop-up box that appears.



Note UNIX generically refers to both Solaris and Linux operating systems.

This takes you to the application class configuration view (see [Figure 8-2](#)).

- Step 5** 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 6** Enter a **Description** for your application class. This description becomes visible in the application class list view.
- 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 8-14](#) 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 9-12](#).

- 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 8-2](#) 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 descendants
- Only descendants of this process

(Creating an application class for "Only descendants 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 descendants of the IIS process from talking on the network.)

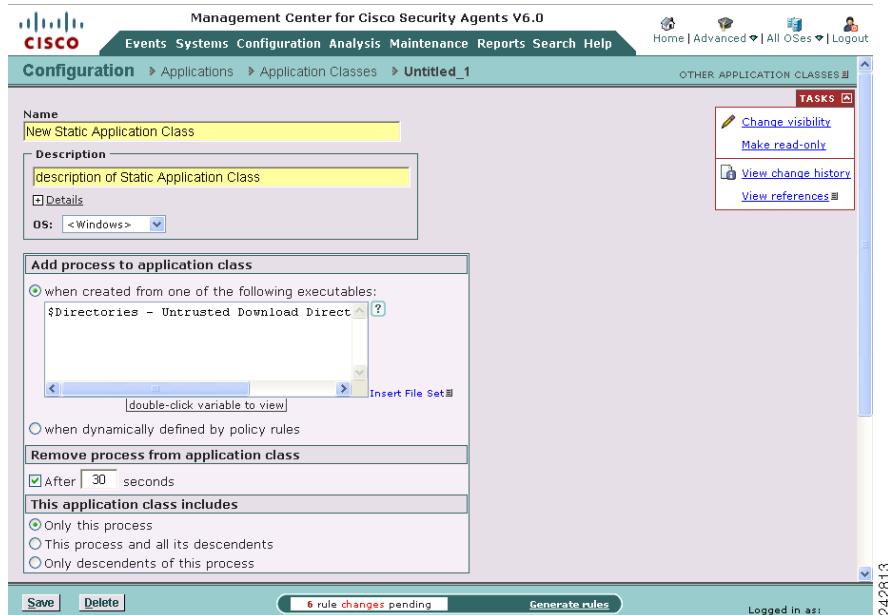
Step 10 When you are finished, click the **Save** button. This application class name, IIS Web Server application, now appears in the application list view and in the application selection fields for rule configurations. When you select it in a rule, you are indicating all the executables that comprise 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 5-10](#) for details on using the Compare tool.

See [Dynamic Application Classes, page 8-12](#) for information on that application class type.

Figure 8-2 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 descendants" 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 descendants 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** Log in to the CSA MC as a user with configure privileges and switch to Advanced Mode.
 - Step 2** 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 3** Click the **New** button to create a new application class.
 - Step 4** If you have not set an operating system admin preference, select whether this is a Windows or a UNIX rule module from the pop-up box that appears.



Note UNIX generically refers to both Solaris and Linux operating systems.

This takes you to the application class configuration view (see [Figure 8-3](#)).

- Step 5** 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 6** Enter a **Description** for your application class.
- Step 7** 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.)

**Tip**

When you use a dynamic application class in rules to define it, those “Defining rules” for the particular application class are accessible by clicking the link beside the **when dynamically defined by policy rules** radio button.

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 8-2](#) 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 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.

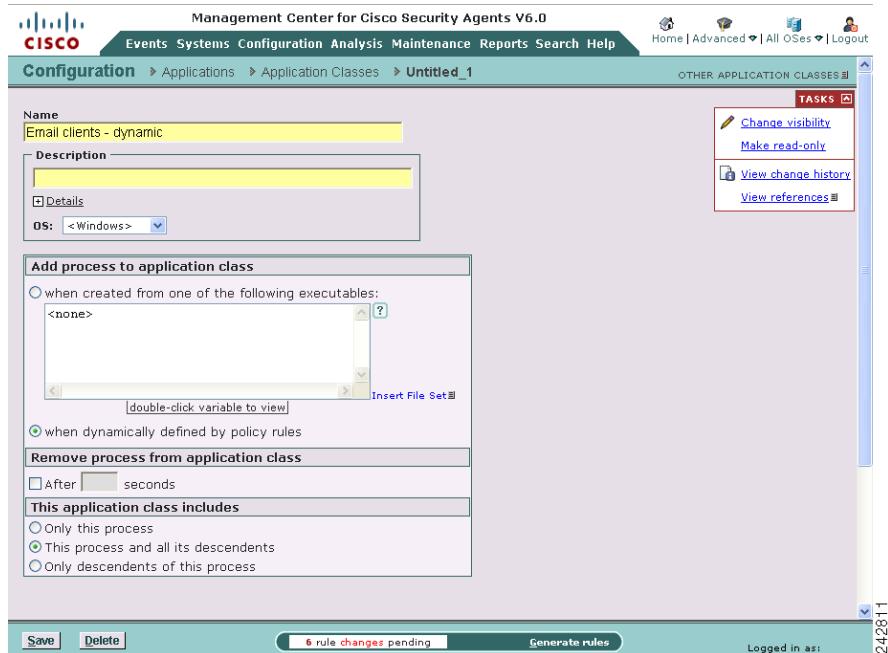
For this example, we will leave the default, **Only this process**, selected.

- Only this process
- This process and all its descendants
- Only descendants of this process

Step 10

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.

■ Dynamic Application Classes**Figure 8-3 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, log on to the CSA MC as a user with configure privileges and switch to Advanced Mode.

Step 2

Move the mouse over **Configuration>Rule Modules** in the menu bar. The list of existing rule modules is displayed in the rule module list page. CSA MC ships with several pre-configured modules.

Step 3

Click the link for the Rule Module to which you want to add this application-builder rule.

Step 4

Expand the Rules area of the rules module and click the **Add**.

Step 5 Click **Add rule** and select **Network access control**.

Step 6 In the Network access control rule, configure the following (see [Figure 8-4](#)):

- Enter a description
- In the **Take the Following Action** list box, select the **Add process to application class** and 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.

- 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 **Attempt to act as a client** from the pulldown list and select the pre-configured variable, **\$Email**, from the list of configured Network services.
- Leave the default of **<all>** entered in the **Communicating with host addresses** field.
- Leave the default of **<all>** entered in the **Use these local interfaces** field.
- **And—An enforcement action of the following type occurs.** Optionally, you can select one more of the available checkboxes. (Terminate, Deny, Allow, or Allowed by Default) 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 8-12

Step 7 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.

■ Dynamic Application Classes

Figure 8-4 Application-Builder Rule

The screenshot shows the Management Center for Cisco Security Agents V6.0 interface. The title bar reads "Management Center for Cisco Security Agents V6.0". The menu bar includes Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, Help, Home, Advanced, Windows, and Logon.

The main window displays the "Configuration" section under "Rule Modules" and "New Rule Module". The current view is "Network access control [719]".

The rule configuration details are as follows:

- Description:** Network access control rule [719]
Email clients - dynamic, app-class builder rule
- Enabled:**
- Take the following action:**
 - Add Process to Application Class: Dynamic Application Class [New|View] Email clients - dynamic
 - and
 - Log
- when:**
 - Applications in the following class: <All Applications>
 - But not in the following class: <none>
 - Attempt to act as a client for network service: \$Email [V6.0 r152]
 - Communicating with host addresses: <all>
 - Using these local interfaces: <all>
- and:**
 - This operation was Allowed by default
 - or it triggered another rule with enforcing action Terminate Deny Allow

At the bottom, there are buttons for Save, Delete, 23 rule changes pending, Generate rules, and a log entry for user 243808. The status bar shows "Logged in as: adm".

Configure a Rule Using a Dynamic Application Class

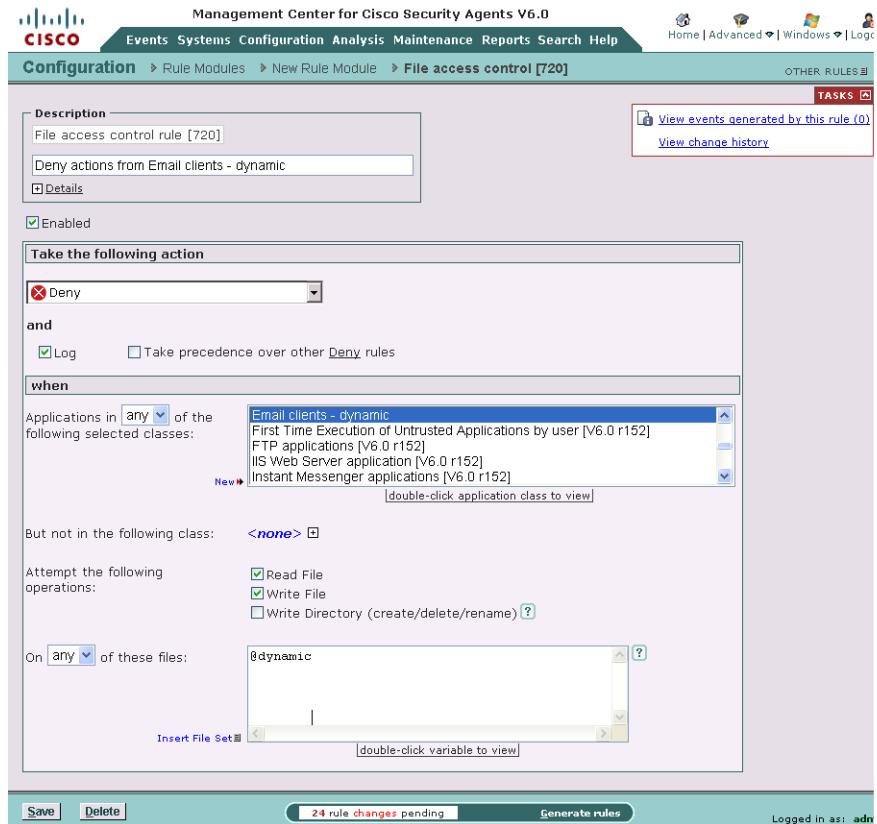
In this example, we are going to use a File access control rule to control the actions of a dynamic application class.

-
- Step 1** Configure this rule in the same manner in which you configure any other rule. For this example, access the same rule module you in which you configured application class builder rule in [Configure an Application-Builder Rule, page 8-17](#) and click **Add** in the Rules area of the module.
- Step 2** From the drop down menu, select **File access control**.
- Step 3** In the File access control rule, configure the following (see [Figure 8-5](#)):
- 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.

Create New Application Classes from Rule Pages

Figure 8-5 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** Log on to the CSA MC as a user with configure privileges and switch to Advanced Mode.
 - Step 2** 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 8-6](#)) there are swap box fields for CSA MC and for Application Behavior Investigation and Application Deployment Investigation.

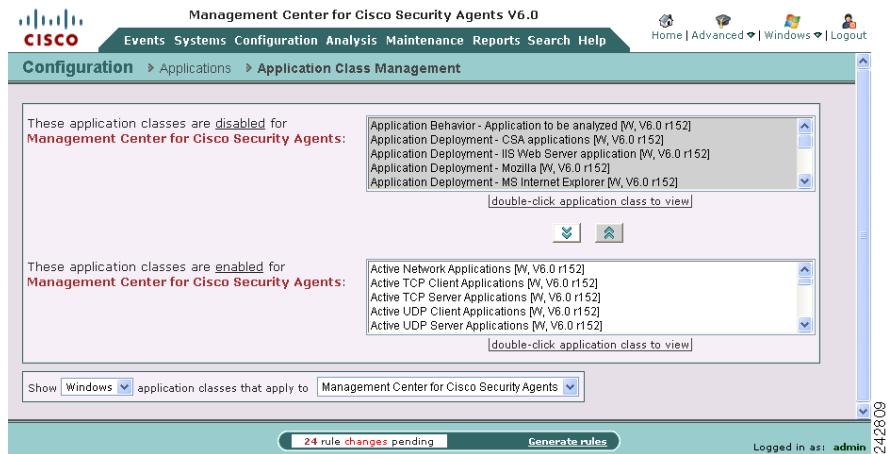
The application classes appearing in the white swap box(es) (the bottom swapbox for each category) are enabled for the feature in question. Those appearing in the gray swap box(es) (the top swapbox for each category) will not appear in the feature in question.
 - Step 3** Select an application class 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.)

Application Class Management



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 8-6 Application Class Management Window





CHAPTER 9

Configuring Variables and State Conditions

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.

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.

This section contains the following topics.

- [Where Variables are Used, page 9-2](#)
- [COM Component Sets, page 9-4](#)
 - [COM Component Extract Utility, page 9-6](#)
- [Data Sets, page 9-7](#)
- [File Sets, page 9-12](#)
- [Network Address Sets, page 9-18](#)

Where Variables are Used

- Network Interface Sets, page 9-21
- Network Services, page 9-24
- Notification Settings, page 9-27
- Query Settings, page 9-29
- Notification and Query Tokens and Syntax, page 9-32
- Localized Language Version Support, page 9-35
- Registry Sets, page 9-35
- Setting State Conditions, page 9-40
 - System State Sets, page 9-40
 - User State Sets, page 9-46

Where Variables are Used

The following section shows how variables relate to access control rules.

Available Variables types (COM Component Sets, Data Sets, Event Sets, File Sets, Network Address Sets, Network Interface Sets, Network Services, Query Settings, and Registry Sets) are shown on the left and the rule types or other configuration pages they can be applied to are shown below them.

- Variable type: *COM Component Sets*
 - COM Component access control rules
- Variable type: *Data Sets*
 - Data access control rules
- Variable type: *Event Sets*
 - Alerts
 - Reports
- Variable type: *Files Sets*
 - Application classes
 - File access control rules
- Variable type: *Network Address Sets*
 - Connection rating limiting rules

- Network access control rules
- Network shield rules
- Variable type: *Network Interface Sets*
 - Connection rating limiting rules
 - Network access control rules
 - Network shield rules
- Variable type: *Network Services*
 - Network access control rules
- Variable type: *Query Settings*
 - All access control query rules
- Variable type: *Registry Sets*
 - Registry access control rules

**Note**

Using variables is generally 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 5-10](#) for details on using the Compare tool.

See for [Chapter 10, “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

■ COM Component Sets

Preferences page and choose another admin preferences that Always uses Show All mode or change the preference assigned to you. See [Configuring Role-Based Administration, page 2-14](#).

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 9-6](#) 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 9-1](#)).

Step 4 In the available edit fields, enter the following information (See [Using the Correct Syntax, page 2-41](#). 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 [Configuring Role-Based Administration, page 2-14](#).

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

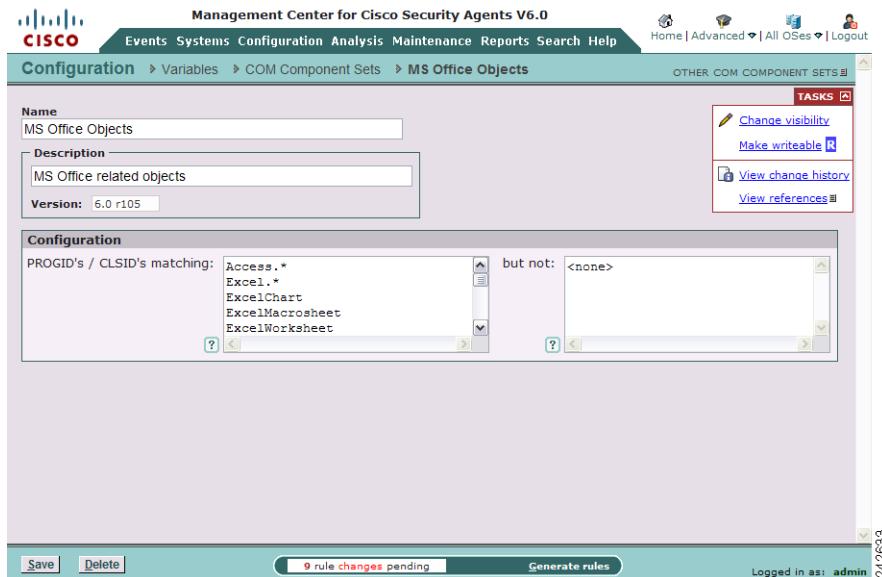
When entering CLSID's (uppercase hexadecimals), using the following syntax (You must include the brackets shown here.):

{000209FF-0000-0000-C000-00000000046}

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.

■ COM Component Sets**Figure 9-1 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 12-11](#).

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 either a set of patterns that will be matched against the URI portion of HTTP requests or MSRPC and LPC patterns for signature matching. 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 URI 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 pre-configured data sets groups for signatures match based upon the following:

- MSRPC Interface ID
- LPC Interface ID

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.



Note Data access control rules specifying HTTP protocol data sets are not supported for desktop versions of Windows operating systems.

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** **Name** the data set. 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.
- Step 5** **Describe** the data set. The text you put in the Description field is displayed in the list view helping you to identify this particular data set configuration.
- Step 6** Configure **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 [Configuring Role-Based Administration, page 2-14](#).
- Step 7** **Protocol**—Select the protocol for which you are configuring this data set. See [Data Set Interface Matching Syntax, page 2-55](#) and [Data Set Pattern Matching Syntax, page 2-55](#) for syntax requirements and examples.
- All:
 - **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.



Note When entering data patterns, the “*” character is a generic wildcard specification.

- **but not**—Make exceptions to the data strings you've entered in the Patterns 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.
- HTTP:
 - **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.
 - **but not**—Make exceptions to the data strings you've entered in the Patterns matching field. By default, this field has a <none> entry indicating no exceptions. When you click inside this field.
- MSRPC:
 - Enter an **Interface ID matching** to include or to exclude. The default is <all>. Generally, you will want to leave the default here and match by patterns over all interfaces.
 - **but not**—Make exceptions to the data strings you've entered in the Interface ID matching field. By default, this field has a <none> entry indicating no exceptions. When you click inside this field.
 - Enter **Patterns matching** to include or to exclude. These patterns are represented by the @signatures or @highrisk_signatures tokens.
 - **but not**—Make exceptions to the data strings you've entered in the Patterns matching field.
- LPC:
 - Enter an **Interface ID matching** to include or to exclude. The default is <all>. Generally, you will want to leave the default here and match by patterns over all interfaces.
 - **but not**—Make exceptions to the data strings you've entered in the Interface ID matching field. By default, this field has a <none> entry indicating no exceptions. When you click inside this field.
 - Enter **Patterns matching** to include or to exclude. These patterns are represented by the @signatures or @highrisk_signatures tokens.

- **but not**—Make exceptions to the data strings you've entered in the Patterns matching field.

**Note**

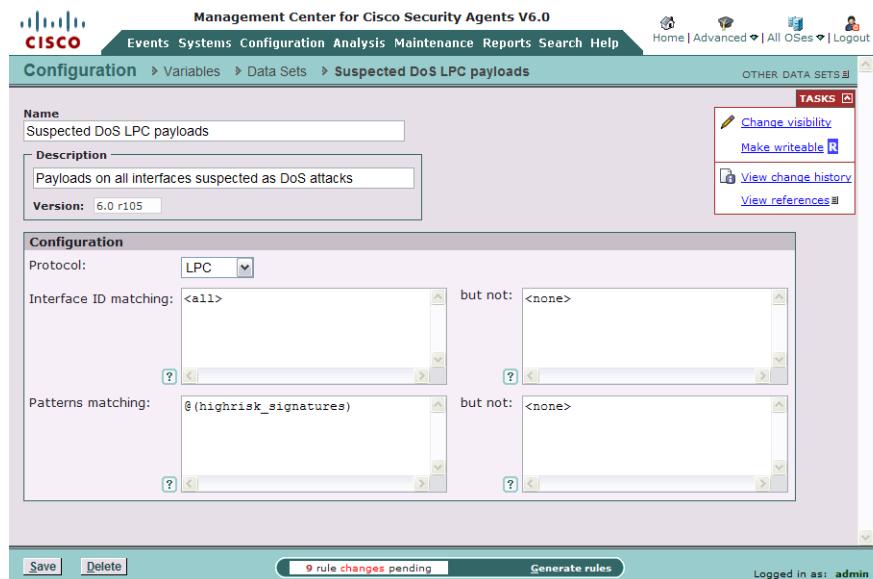
Specifying patterns other than @signatures may impact system performance. This is because a data access control rule specifying a data set of @signatures will be triggered only when the application in the rule attempts to access a payload that is associated with the @signatures token. If the data access control rule specifies a data set of “<all>” the rule will be triggered for every payload accessed by the application specified in the data access control rule.

In some rare cases, you may want to configure a data set using only a specified Interface ID. Such cases may be as follows:

- to block an MSRPC interface entirely; useful for interfaces known to be vulnerable
- use only high-confidence signatures for a particularly solid or mission-critical interface, use lower confidence signatures for an interface known to be vulnerable and less important
- create an exception for false positives on a particular interface
- take different actions based on an interface: query, deny, terminate, etc.

Step 8 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 9-2 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.

**Note**

You do not have to specify a setting for every field in the File Sets 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”.

To configure a file set, do the following.

-
- Step 1** Log on to the CSA MC as a user with configure privileges and switch to **Advanced Mode**.
 - Step 2** From the **Configuration** menu, mouse over **Variables** and select **File Sets**.
 - Step 3** Click the **New** button to create a new file set.
 - Step 4** If you have not configured an operating system preference for your administrator account, click **Windows** or **UNIX** in the pop-up box. If you have configured an operating system preference for your administrator account, the new file set will automatically be created for that operating systems. This takes you to the file set configuration view (see [Figure 9-3](#)).
 - Step 5** In the available edit fields, enter the following information (See [Using the Correct Syntax, page 2-41](#). 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.
- **OS**—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 **OS** list box.

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:

Windows example:

```
c:\Program Files\**\*SQL*\bin\**  
\\Program Files\**\*SQL*\bin
```

UNIX example:

```
/apache/webroot/**  
/usr/admn/sg
```

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 7-10](#) for more information.

Step 10 (UNIX only instruction) File Sets created for UNIX have an additional configuration field: **Attributes Matching**. 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 (Windows only instruction) File Sets created for Windows have an additional configuration field: **Content matching**. The Content matching field allows you to describe a set of files that all have the same tag. Follow these steps to add an **AntiVirus tag** in the Content matching field. The entry for each AntiVirus tag is placed on its own line in the Content matching box.

- a. Next to the Content matching edit fields, click the **Insert content** link. The **File Content Selector** pop-up opens.
- b. In the **Type** field, select **Virus scanning**.
- c. In the Tag field, type the virus tag name and click **OK**. See [Using the Correct Syntax, page 2-41](#) for syntax requirements for the @virusscan token.

If you prefer, you can also edit the Content matching field directly by clicking in the edit box. Follow the syntax guidelines for the @virusscan token.

- d. When you have added all the virus scanning tags, close the File Content Selector pop-up box.

For general information about the AntiVirus feature see [Chapter 15, “AntiVirus Basics.”](#)

Step 12 (Windows only instruction) File Sets created for Windows have an additional configuration field: **Content matching**. The Content matching field allows you to describe a set of files that all have the same tag. Follow this procedure to add a scanning data tag or static data tag in the Content matching field. The entry for each tag is placed on its own line in the Content matching box.

- a. Next to the Content matching edit fields, click the **Insert content** link. The **File Content Selector** pop-up opens.
- b. In the **Type** field, select **Data Classification**.
- c. Select a Data Classification tag from the Tag list box and click **OK**. The Tag list box contains all the enabled scanning data tags and static data tags. Choosing a tag from the Tag list box is the most accurate method of specifying a content type.

You can also click **New** to create your own scanning data tag in the **New Data Classification Setting** pop-up box. Once you have created your own tag, click **Save**. Click **OK** to add the tag to the **Content matching** box. See [Creating a Scanning Data Tag, page 16-11](#) for the procedure to create a content tag.

For more information about the Data Loss Prevention feature, see Chapter 9, “Configuring Variables and State Conditions.”

Step 13 (Windows only instruction) After specifying an AntiVirus, scanning data tag, or static data tag, you can enter exceptions in the **Content Matching but not** field. You can type the token and tag into the text field or insert the token and tag using the **Insert Content** link. Here are two examples of usage:

- You could enter @datascan=<*> in the Content matching field and enter @datascan=<SSN> in the but not field to search for all files with data scanning tags except those tagged <SSN>.
- You could enter, @virusscan=<virus:**> in the Content matching field and enter @virusscan=<Virus:Behavior**> to indicate all files with virus scan tags, except those files tagged with behavior-based AntiVirus tags.

Step 14 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.

Figure 9-3 File Set Configuration View

The screenshot shows the Management Center for Cisco Security Agents V6.0 interface. The title bar reads "Management Center for Cisco Security Agents V6.0". The top menu includes Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, Help, Home, Advanced, All OSes, and Log.

The main content area is titled "Configuration > Variables > File Sets > Application Deployment - MS Office executables".

Name: Application Deployment - MS Office executables

Description: Microsoft Office executable files

OS: <Windows>

Version: 6.0 r105

Configuration

Directories matching: <all> but not: <none>

Files matching: excel.exe, frontpage.exe, frontpg.exe, msaccess.exe, mspub.exe but not: <none>

Content matching: <all> but not: <none>

TASKS

- Change visibility
- Make writeable
- View change history
- View references

Buttons at the bottom: Save, Delete, 9 rule changes pending, Generate rules, Logged in as: admin 24635

Network Address Sets

Configure network address sets for use in network access control rules, network shield rules, and connection rate limiting rules to impose restrictions on specified IP addresses or a range of addresses. Once configured, you can 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 9-4](#)).
 - Step 4** In the available edit fields, enter the following information (See [Using the Correct Syntax, page 2-41](#). 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.
 - Step 5** **Address ranges matching**—In the available edit field, enter a single address, range of addresses, or network address class.
By default, this field has a **<all>** entry. When you click inside this field, the **<all>** disappears so that you can enter your own addresses. See [Using the Correct Syntax, page 2-41](#) for a full description of proper IPv4 and IPv6 address syntax.



-
- Note** IPv6 addresses can only be used by a rule associated with a Vista rule module.

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.

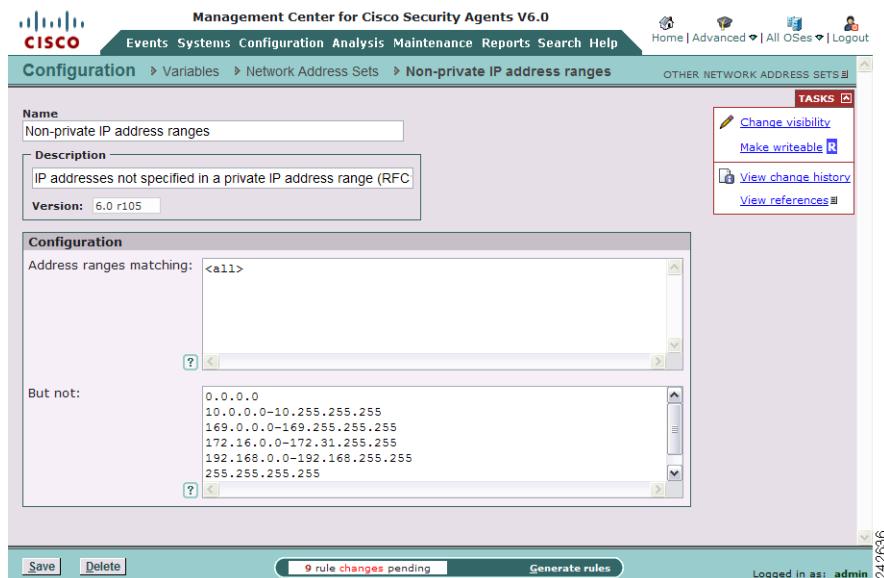
**Caution**

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.

but not—Use this field to make exclusions to addresses within the address ranges entered in the address matching field.

■ Network Address Sets

Figure 9-4 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.

Step 7 Once you have saved the Network Address Set, open the Tasks drop down menu if you want to change the visibility of the Network Address Set or make it Read-only.

Network Interface Sets

Configure network interface sets for use in network access control rules, network shield rules, and connection rate limiting rules to impose restrictions that take the local system interface into consideration. Once configured, you can simply enter the name of the network interface set in any applicable rules you create.

Note that interface types apply only to your local network and do not apply to remote connections. You can use network interface set in rules to control connectivity based on the manner in which a machine is talking on the network (rather than based on an address). For example, if a type of WiFi network interface type is detected, you can apply rules that deny wireless connections on your internal network.

**Note**

Network interface sets can only be used by rules applied to Windows operating systems.

To configure network interface 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 Interface Sets** from the cascading menu. Any existing network interface set configurations are shown.
- Step 3** Click the **New** button to create a new network interface set. This takes you to the configuration view (see [Figure 9-4](#)).
- 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 further information on that field.):
 - **Name**—This is a unique name for this network interface set.
 - **Description**—This is a useful line of text that is displayed in the list view and helps you to identify this particular set of network interfaces.
- Step 5** **Interface characteristics matching**—When you click the **Insert Interface Characteristics** link you can select one or more of the following interface Types and enter their corresponding Name characteristics. (The default entry for the Name field is “*”, meaning *all* or *don’t care*.):

**Note**

You can obtain the adapter name for a host from the host diagnostics. When you click on the **Detailed status and diagnostics** link for the host, the current installed interface and named characteristics for the host are displayed (labeled as InterfaceCharacteristics). For example, *Wired3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible)*. Also note, that wildcard entries can be used for interface type names. If you select WiFi, <Don't care> or wildcard entries are valid for all Mode, Encryption, and SSID fields. You can use the **Insert Interface Characteristics** link to configure these fields or you can enter literals - although it is not recommended that you use literal entries in these fields.

**Note**

<All> is the only valid setting for this field, when the Network Interface Set will be used with a rule protecting a UNIX, Solaris, or Linux system.

**Note**

CSA only deals with IP networks. Therefore, the following list of interface types only pertains to those connection types running over IP.

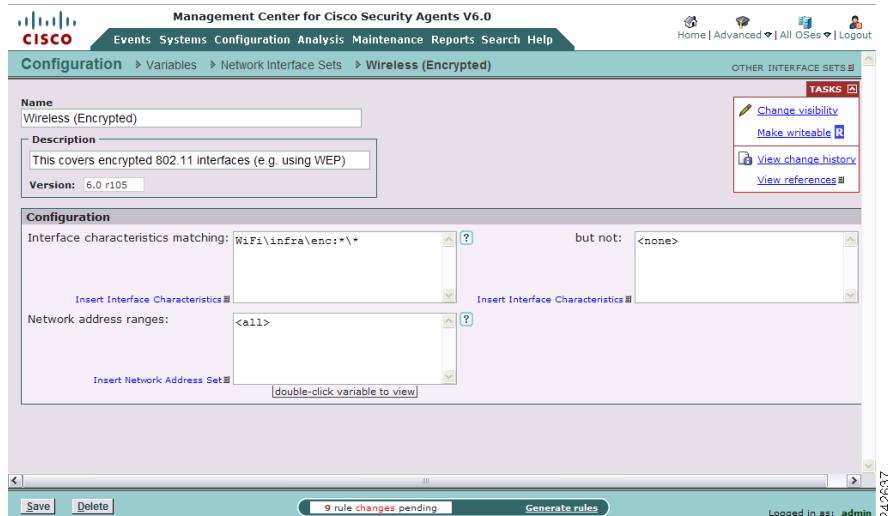
- Wired - Enter the Name (name is another interface characteristic) or enter a wildcard character (*) if you don't care.
- WiFi - Select a Mode as follows: Don't care, Infra, Adhoc
Select a WiFi Encryption type as follows: Don't care, clear, Encrypted (WEP), Encrypted (ckip), Encrypted (tkip), Encrypted (aes), Encrypted (other), Encrypted (any)
Enter an SSID (Service Set Identifier)
- Virtual - Enter the Name (name is another interface characteristic) or enter a wildcard character (*) if you don't care.
- PPP (Point to Point Protocol) - You have several suboptions for controlling connections based on PPP. PPP connections can also use one of the following device types:
<Don't care>, RAS server, unknown, modem, isdn, x25, vpn, pad, generic, serial, framerelay, atm, sonet, sw56, irda, parallel, PPoE.

All options, except for Ras server and unknown, also have **Device name** and **Connection name** fields. These are optional fields that allow for further granularity. It is recommended that you simply leave the default wildcard characters (*) in these fields. They are displayed because the system is able to retrieve this interface data, but it is likely that this is only useful for diagnostic purposes in log files. If you intend to use these fields for highly granular interface controls, note that Device name is referring to the connection device such as “parallel cable”, and Connection name is referring to the connection network information for the remote system receiving the connection. This field would contain the remote machine name or profile.

- Bluetooth - Enter the Name (name is another interface characteristic) or enter a wildcard character (*) if you don’t care.
- IEEE1394 - This is commonly known as FireWire. This interface connection type offers high-speed communications and isochronous real-time data services.
- Loopback - Routes communication between processes running on the same computer.
- Unknown - If CSA cannot determine the network interface, “Unknown” may appear for the adapter name for a host from the host diagnostics page. Although this should not occur often, you can use this Unknown option to write rules for adapter names that CSA cannot determine.
- Other - This includes any interface type not specifically named here, such as IrDA, WAN, ATM, Token Ring, etc. Enter the name or enter a wildcard character (*) if you don’t care. For example, Intel 1394 Net Adapter.

but not—Use this field to make exclusions to the interface characteristics entered in the Interface characteristics matching field.

Network address ranges—By default, this field includes <all> addresses. Click **Insert Network Address Set** to specify a preconfigured set of network addresses. To specify a specific address or a specific address range, enter that information here. Put each entry on its own line. For a complete description of permitted IPv4 and IPv6 addressing syntax, see [Using the Correct Syntax, page 2-41](#).

Figure 9-5 Network Interface Set Configuration View

- Step 6** When all required information is entered, click the **Save** button to save your configuration.

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 9-6).

Step 4 In the available edit fields, enter the following information (See [Using the Correct Syntax, page 2-41](#). 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 [Configuring Role-Based Administration, page 2-14](#).

Step 5 Protocol ports-Destination—Enter a tcp or udp protocol and corresponding port or port range to indicate a restriction.

By default, this field has a <all> entry indicating no ports. When you click inside the edit field, the <all> disappears so that you can enter your own port restrictions.

Use the following syntax:

TCP/21
UDP/1025-65535

Protocol ports-Source—**(CAUTION:** Using a specific source port, rather than the default of <all>, in a Network access control rule may degrade performance.) You can enter a tcp or udp protocol and corresponding port or port range to indicate a restriction if it is necessary. Generally, you will not want specify a specific port here and simply leave <all> as the entry for the source port. You only want to enumerate a specific source port for a data connection that has an ephemeral destination port and a well-known source port.

Since most network connections are keyed off of well-known destination ports, applications that only have well-known source ports, such as multimedia applications or Active FTP data connections, must be controlled off the source port. Therefore, if you are specifying a differentiated service marking for a multimedia connection, you would key off the source port.

**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 2-41](#) 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 9-6 Network Services Configuration View

Notification Settings

From the Notification Settings page, you can configure the notification text, radio buttons and check boxes that appear in the pop-up box the end user sees when notification rules are triggered.

To configure a notification pop-up box for use with a notification rule, do the following:

-
- Step 1** Log on to the CSA MC as a user with configure privileges and switch to **Advanced Mode**.
 - Step 2** From the **Configuration** menu, navigate **Variables > Notification settings**.
 - Step 3** On the Query Settings list page, click the **New** button to create a new query.



Note

CSA MC ships with several preconfigured notifications. You can use an existing one or create a new one.

Notification Settings

Step 4 Enter a unique **Name** for your notification. 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 notification setting for a rule.

Step 5 Enter a **Description** of your notification.

Step 6 In the **Text used to notify user** edit field, enter a description of the issue that likely triggered the notification. This text field allows you to provide localized notification text for agents using the corresponding language on their desktop.

This is the same text that will appear in the notification 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 [Notification and Query Tokens and Syntax, page 9-32](#).

**Note**

All Cisco Security Agent kits contain localized support for English, French, German, Italian, Japanese, Korean, Simplified Chinese, Spanish, Polish, Brazilian Portuguese and Russian 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 9-35](#) for more details.

Step 7 The **Allowed notification responses** multi-select box lets you choose which buttons appear on the notification pop-up box. You can select to display an OK button or a Yes/No button combination.

Step 8 If the notification is not answered by the user within 5 minutes or if the user is not logged in to the system, the **Default response** you select here is taken.

Step 9 In addition to notifying the user, you can require the user to type in a **user justification** statement in a pop-up window edit field. This justification text typed in by the end user appears in the event log message on the MC.

Step 10 Click the **Save** button.

- Step 11** By opening the **Tasks** menu on query settings page you can change the visibility, make this variable read-only, or view more information about the query.

Query Settings

From the Query Settings page, you can configure the query text, radio buttons, and check boxes that appear in the pop-up box the end user sees 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** Log on to the CSA MC as a user with configure privileges and switch to **Advanced Mode**.
- Step 2** From the **Configuration** menu, navigate **Variables > Query settings**.
- Step 3** On the Query Settings list page, click the **New** button to create a new query. See [Figure 9-7](#).



- Note** CSA MC ships with several preconfigured queries. You can use an existing one or create a new one.

-
- Step 4** 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 5** Enter a **Description** of your query.

Step 6 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 [Notification and Query Tokens and Syntax, page 9-32](#).

**Note**

All Cisco Security Agent kits contain localized support for English, French, German, Italian, Japanese, Korean, Simplified Chinese, Spanish, Polish, Brazilian Portuguese and Russian 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 9-35](#) for more details.

Step 7 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 8 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.

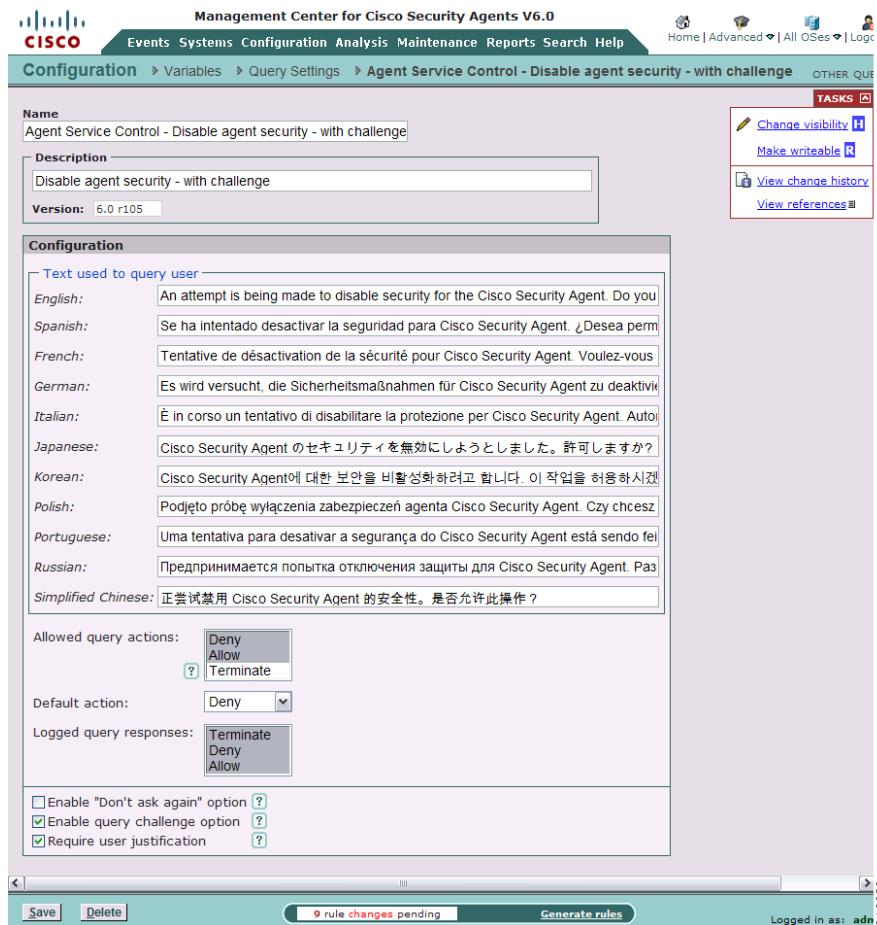
- Step 9** In addition to deciding which query actions (Allow, Deny, Terminate) are available to the user for the query pop-up, you can also configure the query response to log only when a particular query action is selected by the user. Using the multi-select box available from the **Logged query responses** section, you can select one or more response types to produce a log message. For example, if all query actions are being made available for the query, you can configure only a Terminate response to produce a log message. (By default, all query responses are logged.)
- Step 10** 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 11** 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 12** In addition to querying the user, you can require the user to type in a **user justification** statement in a pop-up window edit field. This justification text typed in by the end user appears in the event log message on the MC.
- Step 13** Click the **Save** button.
- Step 14** By opening the **Tasks** menu on query settings page you can change the visibility, make this variable read-only, or view more information about the query.

**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.”

■ Notification and Query Tokens and Syntax

Figure 9-7 Query Settings Configuration View



Notification and Query Tokens and Syntax

The edit fields for query text and notification text use the same syntax: These are the rules for that syntax:

- The query and notification text must be up to 256 characters long including punctuation.

- Any character on your keyboard may be used in the query or notification text.
- You can use specially designated tokens to represent the corresponding values presented to the end user who is responding to the query or notification.
- If tokens are used in one language, they must be used in all languages.

When entering text into the edit field of queries or notifications, you can use the following tokens to represent the values presented to the end user who is responding to the query.

- @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.
- @appname_short - The name of the process triggering the action. Use in all access control rule types.
- @child - The path of the process being invoked. Use in Application control rules
- only.
- @clsid - The GUID of the COM object. Use in COM component access control rules only
- @content - For file access control rules and scan event log rules, this is the content of the file being accessed. For other rule types, @content is the content of the file that triggered entry into the dynamic application class.
- @content_clean - For file access control rules and scan event log rules, this is the simplified content of file being accessed. For other rule types, @content_clean is the content of the file that triggered entry into the dynamic application class.
- @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 and scan event log rules. For other rule types, @filename is the file path that triggered entry into the dynamic application class.

- @filename_short - The name of file being accessed by file access. Use in file access control rules and scan event log rules only. For other rule types, @filename_short is the file name that triggered entry into the dynamic application class.
- @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.
- @hostaddrname - The remote hostname or 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.
- @mediadevice - The name of the media device being monitored. Use in System API control rules only.
- @mediaport - The port on which the media device is being monitored. Use in System API control rules only.
- @netservice - The service/destination port used by the remote connection end. Use in Network access control rules only.
- @netop - The type of network operation (client/server). Use in Network access control rules only.
- @parent - The path of the parent process. Use in Application control rules only.
- @progid - The ProgID of the COM object. Use in COM component 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 and notifications 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 and notifications 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, the queries, notifications, and the events appearing in the Windows Event Log appear in Japanese.

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 **Audit 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 9-8](#)).
- 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 [Configuring Role-Based Administration, page 2-14](#).
- Step 5** **Registry keys matching**—You *must* enter a value in this field if you are creating a registry set.
It is recommended that there be at least one non-wildcarded component in a registry key other than the hive itself. Otherwise, the specified key might be overly generalized.
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 9-1 Example valid and invalid registry key entries

\MSSQLSERVER	This is a valid entry.
-------------------	------------------------

Table 9-1 Example valid and invalid registry key entries

HKLM\SOFTWARE\CSCOpX**	This is a valid entry.
FOO\SOFTWARE\CSCOpX**	This is invalid (FOO is not a hive).
*\SOFTWARE\Cisco**	This is a valid entry.



Note Note that the wildcard syntax explained in [Wildcard notation for directories and filenames, page 2-44](#) also applies to registry sets.



Note The asterisk is a valid single character in a registry key. For example, HKEY_CLASSES_ROOT*\OpenWithList is a registry key. If you want to represent the * with a wildcard, use the "?" character instead of a * character.

The @reg shorthand notation may be used in the Registry keys matching field. See [Referencing Values Stored on Clients, page 2-58](#) for more information on the @reg notation. This is an example of valid syntax for the @reg token.

```
@(reg HKLM\SOFTWARE\MyKey\CustomKey\StringValue)
```

Step 6 **but not**—Make exceptions to registry keys.

Step 7 **Registry values matching**— In the Registry values matching field, enter the values, one per line, to which you are controlling access. CSA MC will look for the value you put in this field in the key you defined in the previous Registry keys matching field. Examples of valid registry values are as follows:

```
BootExecute
run
load
```

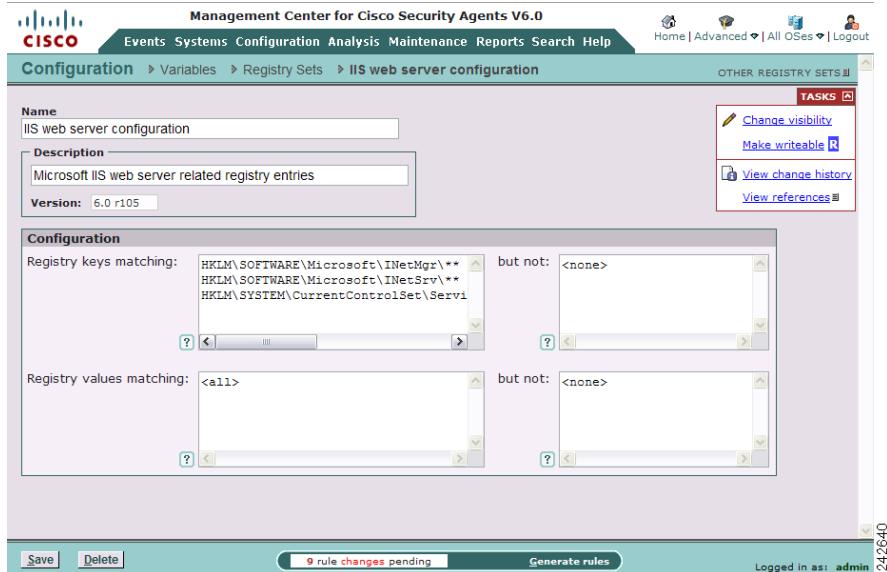
Step 8 **but not**—Make exceptions to registry values.

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.

■ Registry Sets

Figure 9-8 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.

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” rule 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 more lenient 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”.

Configure a System State Set by doing the following:

-
- Step 1** Move the mouse over **Configuration>Variables** 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 9-9](#).
 - 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 **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.

**Note**

Currently, the Cisco Trust Agent is only supported on pre-Vista Windows platforms and Linux platforms. CTA is not supported on Windows Vista platforms.

**Note**

Before setting a Cisco Trust Agent posture, check with your NAC system administrator to learn what the different posture choices imply for your network security.

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 sidebar 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 Interface** field to enter one or more network interface sets to create a state condition based on system address or location or connection type. By default, no restrictions are set here. If you enter interface conditions here, the condition applies if at least one interface matches what is specified. If you enter multiple interfaces here, only one interface has to match for the system state to apply. The interface types apply only to your local network and do not apply to remote connections. You can use this feature to control connectivity based on the manner in which a machine is talking on the network (rather than based on an address). For example, if a type of WiFi network interface type system state is triggered, you can apply rules that deny wireless connections on your internal network. See [Network Interface Sets, page 9-21](#) for Network Interface configuration details.

Step 8 You can use the DNS suffix matching field to set a condition based on the suffix of the DNS server domain name. If any DNS server domain suffix matches an item specified in the DNS suffix matching field, the condition is applied. You can use the **but not** field to make specific exclusions to DNS suffix matching parameters you configure.

These are examples of proper syntax that will match a DNS server with domain suffix, `regional.acme.com`:

You can enter the entire suffix: `regional.acme.com`

You can also enter the suffix expressed with a wildcard: `*.acme.com`.

Step 9 In the **Data Classification** area, you can use the Data Classification matching field to set a state condition based on the presence of a scanning data tag or static data tag.

Click the **Insert Tag** link to add a scanning data tag or static data tag to the **Data classification matching any (or all) of these tags** field. The Tag list box contains all the enabled scanning data tags and static data tags. If multiple tags are entered, use the drop-down box to choose whether the state condition should be set upon matching any or all of these tags. You can use the **but not** field to make specific exclusions to data classification tag parameters you chose.

Step 10 In the **Custom State Conditions** area you can specify one or more custom state tags or leave the field with the default <Don't care> tag. These custom state tags are available to CSA MC administrators to configure if the system states provided do not suit their needs. The custom state conditions are defined using rule types which make use of the "Set" attribute. See [Attribute: Custom-made state condition, page 5-27](#) for information on how these states are defined.

Step 11 In the **Additional State Conditions** area, 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.
- Select the **Untrusted 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 a “Set-detected rootkit-Untrusted” rule in a rule module. When this “Set” rule type triggers, the system state consequently takes effect. See [Attribute: detected rootkit trust status, page 5-32](#) for more information on this setting.

Note that this is a persistent state. This state condition, once set, can only be removed by using the Reset feature. See [Resetting Cisco Security Agents, page 3-9](#). (Most states are not persistent in this way. Most states can be switched in and out using rule triggers. A persistent states can only be switched “on” using rules and must be switched “off” manually.)

- Select the **Virus detected** option to set a state condition to apply if a signature-based or behavior-based virus is detected on a system. Based on that virus detection, a state condition setting can enforce a designated set of rules.
- Select the **Unprotected access detected** option to set a state condition when an application or service, or other system component that is marked as Unprotected does not have a corresponding Protected rule and is therefore not being protected by the agent. See [Attribute: detected access, page 5-30](#) for more information on this setting.
- 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 **Insecure boot detected** option to set a state condition to apply if a previous system boot occurred in a non-standard manner. For example, the system was booted from a peripheral device (CD ROM) rather than from the hard drive. This type of boot can be considered non-standard and therefore possibly suspicious. (This is one way of introducing a Trojan to a system.) This type of peripheral device insecure boot detection works in conjunction with a particular type of compatible BIOS on compliant systems. The compatible BIOS detects a non-standard boot and on the next normal boot, if you have an appropriately configured Kernel Protection rule (see [Kernel Protection, page 6-53](#)), a message is sent to the MC which logs this insecure boot detection. This, in turn, causes the system state (if configured) to trigger.

A Safe Mode boot also falls into this insecure boot category. Compatible BIOS is not required for a Safe Mode boot detection. But, Safe Mode boot detection is only supported on Windows platforms.

This state condition could be met if you are using a “Set-detected boot-as insecure” Kernel Protection rule. When this “Set” rule type triggers, the system state consequently takes effect. See [Using the Set Action, page 5-25](#) for more information on this setting.

Note that this is a persistent state. This state condition, once set, can only be removed by using the Reset feature. See [Resetting Cisco Security Agents, page 3-9](#). (Most states are not persistent in this way. Most states can be switched in and out using rule triggers. A persistent states can only be switched “on” using rules and must be switched “off” manually.)

Step 12 Click the **Save** button.



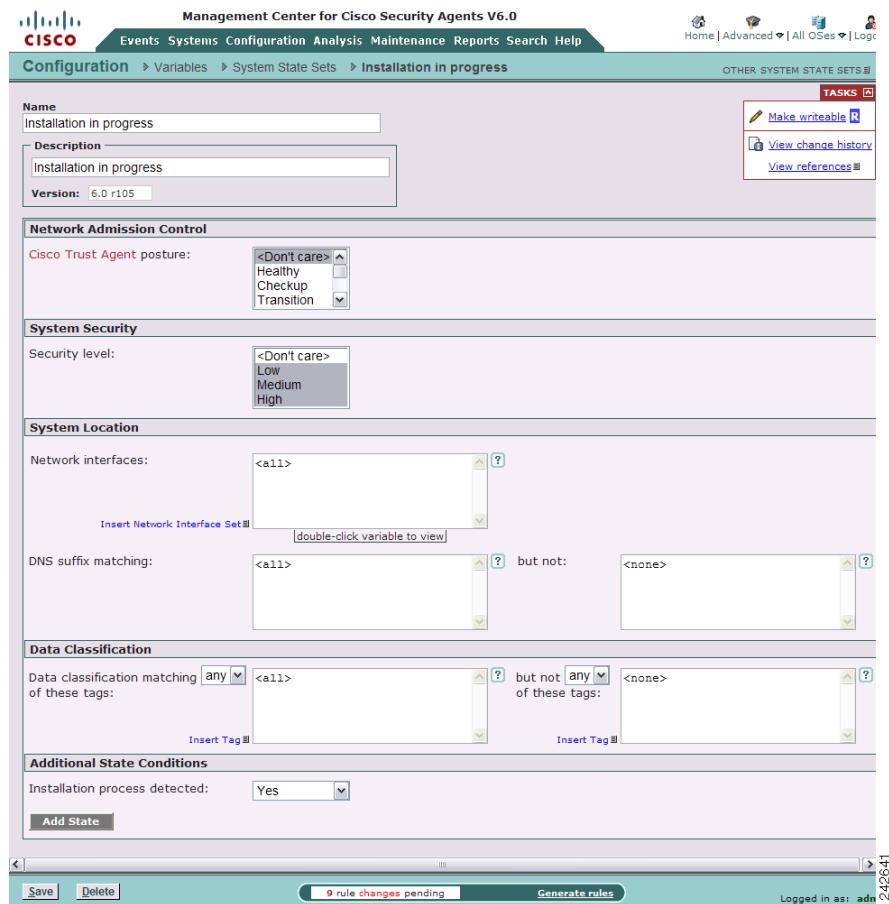
Note

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 9-9 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 9-10](#).
- 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, parentheses, and periods 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/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/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 User and Group names are case sensitive for UNIX. They are not case sensitive for Windows.



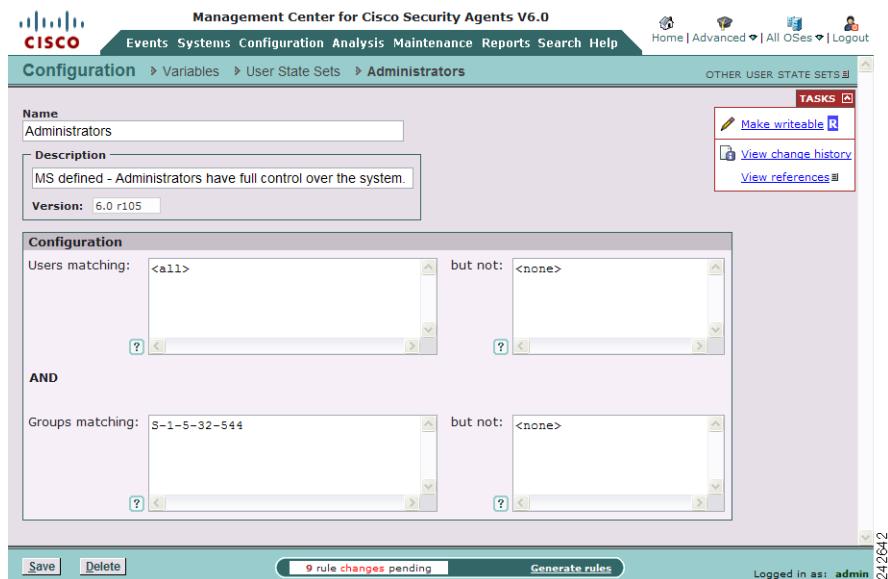
Note It is recommended that you use Group permissions rather than User permissions because Group designations are more widely applicable.

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.



Note In addition to user information found in logged events, you may use the host diagnostic feature to retrieve a record of observed user/group credentials on a given host. This may be useful in troubleshooting policies. It's important to note that the record of credentials that is displayed does not imply that a rule fired in that user's context.

Setting State Conditions**Figure 9-10 User State Conditions**



CHAPTER 10

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, 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 10-2](#)
 - [Filtering Events, page 10-5](#)
 - [Event Aggregation and Suppression, page 10-9](#)
 - [Graphing Similar Events, page 10-11](#)
 - [Reading Event Details, page 10-13](#)
 - [Reading Packet Details, page 10-14](#)
- [Event Monitor, page 10-14](#)
- [Event Analysis, page 10-15](#)
- [Event Managing Tasks, page 10-17](#)

- [How Logging Works, page 10-21](#)
 - [Verbose Logging, page 10-22](#)
 - [Logging and Query User Rules, page 10-22](#)
- [About the Event Management Wizard, page 10-23](#)
 - [Creating Exception Rules, page 10-24](#)
 - [Creating Logging Exception Rules, page 10-28](#)
 - [Perform an Application Behavior Investigation, page 10-33](#)
 - [Suppressing Similar Events, page 10-36](#)
 - [Purge Similar Events, page 10-38](#)
- [Event Sets, page 10-39](#)
- [Third Party Access to Events, page 10-43](#)
- [Configuring Alerts, page 10-45](#)
 - [Generate an Alert Log File for Third Party Applications, page 10-50](#)

The Event Log

The Event Log view lets you view system events provided by registered agents according to designated time frames, event severity levels, and the system that generated the event. To reach the Event Log screen, begin at the CSA MC menu bar and navigate **Events > Event Log**.

Figure 10-1 Event Log Screen

#	Date	Host	Severity	Action	Event
19	4/22/2008 3:28:57 PM	client221	Notice	?	The process 'D:\Program Files\Cisco\CSAgent\BIN\okclient.exe' (as user CLIENT221\Administrator) attempted to access a resource which resulted in the user being asked the following question: 'An attempt is being made to disable security for the Cisco Security Agent. Do you wish to allow this?' The user was prompted and a 'Yes' response was received. The user provided the following justification: 'running vmware' Details Rule 368 Wizard Find
18	4/22/2008 3:28:45 PM	client221	Alert	☒	The process 'D:\Program Files\VMware\VMware Workstation\vmware.exe' (as user CLIENT221\Administrator) attempted to initiate a connection as a client on TCP port 80 to 72.246.126.52 using interface Wired\Intel(R) PRO/1000 MT Desktop Adapter. The operation was denied. Details Rule 409 Wizard Find
17	4/22/2008 3:28:16 PM	client221	Alert	☒	The process 'D:\WINDOWS\System32\svchost.exe -k netsvcs' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on UDP port 138 to 192.168.214.255 using interface Virtual\VMware Virtual Ethernet Adapter for VMnet1. The operation was denied. Details Rule 409 Wizard Find
16	4/22/2008	client221	Alert	☒	The process 'D:\Program Files\Internet Explorer\iexplore.exe' (as user 18 rule changes pending Generate rules Logged in as: admin 18/38

The event log screen (see [Figure 10-1](#)) 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. They also provides the exact time the event was recorded 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 10-13](#), for more information. The Details link also provides packet information when appropriate. By installing Wireshark (<http://www.wireshark.org>) on the same server in which 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 10-14](#) 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 **Wizard** link, where available, to edit the rule that caused the event. See [About the Event Management Wizard, page 10-23](#) for details.

A **System State** link appears with an event when the rule in question has triggered due to a system state condition. (Note that it is not always advisable to generate a wizard exception based on an event that is appearing due to a system state condition triggering. Rather, if you intend to configure an exception, you should create it for the original rule that caused the system state to apply.) Use the pop-up that appears when you click **System State** from an event to trace back to the original rule (if available) that triggered the system state condition.

Use the Find link to open the Find Similar Events dialog box and search for messages similar to the one displayed in the Event log. Use the Graph link to display similar events graphically.

The information displayed on the Event Log page is controlled by the settings defined in the Change Filter window. The Change Filter window allows you to sort information by event set or by defining a custom filter. The way the events are filtered is presented at the top of the Event Log page.

Figure 10-2 Event Log Filter Summary



The event log filter summary provides this information depending on the settings in the event filter.

- **Event log generation time:** This is the timestamp of the moment the filter was applied and a list of events displayed.
- **Event set:** This indicates the name of the Event Set, if any, used to filter the event log view.
- **Time range:** This indicates the start date and end date used to filter the event log view.
- **Severity:** This is the current minimum and maximum severity range set for the event log filter.
- **Host:** This indicates the name of the host used to filter the event log view.
- **Policy:** This displays the name of the policy used to filter the event log view.

- **Security Service:** This displays the name of the security service used to filter the event log view.
- **Rule ID:** This displays the rule number used to filter the event log view.
- **Events per page:** This defines how many events are displayed on each page of the event log.
- **Filter text:** This displays the text string included or excluded from the event log filter.
- **Filter out similar events:** When event filtering is enabled (it's enabled by default), the event log displays an aggregation of events. This aggregation means that one representative event is displayed for all events that are considered similar on the MC. Similar events are defined as having the same rule ID and the same application name and path (excluding drive letter). When similar events are filtered from the event log view in this way, there is italicized text below the viewable representative event. This text displays the number of filtered events that are not visible. Clicking the **Find** link in the row of the event causes all events of this similar type to be displayed in a new event log window.

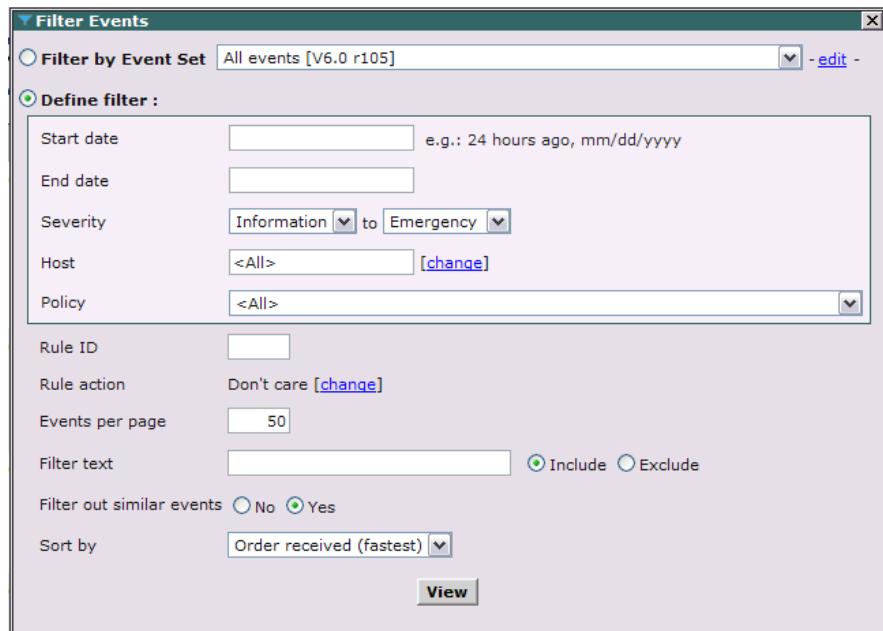
**Note**

This event filtering feature is enabled by default. Accessible from the Change filter link at the top of the Event log page, you can change the Filter out similar events radio button to **No** to turn this feature off.

- **Sort by:** Indicates the list is sorted by the **Order received** or by **Date**.

Filtering Events

Events can be filtered either by event set or by defining a custom filter. Click the change filter link in the event log filter summary area to display the Filter Events dialog box.

Figure 10-3 Filter Events dialog box

107384

Filtering Events by Event Set

An event set is a pre-defined set of search criteria. To learn more about event sets see “Event Sets” section on page 10-39.

-
- Step 1** Click the **change filter** link in the event log filter summary area.
 - Step 2** In the Filter Events dialog, select an event set from the **Filter by event set** pull-down menu.
 - Step 3** Click **View**. The events are filtered by event set and the Event Log screen shows the results.

Filtering Events by Defining a Custom Filter

Searches defined by search criteria are “and” searches. That is, the more attributes you specify to search by, the fewer number of events are likely to be found by the search.

-
- Step 1** Click the **change filter** link in the event log filter summary area.
- Step 2** In the Filter Events dialog, select the **Define filter:** radio button. You can filter your events using any of these attributes:
- **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 specify a relative time using any of the following terms: tomorrow, yesterday, today, now, next, ago, year, month, week, day, hour, minute, and second.
 - You can 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.
 - You can 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 from the following severities:
 - 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.
- **Policy:** In the “Advanced View” of the CSA MC, you can filter events based on what security policy the event triggered.
- **Security Service:** In the “Basic View” of the CSA MC, you can filter events based on what security service was triggered by the event.
- **Rule ID:** This field allows you to enter a specific rule number that you want to search for.
- **Events per 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 6-57](#).

- **Filter text:** Enter a text string to search for. Select **Include** to include events that contain the text string in your search, select **Exclude** to exclude events that contain the text string from your search results.
- **Filter out similar events:** When event filtering is enabled (it’s enabled by default), the event log displays an aggregation of events. This aggregation means that one representative event is displayed for all events that are considered similar on the MC. Similar events are defined as having the same rule ID and the same application name and path (excluding drive letter). When similar events are filtered from the event log view in this way, there is italicized text below the viewable representative event. This text displays the number of filtered events that are not visible. Clicking the **Find Similar** link below the event causes all events of this similar type to be displayed in a new event log window.



Note This event filtering feature is enabled by default. Accessible from the **Change filter** link at the top of the Event log page, you can change the **Filter out similar events** radio button to **No** to turn this feature off.

- **Sort by:** You can sort the final list of events by **Order received** or by **Date**.
- Step 3** Click **View**. The events are filtered by your search criteria and the Event Log screen shows the results.

Event Aggregation and Suppression

When first deploying rules to agents, it is not unusual to have an overwhelming flurry of events appearing in the event log. In some cases, most of these events are similar events or simply “noisy”, not useful events to view. If this is the case, the event log provides two mechanisms for paring down the number of events that appear:

- **Event Filtering (aggregation of events)**

When event filtering is enabled, the event log displays an aggregation of events. This aggregation means that one representative event is displayed for all events that are considered similar on the MC. Similar events are defined as having the same rule ID and the same application name and path (excluding drive letter).

When similar events are filtered from the event log view in this way, there is italicized text below the viewable, representative event. This text displays the number of filtered events that are not visible. Clicking the **Find** link allows you to search for all events of this similar type. Clicking the **Graph** link allows you to graph similar events.

Figure 10-4 Event Log Find Similar

Note This event filtering feature is enabled by default. Accessible from the **Change filter** link at the top of the Event log page, you can select the “Filter out similar events” **No** radio button to turn this feature off.

A “similar” event meets the following criteria:

- Same event code type.
 - Same rule ID.
 - Same application name and path (excluding drive letter).
- **Event Suppression**

When event suppression is enabled, all chosen events are no longer displayed in the event log. Event suppression is best used when you have a reoccurring event that is more noisy than useful to you. This is something you are aware of, but no longer wish to see. Suppressing the event removes all viewable instances of that event and causes further events of the same type to be hidden. Note that these events remain in the database, they are simply not displayed. The visibility of the suppressed events is controlled by Administrator Preference settings. Refer to [Configuring Role-Based Administration, page 2-14](#).

**Note**

Event suppression can also be enabled through the Event Log Wizard. See [About the Event Management Wizard, page 10-23](#). Clicking the **Wizard** link from the event you wish to suppress allows you to create a suppression filter for the event.

Graphing Similar Events

When using the advanced view of the CSA MC, administrators can graphically display similar events using the **Graph** link in the Event Log.

Events may be graphed to show when similar events occurred over time or they may be graphed to show a breakdown of the differences in aggregated events.

Events graphed by time are filtered via a set of criteria, counted per unit of time, and graphed versus time. For example, you could create a graph of Events vs. Time where each day is represented in a point and the value of the “y” axis is the number of events that occurred that day. This filtering is very similar to the Find option.

Events that have a host associated with them can be graphed in the format Hosts vs. Time. In this case the “y” axis value indicates the number of hosts that generated an event meeting the criteria during a day.

Differences in aggregated events are broken down and displayed in a bar chart. This could give you a visual image of how, for example, one application has been denied or allowed access to a variety of different files.

Each point on a graph, or line in a chart, is also a hyperlink. You can mouse over to see summary information about that data or you can click the data point, to display the events it represents.

Graphing Similar Events by Time

-
- Step 1** From the Event Log window, select an event that you want to display graphically, and click the **Graph** link for the event.
 - Step 2** Click the **Time** link.
 - Step 3** In the Graphing Criteria dialog box, select the filtering criteria for your graph:

- Type refers to event type.
- Policy Rule indicates what rule was triggered for the event log entry.
- Application describes the application involved in the event.
- Host is the name of the host.
- Severity is the severity level of the event.
- Time Frame allows you to choose the span of time around the current date and time.
- Filtered text allows you to include or exclude events based on the presence of a text string in the even description.

Step 4 In the **Graph Options** area, select the kind of events to count per day and the time scale of the graph: hours, days, months, or years.

Step 5 Click **Create Graph**. The graph is displayed in a pop-up box.

After the graph has been created you will be able to change graph criteria, print the graph, and download the graphed data as a .csv (comma separated value) file by clicking for that task.

You will also be able to analyze a data point on the graph by clicking it. Mousing over a data point on the graph pops up summary information about the data point. Clicking on the data point will show you all the similar events that it represents.

Graphing Similar Events by Differences

Step 1 Log on to the CSA MC and switch to **Advanced Mode**.

Step 2 From the Event Log window, select an event that you want to display graphically, and click the **Graph** link for the event.

Step 3 Click the **Differences** link. The aspects of the event message that have been aggregated are outlined with a blue box.

Step 4 Click one ore more of the blue criteria fields in order to create the graph based on those criteria. When more than one criteria is selected, the graphing tool interprets that as an “and” request. Both the criteria must be present in the event for it to be graphed.

Step 5 Click **Create Graph**. The graph is displayed below the event.

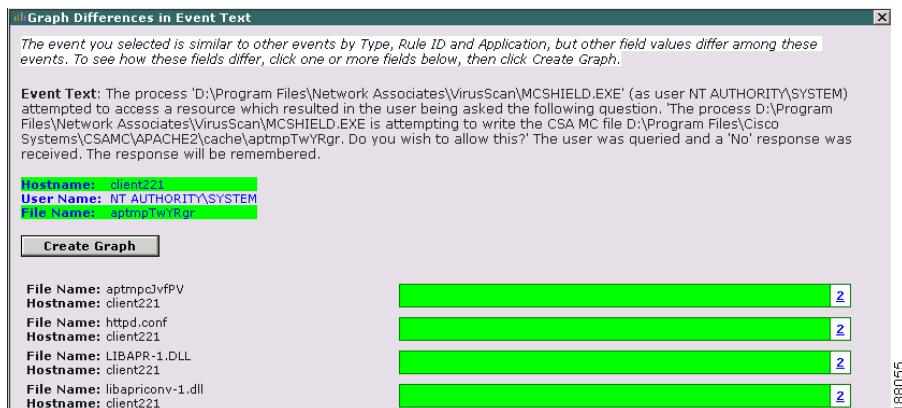
Figure 10-5 Image of rule with highlighted box

Figure 10-5 shows how many different files MCSHIELD attempted to access on host Client221, and how often MCSHIELD attempted to access them.

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.) Release the mouse button. A new browser window opens with the results of the Google search.

Reading Packet Details

CSA MC provides a mechanism which allows you to use “Wireshark” software to translate packets into a readable format. Wireshark is a third-party tool that analyzes protocols and works with WinPcap to analyze packets. Before you can view packet information in readable form, you must first install Wireshark on the same server that runs CSA MC.

To install Wireshark, follow the installation instructions found at <http://www.wireshark.org>. Install the latest released version of Wireshark and the version of WinPcap recommended by Wireshark.

After you have installed Wireshark, 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 10-2](#) 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 Analysis

The Event Analysis tool shows you the applications that are producing the most events and the hosts on which those applications are running.

Viewing Events Using the Event Analysis Filter

Step 1 Log on to the CSA MC with any level of user-privilege. This task can be performed in Simple Mode or Advanced Mode.

Step 2 Move the mouse over **Events** in the menu bar and select **Event Analysis**. The results of the **Default** Event Analysis Filter are displayed.

- The **Most Active Applications** table lists the paths to the applications that have reported the most **Terminate** and **Deny** events.
- Expanding the number in the Hosts column displays a table of Hosts that have reported the most events from the **Most Active Application** row.

- Clicking the number in the Events column opens the Event Log where the events reported by the **Host** and from the **Most Active Application** are listed with boldface type.

Configuring An Event Analysis Filter

-
- Step 1** Log on to the CSA MC with any level of user-privilege. This task can be performed in Simple Mode or Advanced Mode.
- Step 2** Move the mouse over **Events** in the menu bar and select **Event Analysis**. The results of the **Default** Event Analysis Filter are displayed.
- Step 3** Click the change link next to the **Default** event analysis filter.
- Step 4** At the bottom of the Event Analysis Filter page, click **Clone**.
- Step 5** Define the event filter:
- Start date and End date:** 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 specify a relative time using any of the following terms: tomorrow, yesterday, today, now, next, ago, year, month, week, day, hour, minute, and second.
 - You can 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.
 - You can 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 range of severity levels for your filter.
 - Host:** Enter the name of a host in the Host field or click the change link to specify a host or a group of hosts.
 - Policy:** Click the policy box to select a specific policy on which you want to filter.

- **Rule ID:** Enter a specific rule number that you want to search for.
- **Rule action:** Click the change link to specify the kind of action you are searching for. For example, Terminate, Deny, or Allow.
- **Filter text:** Enter a text string to search for. Select Include to include events that contain the text string in your search, select Exclude to exclude events that contain the text string from your search results.
- **Group by:** Choose to group the events by Application or Host.
- Provide a **Name** and short **Description** for this new Event Analysis Filter.
- Select the **Default filter** box if you would like to view this filter first after navigating the Event Analysis page.

Step 6 Click **Save and Apply**. The results of the Event Analysis Filter are displayed on the Event Analysis page.

Event Managing Tasks

The **Event Managing Tasks** 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 Managing Tasks 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 Management Tasks** from the drop-down list that appears.
- Step 2** Click the top bracketed link <**Event Insertion Tasks**> to access the page. See [Figure 10-7](#).

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 10-6](#).

-
- Step 1** Move the mouse over **Events** in the menu bar and select **Event Management Tasks** 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** All conditions in the **Delete Events** area must be met in order for events to be automatically deleted by this event management task. In the Delete Events area configure these settings:
- In the **After** field, specify how old events in the event log can be before they are deleted.
 - In the **Matching the following event set** field, specify the event set of which the events must be a member.
 - In **The database size exceeds** field, specify how large the database must be before events are deleted.
- Step 7** 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 10-6 Event Auto-Pruning

The screenshot shows the 'Management Center for Cisco Security Agents V6.0' interface. The top navigation bar includes links for Home, Advanced, All OSes, and Logout. The main menu has options for Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, and Help. The current page is 'Events > Event Managing Tasks > Configured auto-pruning'. A sub-menu on the right lists 'OTHER EVENT MANAGING TASKS'. The main content area displays a configuration form for 'Configured auto-pruning'. It includes fields for Name (set to 'Configured auto-pruning'), Description (set to 'Prune all events older than 90 days'), Version (set to '6.0 r105'), and a checked checkbox for 'Enabled'. Below this is a 'Delete Events' section containing two conditions: 'After 90 day(s)' and 'Matching the following event set <All Events> [New]'. Another condition 'AND The database size exceeds 3072 MB' is also present. A note at the bottom states 'No deletion recorded so far.' At the bottom of the page are 'Save' and 'Delete' buttons, a status message 'No rule changes pending', a 'Generate rules' button, and a log-in information bar indicating 'Logged in as: admin 187381'.

Event Managing Tasks

Figure 10-7 Event Insertion Task

The screenshot shows the 'Management Center for Cisco Security Agents V6.0' interface. The top navigation bar includes links for Home, Advanced, All OSes, Logout, and other event managing tasks. The main menu has options for Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, and Help. The current page is 'Events > Event Managing Tasks > <Event Insertion Task>'.

Event Count = 12 (suppressed events included)

Level	Description	Count
Information	3 events	3
Notice	0 events	0
Warning	1 event	1
Error	0 events	0
Alert	8 events	8
Critical	0 events	0
Emergency	0 events	0

If total number of events reaches

Threshold	Action
500000	then don't insert new Information level events.
600000	then don't insert new Notice level events.
700000	then don't insert new Warning level events.
800000	then don't insert new Error level events.
900000	then don't insert new Alert level events.
1000000	then don't insert new Critical level events.
<unlimited>	then don't insert new Emergency level events.

Note: 0=unlimited

Buttons at the bottom include Save, No rule changes pending, Generate rules, and Logged in as: admin 18:38:22.

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 Audit 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

When you click the **Wizard** link from an event in the Event Log page, you launch the Event Management Wizard. You can use the Event Management Wizard to accomplish the following tasks:

- **Classify an application.** This allows you to add an application to the White List, Grey List, or Black List. Rules then permit or restrict the application's actions based on the list it is added to. See [Application Trust Levels, page 7-2](#) for a discussion of these lists. See [Using the Event Management Wizard to Set Trust Levels, page 7-3](#) for the procedure to add applications to the White List, Grey List, and Black List using the Event Management Wizard.
- **Create an exception rule to allow an action.** If an action is being denied on an end user systems and you want to allow this action, you can automatically create an “exception” which evaluates the application class and resource information in the event and creates an allow rule which takes precedence over the rule that caused the event. See [Creating Exception Rules, page 10-24](#).
- **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. The following rule types make use of precedence manipulation: File access control, Network access control, Registry access control, COM component access control, and Application control. See [Creating Exception Rules, page 10-24](#).
- **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. See [Perform an Application Behavior Investigation, page 10-33](#).
- **Suppress Similar Events.** “Similar events” have the same rule ID, are of the same event type, and are reported for the same application. For the purpose of grouping similar events, CSA MC ignores the drive letter or share name of the application. See [Event Aggregation and Suppression, page 10-9](#) and [Suppressing Similar Events, page 10-36](#) for more information.
- **Purge similar events from the Event Log.** Use this wizard feature to purge all events similar to the event from which the Wizard link was clicked. This purges all similar events but leaves one, most recent, representative event in the event log. All but one of these events are purged from the Event Log.

About the Event Management Wizard

When administrators in Advanced Mode use the wizard, they have the option of stepping through several configuration screens when performing their task or accepting at once all the choices made by the wizard. Administrators in Simple Mode choose the task they want to perform and then click Finish to accept all the configuration choices made by the wizard.

In most cases, unless you are certain of the behavior that will result from your choices, accept the default choice offered by the wizard when performing your task.

Figure 10-8 Event Management Wizard Link

#	Date	Host	Severity	Action	Event
6	4/22/2008 5:15:45 PM	-	Information	-	Administrator 'admin' logged in from 161.44.181.173 (S3). Wizard
5	4/22/2008 5:01:01 PM	client221	Alert	☒	The process 'D:\WINDOWS\system32\SPOLSV.EXE' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on UDP port 138 to 192.168.232.255 using interface Virtual\VMware Virtual Ethernet Adapter for VMnet8. The operation was denied. Details Rule 409 Wizard
4	4/22/2008 4:59:44 PM	client221	Alert	☒	The process 'D:\WINDOWS\System32\svchost.exe -k netsvc' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 80 to 207.46.211.250 using interface Wired\Intel(R) PRO/1000 MT Desktop Adapter. The operation was denied. Details Rule 409 Wizard
3	4/22/2008 4:59:01 PM	client221	Alert	☒	The process 'D:\Program Files\Google\GoogleToolbarNotifier\1.2.1128.5462\GoogleToolbarNotifier.exe' (as user CLIENT221\Administrator) attempted to initiate a connection as a client on TCP port 80 to 64.233.161.104 using interface Wired\Intel(R) PRO/1000 MT Desktop Adapter. The operation was denied. Details Rule 409 Wizard

No rule changes pending [Generate rules](#) Logged in as: admin 18/387

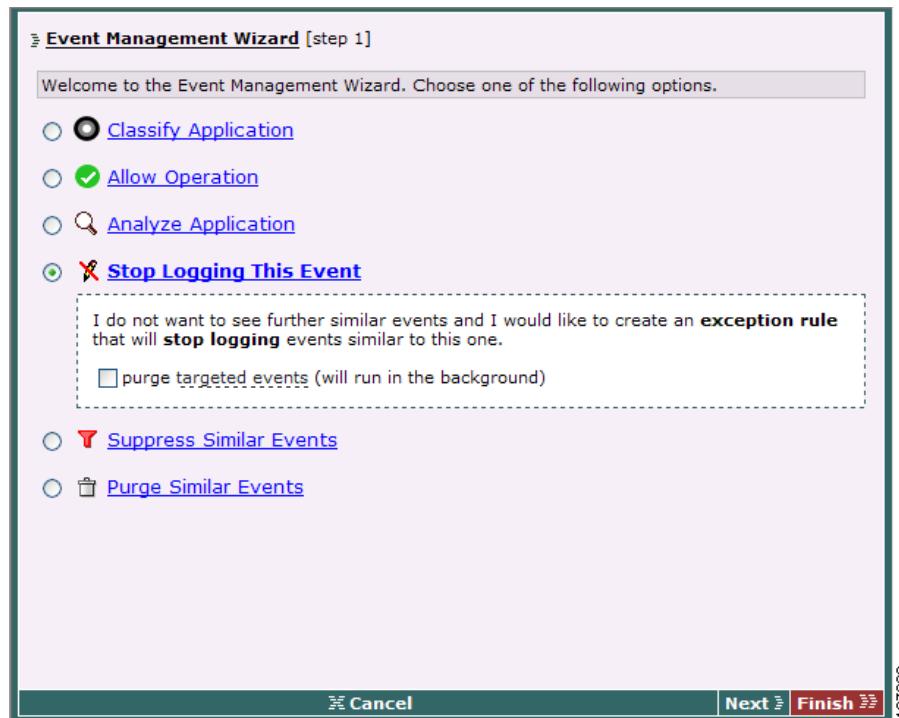
Creating Exception Rules

When you click the **Wizard** link from an event in the Event Log page, you can create an exception rule which will “Allow” an action that was previously “Denied” or stop logging an event. The Event Management Wizard is the tool that creates these exceptions. [Figure 10-9](#) shows the initial page of the Event Management Wizard.

Once the exception rule is created, it is placed in a new rule module, which is attached to the same policy as the rule that triggered the event. The rule module is named, **PolicyName - exceptions** and every subsequent exception for a rule in that policy will be placed in that rule module. If the rule that triggered the event belongs to more than one policy, then an exception is created for every policy to which the rule belongs.

The **PolicyName - exceptions** rule modules are not configurable like other rule modules. All editing of the exceptions must be done in the Exceptions page. Advanced mode users may, however, edit the content of the exception rules.

Figure 10-9 Event Management Wizard



Creating Allow Exception Rules

You can create “Allow” exception rules for the following rule types:

- Application control
- Buffer overflow
- COM component access control
- Data Access Control
- File access control
- Network access control
- Registry access control
- Rootkit/kernel protection
- System API control

To create an exception Allow rule, follow this procedure:

-
- Step 1** Log on to the CSA MC as an administrator with **Configure** privileges. This task may be performed in Simple Mode or Advanced Mode.
- Step 2** From the **Event** menu, select **Event Log**.
- Step 3** Click the Wizard link in the event that denied the action.
- Step 4** In Step 1 of the wizard, select **Allow Operation**.
- Step 5** In the **Justification** field, type an explanation of why you are creating this Allow exception.
- Step 6** (Optional) Select **purge targeted events**.
 - In Simple Mode - If you select **purge targeted events**, all events similar to the one from which you launched the wizard as well as the event from which launched the wizard are purged.
 - In Advanced Mode - If you select **purge targeted events**, and you click **Next**, you have the choice to define what events you want to purge on the next wizard screen.
- Step 7** Click **Next**.
- Step 8** In Step 2 of the wizard, defined the events for which the exception rule will be created and click **Next**.

- Selecting **Take into account all similar events...** will create the exception, and purge the events, for all events similar to the one from which you launched the wizard as well as the event from which you launched the wizard.
- Selecting **Take into account only the current event...** is more restrictive filter and will create the exception, and purge the events, for the event from which you launched the wizard and only for the resources named in that one event.

Step 9 Continue to follow the steps presented by the wizard to create the exception rule and click **Finish** on the last screen.

Unless you are certain of the behavior that will result from your choices, accept the configurations offered by the wizard in order to create the exception rule.

The Allow exception rule is added to a **PolicyName - exceptions** rule module and the module is attached to the policy which includes the originating rule.

The exception is then listed with its policy in the Exceptions page. You can reach that page by mousing-over **Configuration** on the CSA MC menu and selecting **Exceptions**.



Note

If you are working in Advanced Mode you will see all the exceptions that have been made. If you are working in Simple Mode, you will only see the exceptions that have been made to rules, that are in policies, that are visible in Simple Mode.

Step 10 When you are ready to distribute this exception rules to users, you will need to **Generate Rules**.

These are some special use-cases pertaining to “Allow” exception rules:

System API Control/Buffer Overflow:

If the action of the triggering rule is to:

Set - Data payload trust status - as - **untrusted**

the exception rule will not be to “Allow” the action. Instead the exception will:

Set - Data payload trust status - as - **unchanged**

If a payload is marked as both “unchanged” and “untrusted,” the rule marking the payload as “unchanged” takes precedence.

Additionally, if the event is triggered by the “Handle exceptions” or “Access system functions from code executing in data or stack space” sub-rules and a signature was created as a result of the **Set - Data payload trust status - as - untrusted** action, the matching signature (or signatures, if the exception rule is configured to consider “similar events”) will also be purged to prevent Data Access Control rules from denying an action based on an existing signature.

Data Access Control:

This use case is similar to the previously described System API Control/Buffer Overflow use case but describes what happens when the exception is created from the Data Access Control rule (DACL).

“Allow” exceptions to DACLs can be created if the event was triggered because CSA matched a payload with an existing automatically generated signature and the DACL denied the action based on the presence of that signature.

When you attempt to create an “allow” exception for a DACL, the Event Management Wizard does not actually create a DACL exception rule; it will delete the automatically generated signature(s), that matched the payload, thus preventing further deny actions based on an existing signature.

If the corresponding System API Control “Set-data payload trust status-as-untrusted” event and triggering rule are found, the wizard will also create a System API Control exception rule to **Set - data payload trust status - as - unchanged** since the user considers the payload harmless. This prevents further signature generations for that payload.

Rootkit/Kernel Protection:

If the rule that triggered the event was configured with the action to:

Set - detected rootkit trust status - as - untrusted

the exception rule will not be to “Allow” the action. Instead the exception will:

Set - detected rootkit trust status - as - unchanged

If the detected rootkit trust status is marked both “unchanged” and “untrusted,” the rule marking the payload as “unchanged” takes precedence.

Creating Logging Exception Rules

When you create an exception logging rule you create a rule that 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.

See [Rules: Manipulating Precedence, page 5-22](#) for more information on the manipulating precedence feature.

“Stop Log” exceptions can be created for all the rules containing the “Take precedence over other...rules” checkbox, provided that the rule’s action is **not** Set, Monitor, or Add/Remove Process from an application class, and provided that logging is not enabled.

Therefore you cannot create exception logging rules for these rule types:

- Agent UI Control
- NT Event Log
- Syslog Control
- Sniffer and Protocol Detection
- Resource Access Control
- Server Restart

To create a logging exception rule, follow this procedure:

-
- Step 1** Log on to the CSA MC as an administrator with **Configure** privileges. This task may be performed in Simple Mode or Advanced Mode.
- Step 2** From the **Event** menu, select **Event Log**.
- Step 3** Click the **Wizard** link in the event that you want to stop logging.
- Step 4** Select **Stop Logging This Event**.
- Step 5** (Optional) Select **purge targeted events**.
 - In Simple Mode - If you select **purge targeted events**, all events similar to the one from which you launched the wizard as well as the event from which launched the wizard are purged.
 - In Advanced Mode - If you select **purge targeted events**, and you click **Next**, you have the choice to define what events you want to purge on the next wizard screen.
- Step 6** Click **Next**.

Step 7 In Step 2 of the wizard, defined the events for which the exception rule will be created and click **Next**.

- Selecting **Take into account all similar events...** will create the exception, and purge the events, for all events similar to the one from which you launched the wizard as well as the event from which you launched the wizard.
- Selecting **Take into account only the current event...** is more restrictive filter and will create the exception, and purge the events, for the event from which you launched the wizard and only for the resources named in that one event.

Step 8 Continue to follow the steps presented by the wizard to create the exception rule and click **Finish** on the last screen.

Unless you are certain of the behavior that will result from your choices, accept the configurations offered by the wizard in order to create the exception rule.

The logging exception rule is added to a **PolicyName - exceptions** rule module and the module is attached to the policy which includes the originating rule.

The exception is then listed with its policy in the Exceptions page. You can reach that page by mousing-over **Configuration** on the CSA MC menu and selecting **Exceptions**.



Note

If you are working in Advanced Mode you will see all the exceptions that have been made. If you are working in Simple Mode, you will only see the exceptions that have been made to rules, that are in policies, that are visible in Simple Mode.

Step 9 When you are ready to distribute this exception rules to users, you will need to **Generate Rules**.

Configuring Exceptions

The **Exceptions** page lists the policies that contain exceptions to rules. Expanding the policy listing displays the exception rule.

Exception rules are maintained in the policy for which they were created. All exceptions for a particular policy are attached to a special rule module called **PolicyName - exceptions**.

Advanced Mode users will see all the exceptions that have been created. Simple Mode users will see the exceptions that have been created for the policies that are visible in Simple Mode.

Exceptions are created by using the Event Management Wizard. See [Creating Exception Rules, page 10-24](#), [Creating Allow Exception Rules, page 10-25](#), and [Creating Logging Exception Rules, page 10-28](#) for more information on how to create an exception.

Editing Exceptions

Generally speaking, users are expected to accept the configuration choices offered by the wizard in order to create the exception rule. However, even after the exception is created by the wizard, Advanced Mode users can still edit the rule.

This gives the administrator the flexibility of turning on logging or broadening the scope of the exception if it is warranted.

To edit an exception, follow this procedure:

-
- Step 1** Log on to the CSA MC as a user with configure privileges and switch to Advanced Mode.
 - Step 2** From the **Configuration** menu, select **Exceptions**.
 - Step 3** Expand the listed **policies** to show the exceptions made for rules in that policy.
 - Step 4** Click the link to the exception you want to **edit**.
 - Step 5** Edit the rule that is displayed and click **Save**.
 - Step 6** When you are ready to distribute the exception to hosts, **generate rules**.



Note

It is recommended that exceptions can edited through the Exceptions page rather than through the module itself.

Enabling, Disabling, and Deleting Exceptions

-
- Step 1** Log on to the CSA MC as a user with configure privileges. You can perform this task in Simple Mode or Advanced mode, however, if you are working in Advanced Mode you will see all the exceptions that have been made. If you are working in Simple Mode, you will only see the exceptions that have been made to rules that are in policies that are visible in Simple Mode.
- Step 2** From the **Configuration** menu, select **Exceptions**.
- Step 3** Expand the **policies** to show the exceptions made to rules in that policy.
- Step 4** Select the exception you want to enable, disable, or delete.
- Step 5** Click the **Enable**, **Disable**, or **Delete** button at the bottom of the page.
- Step 6** **Generate rules** in order to distribute these changes.

Moving and Copying Exceptions

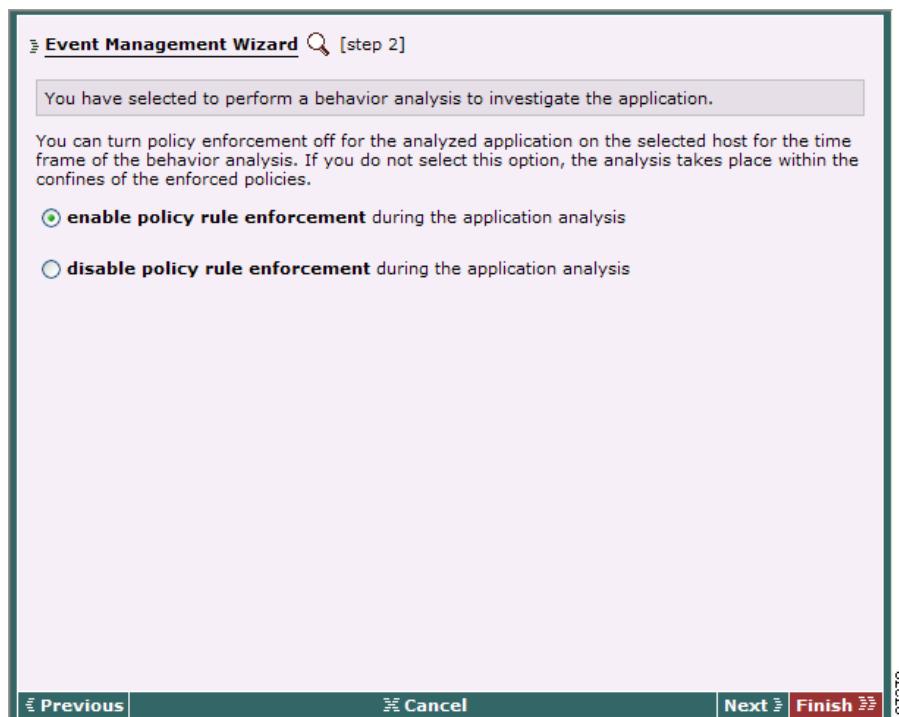
-
- Step 1** Log on to the CSA MC as a user with configure privileges. You can perform this task in Simple Mode or Advanced mode, however, if you are working in Advanced Mode you will see all the exceptions that have been made. If you are working in Simple Mode, you will only see the exceptions that have been made to rules, that are in policies, that are visible in Simple Mode.
- Step 2** From the **Configuration** menu, select **Exceptions**.
- Step 3** Expand the **policies** to show the exceptions made to rules in that policy.
- Step 4** Select the exception you want to move or copy.
- Step 5** Click the **Move** or **Copy** button at the bottom of the page.
- Step 6** Select the policy to which you want to move or copy the file. If you are working in Advanced Mode you may choose from all available policies. If you are working Simple Mode, you may choose from only the policies visible in Simple Mode.
If an exception is moved to a policy it retains its Rule ID. If an exception is copied to another policy, the exception receives a new Rule ID.
- Step 7** **Generate rules** in order to distribute these changes.

Perform an Application Behavior Investigation

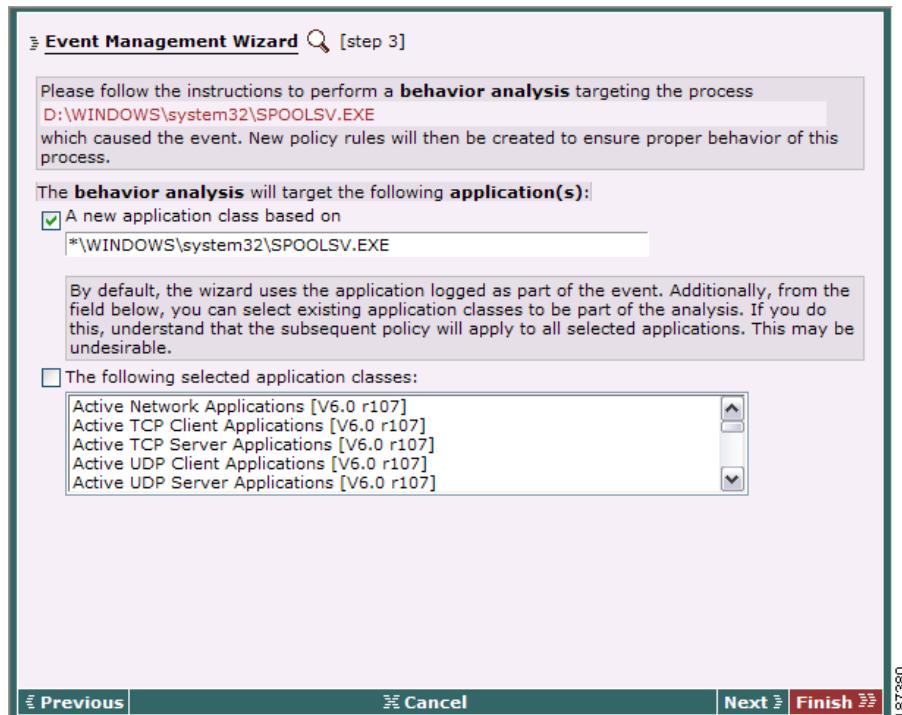
When you click the **Wizard** link from the Event Log page, you can choose to **Analyze Application**, which configures a behavior analysis to investigate the application that triggered the event (see [Figure 10-9](#)). This wizard option is available for users of Advanced Mode only.

If you select Analyze Application, 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** checkbox, 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 10-10 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 10-11 Behavior Analysis Wizard Step 3

The next behavior analysis wizard page (see [Figure 10-11](#)) 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.

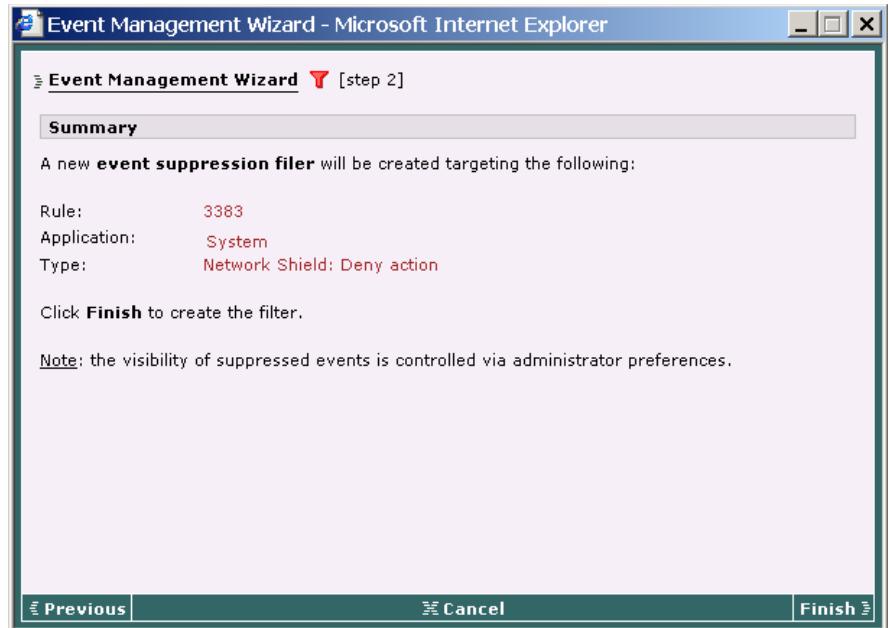
Suppressing Similar Events

When you click the **Wizard** link from the Event Log page, you can choose to **Suppress Similar Events** based on the event from which you click the wizard link (see [Figure 10-9](#)). “Similar events” have the same rule ID, are of the same event type, and are reported for the same application. For the purpose of grouping similar events, CSA MC ignores the drive letter or share name of the application.

Event suppression is best used when you have a reoccurring event that is more noisy than useful to you. This is something you are aware of, but no longer wish to see. Suppressing the event removes all viewable instances of that event and causes further events of the same type to be hidden. Note that these events remain in the database, they are simply not displayed.

Simple Mode users select **Suppress Similar Events** in the Event Management Wizard and then **Finish** to suppress the events.

Advanced Mode users select **Suppress Similar Events** in the Event Management Wizard and can click **Next** to view a summary of the rule type, rule ID, and application for which the event was reported. Clicking **Finish** suppresses the events.

Figure 10-12 Event Suppression Filter Wizard Step 2

Viewing Event Suppression Filters

Once you create the event suppression filter using the Wizard, that filter is viewable from a link in the **Show suppressed events** field at the top of the Event Log page. In [Figure 10-13](#), find the **Show suppressed events: No [2 event suppression filters defined]** link.

Figure 10-13 Show suppressed events link

When you click the **Show suppressed events <#> event suppression filters defined** link, a pop-up window appears from which you can either remove the filter to once again show all the events or purge all the events that have been filtered out. See [Figure 10-14](#).

About the Event Management Wizard

Figure 10-14 Remove Filter or Purge Events Pop-up

Rule	Application	Type	Event Count	Created
<input type="checkbox"/> N/A	N/A	Administrator login successful	18	7/16/2008 11:17:28 PM
<input checked="" type="checkbox"/> Network access control [284] CSA MC Network Security Module [W, V6.0 r185]	\Program Files\Mozilla Firefox\FIREFOX.EXE	Network access control: Deny action	9	7/16/2008 11:17:01 PM

[Remove filter](#) [Purge events](#)

Purge Similar Events

When you click the **Wizard** link from the Event Log page, you can choose to **Purge Similar Events** based on the event from which you click the wizard link (see [Figure 10-9](#)). This purges all similar events but leaves one, most recent, representative event in the event log. All but one of these events are purged from the Event Log. Once purged, they cannot be recovered.

Simple Mode users select **Purge Similar Events** in the Event Management Wizard and then **Finish** to purge the events.

Advanced Mode users select **Purge Similar Events** in the Event Management Wizard and can click **Next** to view a summary of the rule type, rule ID, and application for which the event was reported. Clicking **Finish** purges the events.

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 11, “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 10-15](#)):

- **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.

Event Sets**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 10-15 Event Set Configuration View

The screenshot shows the 'Management Center for Cisco Security Agents V6.0' interface. The top navigation bar includes links for Home, Advanced, All OSes, and Logout. The main menu has options for Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, and Help. The current view is under 'Events > Event Sets > Critical events of all types'.

Name: Critical events of all types

Description: Events with severity levels of Critical or higher

Version: 6.0 r107

Event Specification:

- Include all event types
- Include only the following selected **event types**:
@DYNAMIC: file added
@DYNAMIC: ip address added
Access Control: Notify action
Access Control: Query action
Administrator account created

Severity levels:

- Include all severity levels
- Include only the following selected **severity levels**:
Information
Notice
Warning
Error
Alert
Critical
Emergency

Hosts:

- Include all hosts
- Include only hosts in the following selected **groups**:
<All Linux> [L]
All Linux [L, V6.0 r107]
Desktops [L, V6.0 r105]
Desktops [L, V6.0 r107]
Servers [L, V6.0 r105]

Rule modules:

- Include all policy rules
- Include only rules in the following selected **rule modules**:
Base - CSA client UI control (Linux) [U, V6.0 r107]
Base - CSA service control (Linux) [U, V6.0 r107]

Buttons at the bottom: Save, View, Purge events, Delete, No rule changes pending, Generate rules, Logged in as: admin, and a reference number 18788.

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 “csamc60dsn.”

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 10-48](#) 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 10-1](#).)

Table 10-1 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. (An Audit Mode event is preceded by the string “AUDITMODE”.)
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, SNMP, Log to file, Named pipes and a Custom program that you provide.

Each alert type requires you to enter specific information. See [Table 10-2](#) 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 10-16](#)), 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, SNMP, Log, Named pipe, Custom (for alert configuration information, refer to [Table 10-2](#)).

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.

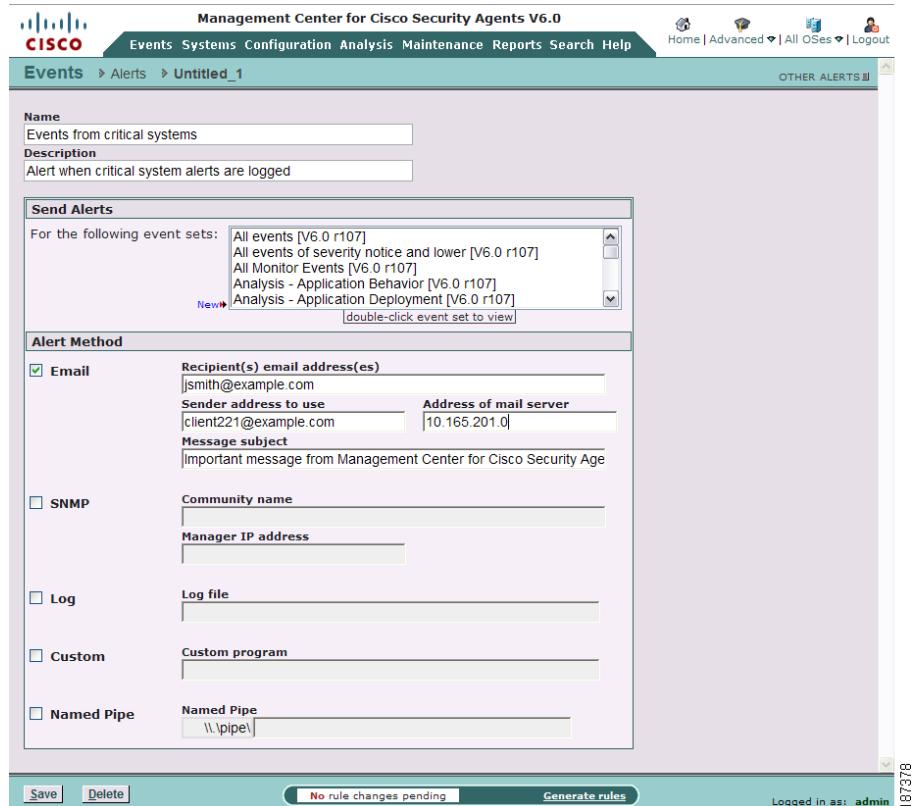
Figure 10-16 Alert Configuration View

Table 10-2 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.
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.) Refer to the CSAMC-SNMPv2.mib document in the CSAMC\CSAMC60\doc directory for SNMP-MIB definitions for Cisco specific objects. Also see Third Party Access to Events, page 10-43 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. c:\alerts\logfile.txt This file can then be used by third party event management applications. See Third Party Access to Events, page 10-43 for details. *In a distributed configuration, the path must correspond to the polling server system.

Alert Type	Information	Description
Custom	Custom Program	<p>Enter a custom alert program name here.</p> <p>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.</p> <p>Your custom program must be an executable file. c :\Program Files\Cisco\CSAMC\CSAMC60\program.exe</p> <p>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.</p> <p>FEATURE NOTES:</p> <ul style="list-style-type: none"> * The custom program must exist on the same system as CSA MC in the CSAMC60 directory or subdirectory. *Custom programs cannot require any user input. *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.) *In a distributed configuration, the path must correspond to the polling server system.
Named Pipe	Named Pipe	<p>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.</p> <p>Note that this feature is for use with third party vendors that support alerts over Windows named pipes.</p>

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 10-16](#)), 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. The third party application that consumes the log files is expected to manage the deletion and archiving of these files once processing is complete.



Note

This file data is encoded in UTF-8 format.



CHAPTER 11

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 11-2](#)
- [Viewing Reports, page 11-2](#)
- [Generating Reports, page 11-3](#)
 - [Events by Severity, page 11-3](#)
 - [Events by Group, page 11-5](#)
 - [Host Detail, page 11-6](#)
 - [Policy Detail, page 11-7](#)
 - [Group Detail, page 11-8](#)
 - [Clam AntiVirus Reports, page 11-9](#)
 - [Data Loss Prevention Reports, page 11-14](#)
 - [Signature Information Detail, page 11-19](#)

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.

- PDF: This option will generate the complete report as a PDF file that can be viewed, printed, and saved using the browser PDF plug-in. If you do not have a PDF plug-in installed on your browser, you will have to install a PDF browser plug-in to view this report type.
- HTML: This option breaks the report into individual HTML pages which can be viewed one page at a time in a browser window. Only the currently viewed report page can be printed. (Supported by Internet Explorer 6.0 or higher and FireFox 1.5.0.x or 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.

**Caution**

When you print reports, it is recommended that you print using Landscape mode. Reports do not print correctly using Portrait mode.

**Caution**

CSA MC requires and installs Sun JRE (Java Runtime Environment) to generate reports using the Jasper reporting tool. If you remove the Java directory from the CSA MC system, you cannot generate reports.

Generating Reports

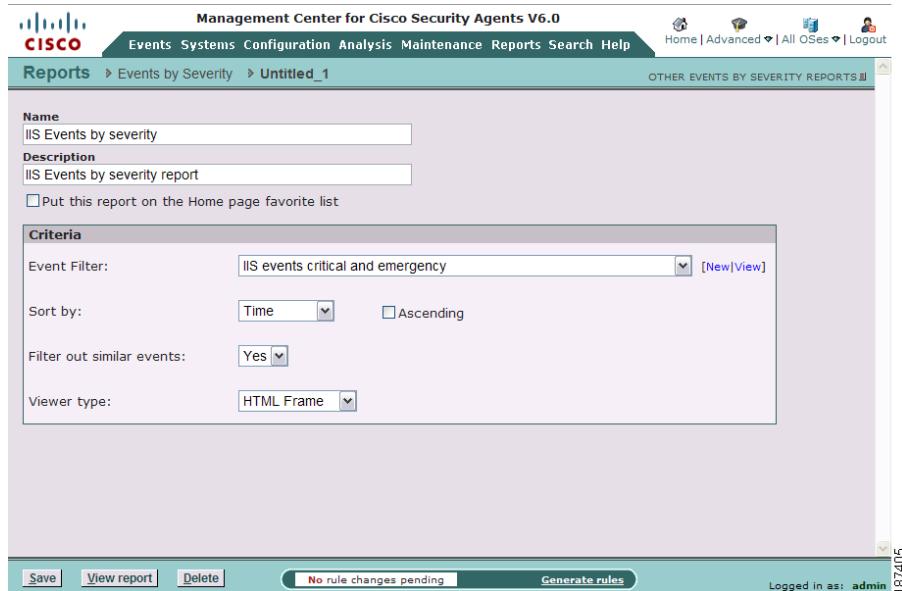
You generate reports by selecting various sorting options in the CSA MC report configuration views. When you are finished selecting sorting parameters, you can generate your report.

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 10-39](#)).
 - Step 5** From the **Sort by** pulldown list, select a parameter for sorting this report's contents (see [Figure 11-1](#)).
 - 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**, PDF or HTML.
 - 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.

Figure 11-1 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.

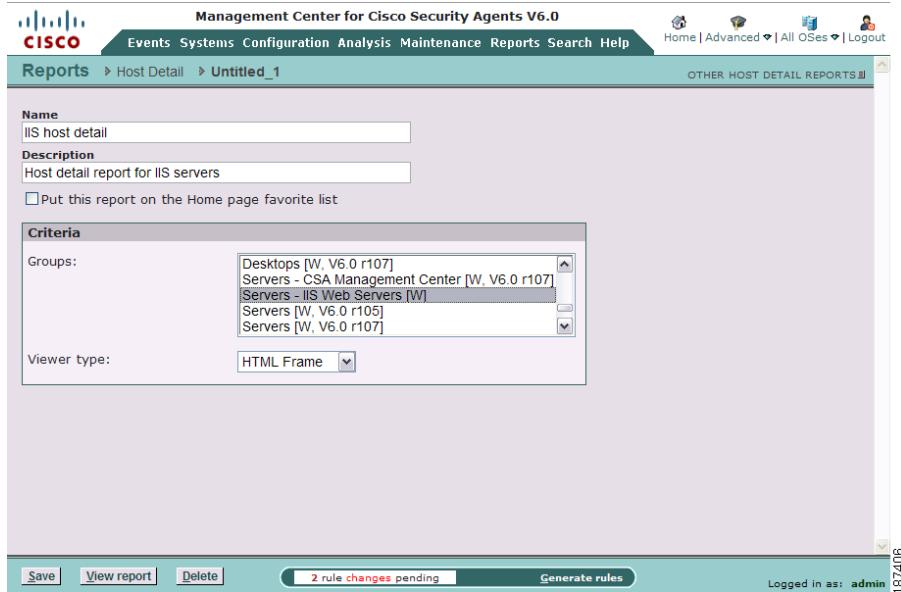
-
- Step 1** Move the mouse over **Reports** in the menu bar of CSA MC. Select **Events by Group** from the drop-down list that appears. Any existing reports are shown.
 - Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
 - Step 3** In the Events by 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 10-39](#)).
 - 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**, PDF or HTML.
 - 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.

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 11-2](#)), 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** Select a **Viewer type**, PDF or HTML.
 - 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 11-2 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** Select a **Viewer type**, PDF or HTML.
- 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 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** Select a **Viewer type**, PDF or HTML.
 - 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 window.

Clam AntiVirus Reports

These reports provide information about the age of signature files on hosts and the number of infected hosts in the deployment. These are the AntiVirus reports available:

- AntiVirus Update
- AntiVirus Summary
- Restored Infection Details
- Virus Infections
- Virus Infections Details

Creating an AntiVirus Update Detail Report

This report shows how old signature files are on hosts in a group. The bar chart breaks down the number of hosts using signatures that are older than X days.

Some reports are provided by default. If you would like to create your own report, follow this procedure:

-
- Step 1** From the **Reports** menu, navigate **AntiVirus > AntiVirus Update**.
- Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
- Step 3** Enter a **Name** and a short **Description** of the report.
- Step 4** If you want this report to appear on the CSA MC Home page, select **Put this report on the Home page favorite list**.
- Step 5** In the Criteria area, select a **Host Filter** from the drop down menu. The report will include all the hosts described by the selection in the Host Filter drop down menu. Only one Host Filter can be applied to one report.
- Step 6** In the Group Filter area, select one of these two radio buttons:
- **No Group Filter** - if you do not want to restrict your reports to hosts in certain groups.
 - **Groups Matching** - if you do want to restrict your report to hosts in certain groups. You may pick one or more groups from the Groups Matching menu.
- Step 7** From the **Sort by AV Update Date** menu select ascending or descending.

- Step 8** In the Viewer type menu, select PDF or HTML output. See the “[Viewing Reports](#)” section on page 11-2 for information more information about PDF and HTML output choices.
- Step 9** Click one of these buttons:
- **Save** to be able to view this report in the future.
 - **View Report** to view the report immediately, whether it is saved or not.

Creating an AntiVirus Summary Report

This report can identify the most frequently occurring virus infections and the most infected hosts in your enterprise. The **Top 10 Infected Hosts** and the **Top 10 Virus Infections** reports are provided by default. To create your own report, follow this procedure:

-
- Step 1** From the **Reports** menu, navigate **AntiVirus > AntiVirus Summary**.
- Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
- Step 3** Enter a **Name** and a short **Description** of the report.
- Step 4** If you want this report to appear on the CSA MC Home page, select **Put this report on the Home page favorite list**.
- Step 5** From the **Report type** list box, select the kind of report you want to create.
- Step 6** In the **Groups matching** field, select the group, or groups, which you want to include in this report.
- Step 7** Specify the time frame for the report by entering the **From** and **Until** parameters in the **Time Frame** area. Alternatively, you may check **All times** if you want a report of all virus infections ever recorded.

You can specify the **From** and **Until** parameters in these ways:

- 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.
- You can 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.

- You can 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.
- Step 8** In the **Viewer type** menu, select **PDF** or **HTML** output. See the “[Viewing Reports](#)” section on page 11-2 for information more information about PDF and HTML output choices.
- Step 9** Click one of these buttons:
- **Save** to be able to view this report in the future
 - **View Report** to view the report immediately, whether it is saved or not.

Creating a Restored Infection Details Report

This report provides administrators with a list of files which have been tagged with signature-based or behavior-based AntiVirus tags but that users have chosen to remove from quarantine through their local agent interface. This report allows an administrator to identify trends in these restored files. For example, if the same file is being restored by many users in one particular group, then an exception may be warranted for this file.

The report identifies the name of the virus that was found, the file that was restored, the user that restored the file, the host on which the file was restored, and the time at which the file was restored.

To create a Restored Infection Details report, follow this procedure:

-
- Step 1** From the **Reports** menu, navigate **AntiVirus > Restored Infection Details**.
- Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
- Step 3** Enter a **Name** and a short **Description** of the report.
- Step 4** If you want this report to appear on the CSA MC Home page, select **Put this report on the Home page favorite list**.
- Step 5** In the **Groups matching** field, select the group, or groups, which you want to include in this report.
- Step 6** Specify the time frame for the report by entering the **From** and **Until** parameters in the **Time Frame** area. Alternatively, you may check **All times** if you want a report of all virus infections ever recorded.

You can specify the **From** and **Until** parameters in these ways:

- 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.
- You can 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.
- You can 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.

- Step 7** In the **Viewer type** menu, select **PDF** or **HTML** output. See the “[Viewing Reports](#)” section on page 11-2 for information more information about PDF and HTML output choices.
- Step 8** Click one of these buttons:
- **Save** to be able to view this report in the future
 - **View Report** to view the report immediately, whether it is saved or not.

Creating Virus Infections Reports

The **Virus Infections report** graphically displays the number of infected files found on a host. You can configure the report to sort the information by tag or by host.

The information in the report is based on the events passed from the agents to the CSA MC when the agents last polled. The information from the latest polling event overwrites the information from the previous polling event.

Some Virus Infections reports are provided by default. To create your own Virus Infections report, follow this procedure:

-
- Step 1** From the **Reports** menu, navigate **AntiVirus > Virus Infections**.
- Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
- Step 3** Enter a **Name** and a short **Description** of the report.
- Step 4** If you want this report to appear on the CSA MC Home page, select **Put this report on the Home page favorite list**.

- Step 5** In the **Groups matching** field, select the group, or groups, which you want to include in this report.
- Step 6** If you know the name of the virus you want to search for, enter it in the **Virus Name** field, otherwise leave the * entry to search for all viruses.
- Step 7** You can choose to group the report output by **Host Name** or **Virus Name** by selecting one or the other in the **Group by** field.
- Step 8** In the Viewer type menu, select PDF or HTML output. See the “[Viewing Reports](#)” section on page 11-2 for information more information about PDF and HTML output choices.
- Step 9** Select **Order by number of infections** if you would like the report presenting the viruses with the highest number of occurrences first.
- Step 10** Click one of these buttons:
- **Save** to view this report in the future.
 - **View Report** to view the report immediately, whether it is saved or not.

Creating Virus Infections Details Reports

The **Virus Infection Details** report lists the locations of infected files. The information in the report is derived from events, generated by a scan event log rule that is set to “monitor” or “notify.” These events are collected by the CSA MC. This information can be sorted by host or by virus.

Some Virus Infections Details reports are provided by default. To create your own Virus Infections Details report, follow this procedure:

-
- Step 1** From the **Reports** menu, navigate **AntiVirus > Virus Infection Details**.
- Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
- Step 3** Enter a **Name** and a short **Description** of the report.
- Step 4** If you want this report to appear on the CSA MC Home page, select **Put this report on the Home page favorite list**.
- Step 5** In the **Groups matching** field, select the group, or groups, which you want to include in this report.
- Step 6** If you know the name of the virus you want to search for, enter it in the **Virus Name** field, otherwise leave the * entry to search for all viruses.

Step 7 Specify the time frame for the report by entering the **From** and **Until** parameters in the Time Frame area. Alternatively, you may check **All times** if you want a report of all virus infections ever recorded.

You can specify the **From** and **Until** parameters in these ways:

- 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.
- You can 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.
- You can 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.

Step 8 You can choose to group the report output by **Host Name** or **Virus Name** by selecting one or the other in the **Group by** field.

Step 9 In the **Viewer type** menu, select PDF or HTML output. See the “[Viewing Reports](#)” section on page 11-2 for information more information about PDF and HTML output choices.

Step 10 Click one of these buttons:

- **Save** to be able to view this report in the future
- **View Report** to view the report immediately, whether it is saved or not.

Data Loss Prevention Reports

Data Loss Prevention reports can be generated for any host that is running a data loss prevention policy. To use this policy, the CSA MC has to have an available data loss prevention license for that host.

These procedures create reports describing files that have been tagged with scanning data tags or static data tags.

- [Creating Data Discovery Reports, page 11-15](#)
- [Creating a Data Justification Details Report, page 11-16](#)
- [Creating a Protected Data Movement Report, page 11-17](#)

Creating Data Discovery Reports

The Data Discovery report graphically displays the number of files, with a particular scanning data tag or static data tag, found on the fixed local drives of a host. You can configure the report to sort the information by tag or by host.

The information in the report is based on the events passed from the agents to the CSA MC when the agents last polled. The information from the latest polling event overwrites the information from the previous polling event.

Reports for Credit card and SSN information and Sensitive data details are provided for you by default.

To create a Data Discovery report, follow this procedure:

-
- Step 1** From the **Reports** menu, navigate **Data Loss Prevention > Data Discovery**.
 - Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
 - Step 3** Enter a **Name** and a short **Description** of the report.
 - Step 4** If you want this report to appear on the CSA MC Home page, select **Put this report on the Home page favorite list**.
 - Step 5** In the **Groups matching** field, select the group which you want to include in this report. You may choose more than one group. You may also choose <All Groups>.
 - Step 6** In the **Tags matching** field, select the tag, or tags, for which you want to create a report. You may also choose <All tags>.
 - Step 7** Choose to group the report output by **Host Name** or **Tag Name** by selecting one of those items from the **Group by** field. If you select **Host Name**, the report displays one pie chart, per host, per report page. The name of the data tags and the number of files with that tag are listed below the chart. If you select **Tag Name**, the report is a bar chart indicating the tag and the number of files with that tag. The host name and number of files with that tag are listed below the chart.
 - Step 8** In the **Viewer type menu**, select **PDF** or **HTML** output. See the “[Viewing Reports](#)” section on page 11-2 for information more information about PDF and HTML output choices.
 - Step 9** Select **Order by number of tags** if you would like the report presenting the tags with the highest number of occurrences first.
 - Step 10** Click one of these buttons:

- **Save** to view this report whenever you want.
- **View Report** to view the report immediately, whether it is saved or not.

Creating a Data Justification Details Report

The **Data Justification Details report** reports the explanations users provide when acting on files tagged with scanning data tags or static data tags.

Data Justification Details reports can be generated for any host that is running a data loss prevention policy and that is using at least one scan event log rule that queries or notifies the user and asks for a justification of their action. The host must also have a data loss prevention license assigned to it.

The Data Justification Details report lists the date of the justification, the username that was prompted for the justification, the application that was acting, the file on which the application was acting, and the justification message if one was provided.



Note If a host is part of a group which is configured to filter user info from events, the username will not appear in the report.

To create a Data Justification Details report, follow this procedure:

-
- Step 1** From the Reports menu, navigate **Data Loss Prevention > Data Justification Details**.
 - Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
 - Step 3** Enter a **Name** and a short **Description** of the report.
 - Step 4** If you want this report to appear on the CSA MC Home page, select **Put this report on the Home page favorite list**.
 - Step 5** In the **Groups matching** field, select the group which you want to include in this report. You may select more than one group. You may also choose <All Groups>.
 - Step 6** In the **Tags matching** field, select the tag, or tags, for which you want to create a report. You may also choose <All tags>.

- Step 7** Specify the time frame for the report by entering the **From** and **Until** parameters in the **Time Frame** area. Alternatively, you may check All times if you want a report of covering all available data. You can specify the From and Until parameters in these ways:
- 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.
 - You can 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.
 - You can 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.
- Step 8** Choose to group the report output by **Host Name** or **Tag Name** by selecting one of those items from the Group by field. If you select Host Name, the report lists the directory locations of tagged files grouped by host and then by tag. If you select Tag Name, the report lists the directory locations of the tagged files grouped by tag and then by host.
- Step 9** In the Viewer type menu, select **PDF** or **HTML** output. See the “[Viewing Reports](#)” section on page 11-2 for information more information about PDF and HTML output choices.
- Step 10** Click one of these buttons:
- **Save** to view this report in the future.
 - **View Report** to view the report immediately, whether it is saved or not.

Creating a Protected Data Movement Report

Protected Data Movement reports gather information generated by monitoring events and notification events of Scan Event Log Rules (SACLs). These events are triggered if the SACL detects a user performing a file operation on a file with a data loss prevention tag.

The Protected Data Movement report shows which files, with data tags, were accessed. This report can be sorted by host or by tag name.

Protected Data Movement reports can be generated for any host that is running the Data Loss Prevention policy and that is using at least one scan event log rule that monitors events or notifies the user of file movement.

To create a Protected Data Movement report, follow this procedure:

-
- Step 1** From the Reports menu, navigate **Data Loss Prevention > Data Discovery Details**.
- Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
- Step 3** Enter a **Name** and a short **Description** of the report.
- Step 4** If you want this report to appear on the CSA MC Home page, select **Put this report on the Home page** favorite list.
- Step 5** In the **Groups matching** field, select the group which you want to include in this report. You may choose more than one group. You may also choose <All Groups>.
- Step 6** In the **Tags matching** field, select the tag, or tags, for which you want to create a report. You may also choose <All tags>.
- Step 7** Specify the time frame for the report by entering the **From** and **Until** parameters in the **Time Frame** area. Alternatively, you may check **All times** if you want a report of all virus infections ever recorded. You can specify the From and Until parameters in these ways:
- 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.
 - You can 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.
 - You can 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.
- Step 8** Choose to group the report output by **Host Name** or **Tag Name** by selecting one of those items from the Group by field. If you select Host Name, the report lists the directory locations of tagged files grouped by host and then by tag. If you select Tag Name, the report lists the directory locations of the tagged files grouped by tag and then by host.

Step 9 Select a Viewer type, **PDF** or **HTML**.

Step 10 Click one of these buttons:

- **Save** to be able to view this report in the future.
- **View Report** to view the report immediately, whether it is saved or not.

Signature Information Detail

You can generate reports related to the automatic signature generation feature. Signature reports provide in-depth information on these signature details:

- [Denial of Service Detail](#)
- [Filtering Detail](#)
- [Generation Detail](#)

Denial of Service Detail

Denial of service (DoS) detail reports the number of times payloads have been associated with the @highrisk_signatures token.

To generate a DoS detail report, do the following:

Step 1 Move the mouse over **Reports** in the menu bar and navigate **Signatures>Denial of Service**.

Step 2 Click the **New** button to create a new report. This takes you to the configuration view.

Step 3 In the Denial of Service Detail report configuration view, enter a **Name** and a **Description** for the report.

Step 4 In the **Time Frame** area, specify the time period that the report should address in the **From** and **Until** fields. 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 specify a relative time using any of the following terms: tomorrow, yesterday, today, now, next, ago, year, month, week, day, hour, minute, and second.

- You can 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.
- You can 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.

- Step 5** In the **Viewer Type** field select the format in which you want to display the report, HTML or PDF.
- 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 window.

Filtering Detail

Filter Detail reports describe the number of times CSA acted as a result of a matching an attack payload to an existing signature.

To generate a Filtering Detail report, do the following:

-
- Step 1** Move the mouse over **Reports** in the menu bar and navigate **Signatures>Filtering Detail**.
- Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
- Step 3** In the Filtering Detail report configuration view, enter a **Name** and a **Description** for the report.
- Step 4** Select an **Event Filter** from the drop down menu list.
- 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** Choose whether or not to remove similar events from the report by choosing Yes or No in the **Filter out Similar Events** field.

Step 8 In the **Time Frame** area, specify the time period that the report should address in the **From** and **Until** fields. 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 specify a relative time using any of the following terms: tomorrow, yesterday, today, now, next, ago, year, month, week, day, hour, minute, and second.
- You can 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.
- You can 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.

Or you can select **All times** checkbox if you do not want to limit the time frame of the report.

Step 9 Select a **Viewer type**, PDF or HTML.

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. Your report is created and is automatically displayed in a new window.

Generation Detail

Generation Detail reports describe the number of times CSA correlated a signature.

To generate a Generation Detail report, do the following:

Step 1 Move the mouse over **Reports** in the menu bar and navigate **Signatures>Generation Detail**.

Step 2 Click the **New** button to create a new report. This takes you to the configuration view.

Step 3 In the Generation Detail report configuration view, enter a **Name** and a **Description** for the report.

Step 4 In the **Signature Type** field select Local or Global.

Step 5 For Global signature generation details provide a **Correlation start time** and **Correlation end time**. 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 specify a relative time using any of the following terms: tomorrow, yesterday, today, now, next, ago, year, month, week, day, hour, minute, and second.
- You can 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.
- You can 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.

Step 6 In the **Sort by Sig update time** field, select Ascending or Descending.

Step 7 Select a **Viewer type**, PDF or HTML.

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. Your report is created and is automatically displayed in a new window.



12

CHAPTER

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 12-2](#)
- [Start and Stop Agent Service, page 12-2](#)
- [Backing Up Configurations, page 12-3](#)
- [Restoring Backup Configurations, page 12-6](#)
- [Database Maintenance \(Free Up Disk Space on CSA MC\), page 12-8](#)
- [Using the Webmgr Utility, page 12-10](#)
- [Using the COM Extract Utility, page 12-11](#)
- [Manual Agent Data Filter Installation, page 12-11
 - \[Internet Information Services Installation for Windows Vista, page 12-12\]\(#\)
 - \[Install Data Filter on Windows, page 12-13\]\(#\)
 - \[Uninstall Data Filter on Windows, page 12-13\]\(#\)](#)

Start and Stop Server Service

- [Install Data Filter on Linux, page 12-14](#)
- [Uninstall Data Filter on Linux, page 12-15](#)
- [Install Data Filter on Solaris, page 12-16](#)
- [Uninstall Data Filter on Solaris, page 12-16](#)
- [Exporting and Importing Configurations, page 12-17](#)
 - [Exporting Configurations, page 12-17](#)
 - [Importing Configurations, page 12-19](#)
 - [View Import History, page 12-21](#)
- [Cisco Security Agent Posture Plug-in for CTA, page 12-22](#)

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:

From the CSA MC /bin directory, run the following:

To stop the service:

```
csicontrol.exe -c end -t s -a <login name> -p <password>
```

To start the service

```
csicontrol.exe -c start -t s -a <login name> -p <password>
```

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 csagent  
net start csagent
```

**Note**

On Windows Vista desktops, standard users must elevate their privileges to “administrator” in order to run these commands.

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 6-3](#).

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**

Specifically, it is recommended that you backup all necessary files, at least once a week (e.g. auto-backup on Monday at 1 AM), to a safe, remote, and unique location for each backup. This way, previously backed up files are not overwritten by new ones.

**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.

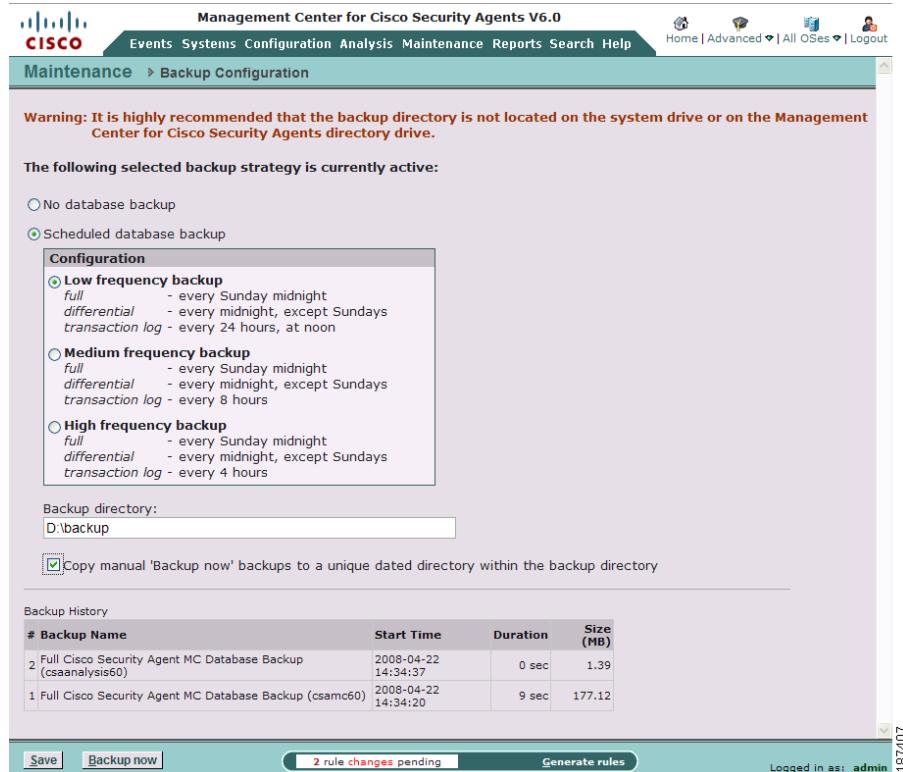
differential—This type of backup occurs every night at midnight (except Sunday nights when a full backup occurs). A differential backup includes only data that has changed since the last backup (full or differential) occurred.

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.

**Note**

When you configure a scheduled database backup and click **Save**, an initial backup is performed immediately.

Figure 12-1 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

■ Restoring Backup Configurations

- 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

Step 3 Optionally, click the **Copy manual 'Backup now' backups to a unique dated directory within the backup directory** checkbox. With this checkbox selected, when you click the Backup now button (only when you manually click the Backup now button), the backup file is saved to the specified directory and a copy is saved to a unique directory.

Restoring Backup Configurations

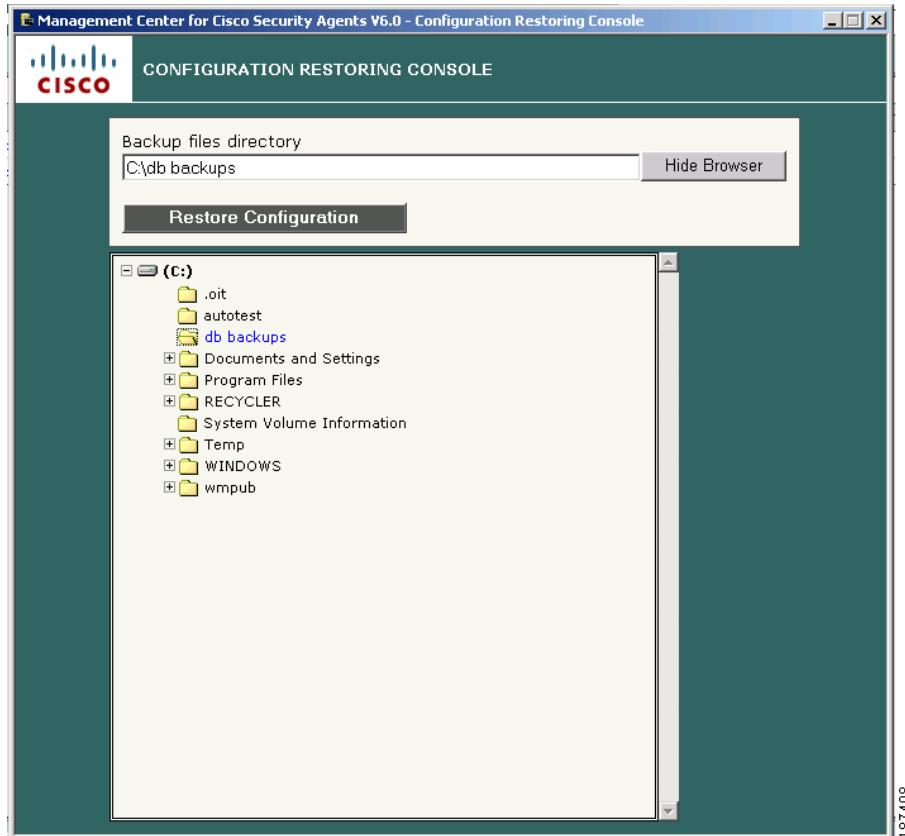
Restore backup CSA MC configurations, including database, license information, and transaction logs by running the Restore utility, called **Restore Configuration**, located in the default CSAMC60\bin directory:



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 CSAMC\CSAMC60\bin directory) to display the CSA MC restore user interface. See [Figure 12-2](#).
- Step 2** Enter or browse to the directory path where the backup files are stored.

Figure 12-2 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. CSA MC provides maintenance recommendations for each database listed on the database menu page.

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 csamc60

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 csamc60. 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.

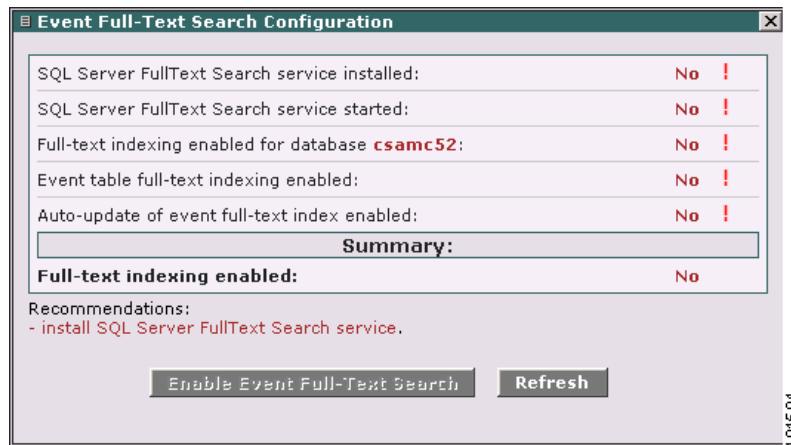
Note that **Transaction log size** is also displayed here. SQL Server 2005 breaks that out as a separate category when calculating the database size.

The **Event full-text search** function is present here and disabled by default. (See [Figure 12-3](#).) Enabling this feature allows you to utilize the SQL Server full-text search function. If this feature is disabled and you perform an event text-filtering search, when it completes, we will warn you that you can enable this feature to perform a full-text search. NOTE that full-text search configuration changes can only be performed if the db user is part of the db_owner fixed database role (for remote db this is not required). If the full-text enabling/disabling fails, you will see a message advising you to adjust the db user rights or run the operation from the command line.

**Note**

Full-text searching is an optional component of SQL Server. When installed, it offers additional string querying abilities such as string comparisons similar to internet search engines, returning both results and a matching score or weight. Without full-text searching, string matching is usually limited to an exact match, or a wildcard match. Full-text searching allows for searching for phrases, groups of words, words near one another, or different tenses of words.

Figure 12-3 Event Full-Text Search Function Window

**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 csamc60`).

Using the Webmgr Utility

Use the `webmgr` (webmanager) command to add a new administrator with monitoring rights to the CSA MC database without accessing the user interface. Running `webmgr` also lets you unblock an existing administrator and reset their password. You would want to do this in cases where an administrator is locked out of the MC due to too many invalid login attempts (25 invalid login attempts allowed before administrator blocking occurs).

Using this utility, you can also log out all currently logged in administrators, effective immediately. This is useful if the server has reached the maximum number of administrators that can be logged in at once (20 admins can be logged in to the MC at the same time).

From a command prompt window, run `webmgr` from the `CSAMC\CSAMC60\bin` directory. It displays the syntax required to make the administrator changes described above.

- Add a new administrator by entering the new name and new password followed by your existing user name and password, as follows:

```
webmgr newuser NAME PASSWORD DESCRIPTION  
EXISTINGNAME EXISTINGPASSWORD
```



Note If you have spaces in the description part of your entry, you must put quotation marks around the entire description phrase.

- Unblock an existing administrator (resetting the password) by entering data in the following manner:

```
webmgr unblock NAME OLDPASSWORD NEWPASSWORD
```

- Log out all currently logged in administrators:

```
webmgr clearsessions
```

Using the COM Extract Utility

CSA MC provides a COM component extraction utility on agent systems, 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 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\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\CSAgent\bin>extract_com foo.txt
```

The agent creates the "foo.txt" file in the current directory. In this example, that would be `..\Cisco\CSAgent\bin\foo.txt`. 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 9-4](#).

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 For Windows Vista, if you want to install Internet Information Services (IIS), you need to make sure that the **IIS Metabase and IIS 6 configuration compatibility** and **ISAPI Filters** features are included in the installation. See [Internet Information Services Installation for Windows Vista](#) for instructions.



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 servers for Solaris and 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.

Internet Information Services Installation for Windows Vista

Follow this procedure to install IIS on Windows Vista so that data access control rules will be supported

-
- Step 1** From the Vista Start menu, navigate **Control Panel > Programs and Features**.
 - Step 2** In the Tasks column, click **Turn Windows features on or off**.
 - Step 3** In the Windows Features dialog box, select the **Internet Information Services feature** and expand the feature tree.
 - Step 4** Expand the **Web Management Tools** tree.
 - Step 5** Expand the **IIS 6 Management Compatibility** tree.
 - Step 6** Select **IIS Metabase and IIS 6 configuration compatibility**.
 - Step 7** Expand the **World Wide Web Services** tree.
 - Step 8** Expand the **Application Development Features** tree.
 - Step 9** Select **ISAPI Filters**.
 - Step 10** Click **OK**.

Step 11 If you installed IIS after you install the Cisco Security Agent, you must manually install the Cisco Security Agent data filter in order to use Data access control rules on the system in question. See, [Install Data Filter on Windows](#) for that procedure.

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 Linux

For every HTTP server running on a Linux computer, to which you want to restrict access to web pages using data access control rules, the computer must have the following software installed, in this order:

1. httpd-devel rpm
2. Cisco Security Agent
3. csa_apache_conf

Determine if httpd-devel rpm is installed on your server

- Step 1** Log on to the Linux server.
- Step 2** Open a terminal window.
- Step 3** At the prompt, enter: `rpm -qa|grep http`
- Step 4** If you do not have an `httpd-devel` rpm installed on your server, install it before proceeding. Note that the `httpd-devel` rpm version must match the `httpd-devel` daemon.

Install Cisco Security Agent

Install a Cisco Security Agent agent kit for Linux servers. At the end of the agent installation, you will receive this message:

If this system is running a web server, the csa service module must be installed. Execute `/opt/CSCOcsa/app_plugins/apache/i.csafilter` to copy the module and modify the `httpd-configuration` appropriately. The web server will be restarted automatically.

Install the csa_apache conf module

-
- Step 1** Log on to the server as **root**.
 - Step 2** Open a terminal window.
 - Step 3** Change the directory to `/opt/CSCOcsa/app_plugins/apache`
 - Step 4** At the prompt, run the `i.csafilter` shell script with the `install` command. For example: `sh i.csafilter install`
 - Step 5** When prompted, enter the path of the Apache root directory. This value is passed to the `csa_apache_conf` script which installs the CSA Apache module in the same location as the other Apache modules.

**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 Linux

-
- Step 1** Log on to the server as **root**.
 - Step 2** Open a terminal window.
 - Step 3** Change the directory to `/opt/CSCOcsa/app_plugins/apache`
 - Step 4** At the prompt, run the `i.csafilter` shell script with the `remove` command. For example: `sh i.csafilter remove`

[output:]

```
CSA web server filter removal:  
Should I uninstall filters for Apache [No] y  
Enter the path of the Apache root (null for none):  
webserver:root>
```

Install Data Filter on Solaris

-
- Step 1** Log on to the server as **root**.
 - Step 2** Open a terminal window.
 - Step 3** Change the directory to `/opt/CSCOcsa/drv`
 - Step 4** At the prompt, run the `i.csafilter` shell script with the `install` command. For example: `./i.csafilter install`

[output:]

```
CSA web server filter installation:  
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.
-

Uninstall Data Filter on Solaris

-
- Step 1** Log on to the server as **root**.
 - Step 2** Open a terminal window.
 - Step 3** Change the directory to `/opt/CSCOcsa/drv`
- At the prompt, run the `i.csafilter` shell script with the `remove` command. For example: `./i.csafilter remove`

[output:]

```
SA web server filter removal:  
Should I uninstall filters for Apache [No] y  
Enter the path of the Apache root (null for none):
```

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.

Exporting Configurations

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 12-4](#)). (You can also select the top checkbox beside the Name field to select all items.)

■ Exporting and Importing Configurations

Figure 12-4 Export Configurations

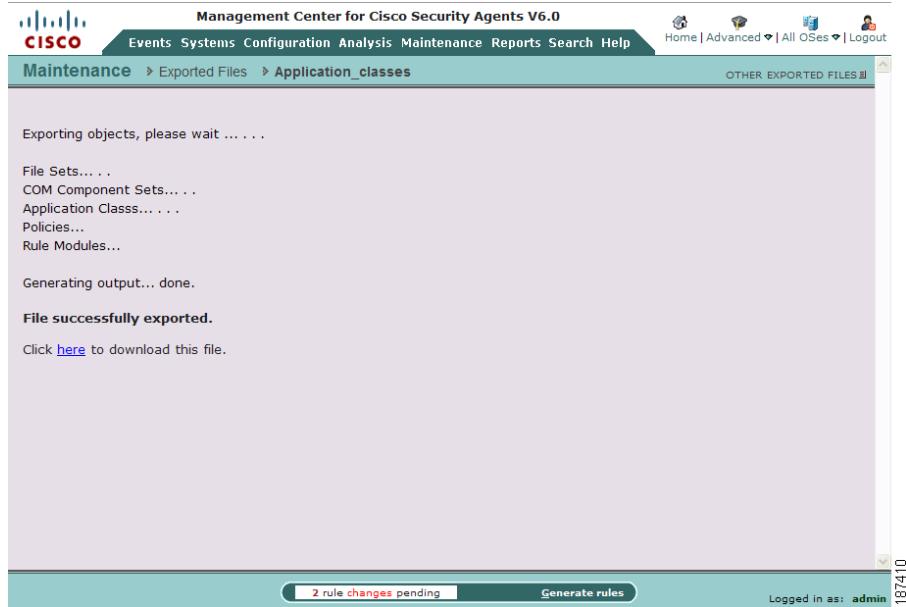
Name	Version	Type	Description
<All Linux>		Linux Group	Auto-enrollment group for Linux hosts
All Linux	6.0 r107	Linux Group	Prototype auto-enrollment group for Linux hosts (not used, see detailed description)
Desktops	6.0 r107	Linux Group	Default group for systems that install the Desktop agent kit
Desktops	6.0 r105	Linux Group	Default group for systems that install the Desktop agent kit
Servers	6.0 r105	Linux Group	Default group for systems that install the Server agent kit
Servers	6.0 r107	Linux Group	Default group for systems that install the Server agent kit
Systems - Audit Mode	6.0 r107	Linux Group	Systems operating in audit mode
Systems - Learn Mode	6.0 r107	Linux Group	Systems operating in Learn mode
Systems - Mission Critical	6.0 r107	Linux Group	Systems that need to be monitored at a higher priority
<All Solaris>		Solaris Group	Auto-enrollment group for Solaris hosts

- 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 12-5](#)).
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 12-5 Export Download View

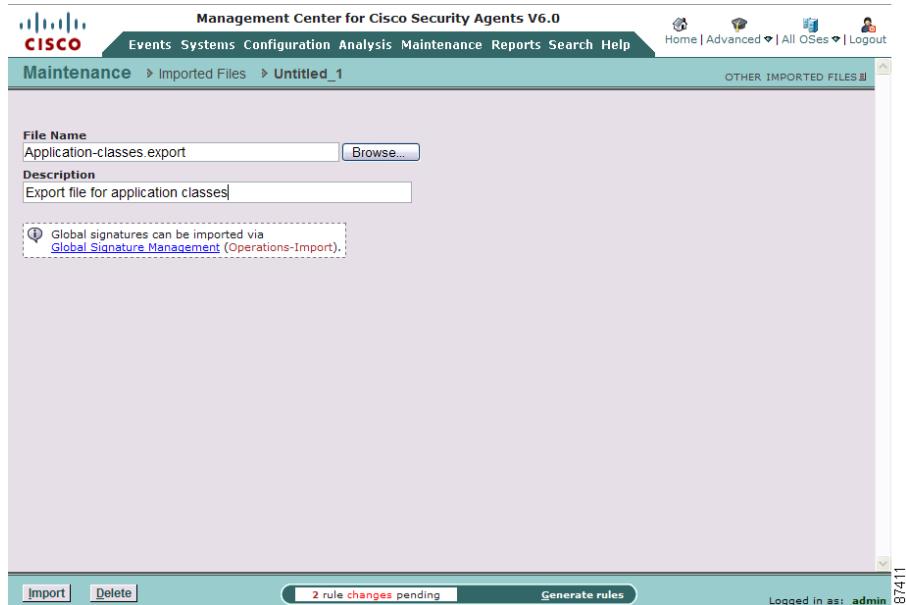
Importing Configurations

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 12-6](#)).
 - 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.

■ Exporting and Importing Configurations

Figure 12-6 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 reverisioned 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 is installed separately from CSA. 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.

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 audit 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.



CHAPTER **13**

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 13-1](#)
- [The Application Deployment Investigation Process, page 13-3](#)
 - [Reporting Categories, page 13-3](#)
- [Turning Application Deployment Investigation On, page 13-4](#)
 - [Configure Group Settings, page 13-4](#)
 - [Configure Product Associations, page 13-7](#)
 - [Associate Unknown Applications, page 13-10](#)
 - [About Data Management, page 13-11](#)
 - [Generating Application Deployment Reports, page 13-12](#)
 - [AntiVirus Installations Report, page 13-13](#)
 - [Installed Products Report, page 13-14](#)
 - [Unprotected Hosts Report, page 13-16](#)

- Unprotected Products Report, page 13-18
- Product Usage Report, page 13-19
- Network Data Flows Report, page 13-21
- Network Server Applications Report, page 13-23
- Viewing Reports, page 13-25
- Exporting Reports, page 13-25
- What is Application Behavior Investigation, page 13-26
- How Application Behavior Investigation Works, page 13-26
- The Application Behavior Investigation Process, page 13-26
 - Behavior Analyses, page 13-27
 - Creating, Saving, and Cancelling Analysis Data, page 13-28
- Configure a Behavior Analysis Investigation, page 13-29
- Start Behavior Analysis, page 13-33
- Importing the Rule Module, page 13-33
- Application Behavior Reports, page 13-34
 - Report Components, page 13-34
 - Working with Reports, page 13-37
- The Behavior Analysis Rule Module, page 13-37
 - Behavior Analysis Methodology, page 13-38
 - Reviewing the Rule Module, page 13-37

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 13-2](#).
- 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:

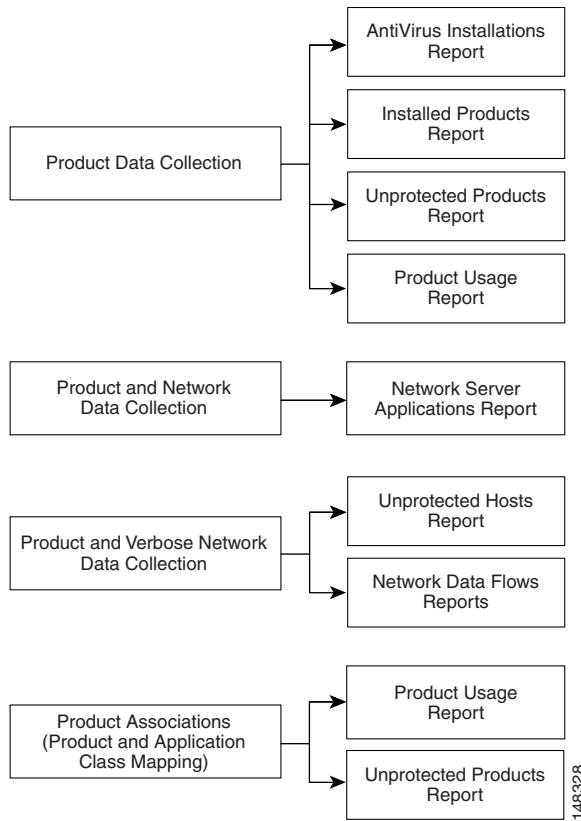
- Product data collection - which would apply to the following reports:
AntiVirus Installations, Installed Products, Unprotected Products, Product Usage
- Product and network data collection - which would apply to the following additional report:
Network Server Applications
- Product and verbose network 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 13-1 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.



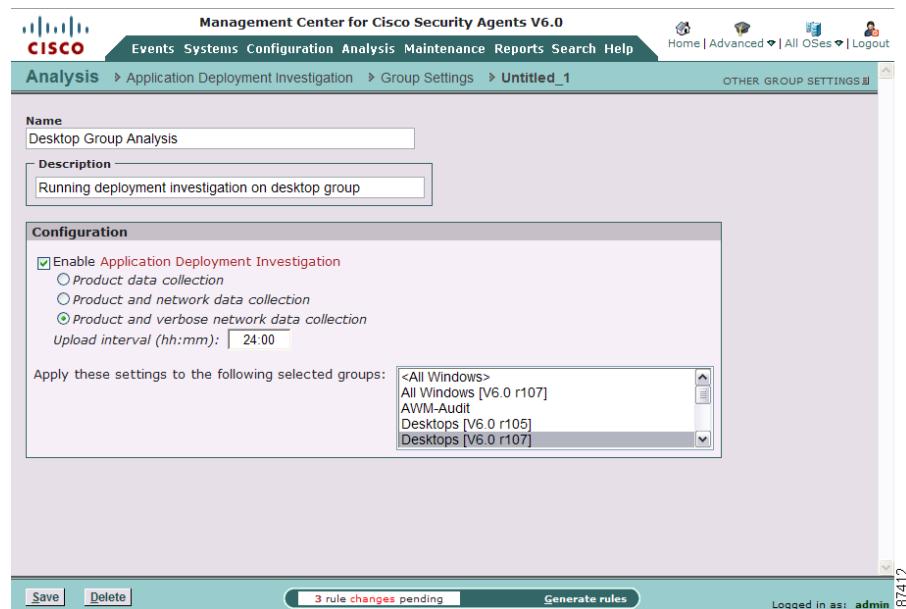
The uploading of data occurs at the end of the interval in question. Therefore, it may take more than one interval receive collected data. It depends upon when the hosts polls into the MC.

- 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 13-2 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 13-3](#). 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 13-3 Product Association List Window

The screenshot shows the 'Product Associations' page of the Cisco Management Center. At the top, there's a navigation bar with links for Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, and Help. Below the navigation bar, the title 'Analysis > Application Deployment Investigation > Product Associations' is displayed. A message 'Management Center for Cisco Security Agents V6.0' is shown above the main content area. The main content area contains a table with the following data:

Name	Description	Configured
Generic Windows Operating System		✓
Management Center for Cisco Security Agents		✓
McAfee VirusScan Enterprise (7.0.0)		✓
Microsoft Internet Explorer 6 SP1		✓
Microsoft Office Professional Edition 2003 (11.0.5614.0)		✓
Mozilla (1.6)		✓
Netscape (7.2)		✓
Norton AntiVirus 2001 Professional Edition		✓
World Wide Web Publishing Service (5.0)		✓

Below the table, there are buttons for 'Map to application class', 'Merge', 'Ignore', and 'View ignored'. A status bar at the bottom indicates '3 rule changes pending' and 'Generate rules'. The bottom right corner shows 'Logged in 18/4/13'.

- 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 the Product Associations 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.

Once you merge products, they will no longer appear as separate items in your product list.

**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. 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.

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.

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 management** 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 lose 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.
 - 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, PDF document 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.

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, PDF document 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, PDF document 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.

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. Enter a **Name** and **Description** for the report.

Step 2 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 3 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 4 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 5 Select criteria by which to sort the report. You can first sort by host and then by product or vice-versa.

Step 6 Select a **Viewer type**. By default, PDF document is selected. This is the recommended viewer.

Step 7 Click the **Save** button to save the parameters you've just configured for generating this report.

Step 8 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.

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 13-7](#).

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.

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, PDF document 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.

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.
 - 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, PDF document 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.

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.

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, PDF document 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.

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.

- PDF: This option will generate the complete report as a PDF file that can be viewed, printed, and saved using the browser PDF plug-in. If you do not have a PDF plug-in installed on your browser, you will have to install a PDF browser plug-in to view this report type.
- HTML: This option breaks the report into individual HTML pages which can be viewed one page at a time in a browser window. Only the currently viewed report page can be printed. (Supported by Internet Explorer 3.02 and higher and FireFox 1.5.0.x or 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.

**Caution**

When you print reports, it is recommended that you print using Landscape mode. Reports do not print correctly using Portrait mode.

**Caution**

CSA MC requires and installs Sun JRE (Java Runtime Environment) to generate reports using the Jasper reporting tool. If you remove the Java directory from the CSA MC system, you cannot generate reports.

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 4, “Building Policies”](#) 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 13-30](#) 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 10-23](#) 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.
- 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."

- 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.

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. This begins the analysis. An Event Log message appears informing you that "Data analysis has started."

- 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.

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.

**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.

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.

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, 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.

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.”

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 Audit 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 13-34](#) 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.



14

CHAPTER

Automatic Signature Generation

Overview

The automatic signature generation feature provides several new functions for hosts running on Windows platforms:

- Automatically generated signatures
- Denial of Service attack protection
- Process stack recovery

The Cisco Security Agent now responds to certain attacks by identifying malicious payloads used in an attack, dynamically creating a signature that represents those payloads, and then using the signature to prevent further attacks from similar payloads.

These automatically generated signatures are intended to catch a variety of attacks, primarily buffer overflows, including highly specific, targeted, and polymorphic ones. Currently, the automatic signature generation feature focuses on protecting LPC and MSRPC interfaces.

The automatic signature generation feature works by using rules that look for categories of suspicious behavior. When suspicious behavior is seen, the rules trigger and suspicious payloads are simultaneously sent to the CSA MC and analyzed by the agent. Once enough similar payloads are received, the agent can create a signature locally to defend one host, or the CSA MC generates a signature based on all the payloads it has received and distributes the signature to all hosts.

Automatic signature generation is effective because it does not rely on static signatures being downloaded at intervals. Signatures are created in real-time and can be distributed to all agents automatically or after they are reviewed by an administrator. CSA MC rules do not need to be generated in order for the signatures to be distributed.

The denial of service (DoS) protection function detects a denial of service attack on an MSRPC or LPC interface. Malicious payloads sent to that interface can be identified and dropped.

If you are using the Stack Recovery action in a System API control set rule, you are configuring the system to try to recover from unhandled exceptions. Stack recovery discards the malicious payload and unwinds the stack to the point where the program was called to process that payload. CSA tries to recover the application by handing the control of execution back to the application under attack instead of allowing it to crash or the exploit to take control.

**Note**

During the process of testing the automatic signature generation feature, CSA automatically generated several signatures that successfully defended against attacks on MSRPC and LPC interfaces. We have included these signatures in the product for the benefit of our customers. Were Cisco not to provide these signatures, the automatic signature generation feature would have dynamically created them for you.

Though Cisco provided some signatures in this release, we will not regularly distribute additional signatures in the future. The automatic signature generation feature creates signatures “on the fly” to protect against immediate attacks. It does not depend on distributed signature updates.

This chapter contains the following sections:

- [Basics, page 14-3](#)
 - [Protected Interfaces, page 14-5](#)
 - [Automatic Signature Generation, page 14-3](#)
 - [Preventing Denial of Service Attacks, page 14-4](#)
 - [Stack Recovery, page 14-5](#)
 - [Untrusted vs. Unchanged Payloads, page 14-6](#)
 - [Signature Confidence Levels, page 14-6](#)

- Signature Grouping and Tagging, page 14-7
- Refining Signatures, page 14-7
- Permanent and Expiring Signatures, page 14-7
- Offline Agents and Correlated Signatures, page 14-8
- Differences Between Signature-based AntiVirus and Automatic Signature Generation, page 14-8
- Managing Global and Local Signatures, page 14-9
 - Managing Global Signatures, page 14-11
 - Managing Local Signatures, page 14-17
 - Importing, Exporting, and Upgrading Signatures, page 14-17
- Signature Reporting, page 14-18
- Deploying the Signature Feature, page 14-18
 - Distinguish Legitimate Signatures from False Positives, page 14-19
 - Use the Wizard to Create Exceptions for Generated Signatures, page 14-20

Basics

This section describes the basic concepts behind automatic signature generation stack recovery, and interface blocking.

Automatic Signature Generation

When an MSRPC or LPC interface is attacked on a host, the local agent retrieves the payload associated with the attack, marks it as “untrusted,” and forwards it to the CSA MC. The CSA MC correlates similar untrusted payloads and creates a signature representing the attack. The local agent also correlates the same untrusted payloads and creates its own signature if it has not already received a signature from the CSA MC. The signature is referenced by a signature tag and the signature payload is made up of the substrings common to all the attack payloads.

Once a signature is created, either as a global signature or a local signature, it is associated with the @signatures token. Once associated with the @signatures token, a CSA rule can be written to act on every signature associated with that token the same way. For example, rules in the *Firewall - Centrally Managed (desktops)*, *Firewall - Centrally Managed (servers)* and *Firewall - User Managed* policies will drop an incoming attack payload if it matches any of the signatures associated with the @signatures token. This stops the attack for which the signature was generated.

Global and local signatures are created after the number of untrusted payloads received exceeds a configurable threshold. The default configuration for correlating a global signature is after two agents have sent two similar payloads in 1,440 minutes (24 hours). Local signatures are generated after the agent gathers three untrusted payloads within 1,440 minutes.

Globally correlated signatures are distributed to agents when they poll in. If a globally correlated signature is distributed and it matches a locally correlated signature already on the agent, the globally correlated signature replaces the locally correlated signature.

Preventing Denial of Service Attacks

If an MSRPC or LPC interface is attacked continuously without a signature being generated, CSA treats this as a denial of service attack. Future payloads attacking the interface are associated with the @highrisk_signatures token. Once associated with the @highrisk_signatures token, a CSA rule can be written to act on every signature tag associated with that token the same way. For example, rules in the *Firewall - Centrally Managed (desktops)*, *Firewall - Centrally Managed (servers)* and *Firewall - User Managed* policies supplied with this release, will drop an incoming attack payload if the payload tag matches any of the signature tags associated with the @highrisk_signatures token. This stops the denial of service attack using that payload.

Signature tags are associated with the @highrisk_signatures token after an MSRPC or LPC interface has triggered local signature correlation a configurable amount of time without success. By default, signature tags are added to @highrisk_signatures after an MSRPC or LPC interface has triggered local signature generation 10 times within the last 30 minutes.

Stack Recovery

“A call stack is a dynamic stack data structure which stores information about the active subroutines of a computer program. This kind of stack is also known as an execution stack, control stack, function stack, or run-time stack, and is often shortened to just ‘the stack’.” (http://en.wikipedia.org/wiki/Call_stack)

If you are using the Stack Recovery action in a System API control set rule, you are configuring the system to try to recover from an unhandled exception. Stack recovery discards the malicious payload and unwinds the stack to the point where the program was called to process that payload. CSA tries to recover the application by handing the control of execution back to the application under attack instead of allowing it to crash or the exploit to take control.

This feature may be appropriate for vital applications that respond to user requests for information but do not process transactions or interact with a database.

Allowing non-vital services to fail until a signature can be generated is a more conservative, though still effective, approach to protecting these services safely.



Warning

An application saved from crashing using stack unwinding may have some residual corruption. The Stack Recovery feature is not appropriate for protecting database applications, applications that process transactions, or applications that maintain their own record-keeping in order to recover from a failure. If you are not certain of all the behaviors of an application, do not protect it with the stack recovery feature.

Protected Interfaces

Currently, the agent can analyze payloads reaching MSRPC and LPC interfaces.

- MSRPC (Microsoft Remote Procedure Call)

The MSRPC protocol encapsulates various services from Microsoft. These are out-of-the box Microsoft OS interfaces to the network, which can be targeted for attacks.

- LPC (Local Procedure Call)

The LPC protocol is used for inter-process system communications. LPC could be used to elevate privileges of malware or used in a remote exploit.

Both MSRPC and LPC signatures are specific to the targeted application, running on a particular operating system.

Untrusted vs. Unchanged Payloads

Data payloads are gathered by the agent when a System API Control “Set” rule indicates that a payload, matching certain criteria, should be marked either “unchanged” or “untrusted.”

Signatures are only generated from “untrusted” payloads. Marking payloads “unchanged” prevents a signature from being created for that payload. If a payload is marked both unchanged and untrusted, the unchanged tag takes precedence and the payload will not be used for signature generation.

Signature Confidence Levels

When a signature is automatically generated, CSA MC assigns it a confidence level of Low by default. When a signature is imported to the CSA MC, its confidence level is imported with the signature. Administrators can change the confidence level assigned to a signature to Low, Medium, or High.

Assigning signatures confidence levels allows them to be associated with data sets that specify signature confidence level. This allows you to create data access control rules (DACLs) that act on the payload based on the confidence level of the signature. For example, you may create a DACL that drops a packet that matches a signature in which you have high confidence or notify the user when a packet matches a signature in which you have low confidence.

DACLs in the *Firewall - Centrally Managed (desktops)*, *Firewall - Centrally Managed (servers)* and *Firewall - User Managed* policies, provided with this release, reflect this strategy.

Signature Grouping and Tagging

CSA gives the payload, identified in an attack, a tag which identifies the target of the attack. The tag consists of the operating system under attack, the process being attacked, whether the attack was a buffer overflow or a result of exception handling, the protocol used in the attack, the API, the interface or the port being attacked, and the rule ID which captured the payload.

Payloads with the same tag are grouped together to form a signature. The tag used to compare the payloads become the signature tag. See [Viewing Global Signatures, page 14-13](#) for more information about global signature tags.

Refining Signatures

All the common substrings of two or more payloads attacking the same interface, create the signature of an attack. As more payloads attack the same interface, the substrings in the latest payload are compared to the common substrings in the signature. CSA refines the signature by keeping in the signature only the common substrings from the latest payload and the existing signature.

Signatures that are marked **Permanent** in the **Manage Global Signatures** dialog cannot be refined.

Permanent and Expiring Signatures

Signatures that “expire” are deleted from CSA MC after a configurable period of time. By default, automatically generated signatures expire. Signatures identified by @signatures expire based on the value of the **Expire signatures after X days** field in the <Common> area of the Signatures Settings page. The default expiration period is 30 days.

“Permanent” signatures are not deleted from the CSA MC and they are not refineable.

Payloads identified by @highrisk_signatures token expire based on the settings in the “Local” section of the MSRPC and LPC protocol areas of the Signature Settings page. The default expiration period for interfaces identified by @highrisk_signatures is 60 minutes.

See the “[Global Signatures Operations](#)” section on page 14-15 for more information about how to set signatures as permanent or expiring.

Offline Agents and Correlated Signatures

If an agent can not reach its CSA MC for some reason, it will still benefit from local signature correlation but it will not benefit from globally correlated signatures until it can reach the CSA MC and polls in. The local functionality of an agent will protect the host from buffer overflow, exception handling, and denial of service attacks that use MSRPC and LPC protocols.

Differences Between Signature-based AntiVirus and Automatic Signature Generation

Signature-based AntiVirus protection in this release of CSA is a traditional antivirus security feature. It scans the contents of files and compares the content to a library of known virus signatures. If a file contains a virus, the file is rendered inert by CSA policies which prevent the file from being read, written to, or executed.

All local files are scanned periodically. Some files are scanned when they are opened or closed, based on rules in the AntiVirus - Signature based policies for desktops and servers. Regular updates of virus signature files are required to ensure that AntiVirus properly identifies the latest known viruses residing in files.

The Automatic Signature Generation feature is designed to protect MSRPC and LPC interfaces from buffer overflow and denial of service attacks. As one of these interfaces is being attacked, the Automatic Signature Generation feature dynamically creates a signature that identifies the attack. That signature is then used by rules to prevent other similar attacks.

Automatically generated signatures are created in real time, this feature does not depend on static signatures which you need to download periodically.

Managing Global and Local Signatures

The **Signature Settings** page is accessible from the CSA MC menu bar by navigating **Configuration > Global Settings > Signature Settings**. You can use this page to set the values for global and local signature correlation, thresholds to prevent denial of service attacks, globally enable new signatures and other managerial tasks related to signature correlation. The Signature Settings page is only viewable in Advanced Mode.

Figure 14-1 Signature Settings page

The screenshot shows the 'Management Center for Cisco Security Agents V6.0' interface in Microsoft Internet Explorer. The title bar reads 'Management Center for Cisco Security Agents V6.0 - Microsoft Internet Explorer'. The address bar shows the URL 'https://client221/csamc60/webadmin'. The main navigation menu includes 'Events', 'Systems', 'Configuration', 'Analysis', 'Maintenance', 'Reports', 'Search', 'Help', and 'Logout'. Below the menu, the current location is 'Configuration > Signature Settings'. The main content area contains several sections for different protocols:

- <Common>**: Settings common to all protocols. Includes an option to 'Enable new signatures'.
- <MSRPC>**: Settings specific to protocol MSRPC. Contains two sections: 'Central:' and 'Local:'. Under 'Central:', there is a checked checkbox for 'Correlate untrusted MSRPC payloads received by Cisco Security Agent systems' [Events: 0]. Under 'Local:', there are two bullet points: 'Add to @highrisk_signatures any payloads on an MSRPC interface that has triggered local signature generation [10] times within the last [30] minutes' and 'Remove from @highrisk_signatures any payloads on an MSRPC interface that has not triggered any local signature generation within the last [60] minutes'.
- <LPC>**: Settings specific to protocol LPC. Contains two sections: 'Central:' and 'Local:'. Under 'Central:', there is a checked checkbox for 'Correlate untrusted LPC payloads received by Cisco Security Agent systems' [Events: 0]. Under 'Local:', there are two bullet points: 'Add to @highrisk_signatures any payloads on an LPC interface that has triggered local signature generation [10] times within the last [30] minutes' and 'Remove from @highrisk_signatures any payloads on an LPC interface that has not triggered any local signature generation within the last [60] minutes'.

At the bottom of the page, there are 'Save' and 'Generate rules' buttons, and a status message 'No rule changes pending'. The bottom right corner shows the user is logged in as 'administrator' and the IP address is '24.8.31.1'.

The following sections are included in the Signature Settings page:

- **Common** - This section contains signature settings that are common to all hosts that benefit from automatic signature generation.

The **Expire signatures after X days** field indicates when a local or global signature expires. By default, signatures correlated locally or globally expire after 30 days.

The **Enable new local signatures** check box is enabled by default. This allows local signatures to be generated locally. If **Enable new local signatures** is not selected, then no local signatures are generated.

The **Enable new global signatures** check box is enabled by default. When **Enable new global signatures** is enabled, signatures are automatically generated after the MSRPC or LPC correlation thresholds are met and they are assigned a confidence level of Low. Globally enabled signatures are distributed to hosts when they next poll in.



Note If you want **new** global signatures disabled automatically, select the **Enable new signatures** checkbox and generate rules on the CSA MC.

- **MSRPC** - The **Correlate untrusted MSRPC payloads received by Cisco Security Agent systems** checkbox, turns on untrusted MSRPC payload signature generation. The checkbox is selected by default. The next section determines how many agents within a specific time frame, with similar events for receiving untrusted MSRPC payloads, are required to trigger a global signature correlation. The default is two systems reporting two similar MSRPC payloads within 1440 minutes (24 hours).

The next section for MSRPC signature generation deals only with local payloads associated with Denial of Service (DoS) attacks. Administrators define DoS attacks as a specified number of attacks on an interface, over a specified period of time, without a signature being correlated. Once that threshold is met, future payloads attacking the interface are associated with the @highrisk_signatures token. After a configurable amount of time, the payloads are no longer associated with the @highrisk_signatures token.

By default, an interface is considered receiving a DoS attack if ten payloads are received within 30 minutes and a signature could not be created for the attack; after 60 minutes, the payloads are disassociated with the @highrisk_signatures token.

- **LPC** - The **Correlate untrusted LPC payloads received by Cisco Security Agent systems** checkbox, turns on untrusted LPC payload signature generation. The checkbox is selected by default. The next section determines how many agents within a specific time frame, with similar events for receiving untrusted LPC payloads, are required to trigger a global signature correlation for all agents. The default is two systems reporting two similar LPC payloads within 1440 minutes (24 hours).

The next section for LPC signature generation deals only with local payloads associated with Denial of Service (DoS) attacks. Administrators define DoS attacks as a specified number of attacks on an interface, over a specified period of time, without a signature being correlated. Once that threshold is met, future payloads attacking the interface are associated with the @highrisk_signatures token. After a configurable amount of time, the payloads are no longer associated with the @highrisk_signatures token.

By default, an interface is considered receiving a DoS attack if ten payloads are received within 30 minutes and a signature could not be created for the attack, and after 60 minutes, the payloads are disassociated with the @highrisk_signatures token.

- The links labeled **Expand all** and **Collapse all** allow you to display or hide all the settings for the <Common>, <MSRPC>, and <LPC> areas of this page.
- The Tasks menu has one menu item. Clicking **Manage Global Signatures** allows you to see the list of globally correlated signatures and manage them.

Managing Global Signatures

From the Signature Settings page, click the **Manage global signatures** link under the **Tasks** menu. This opens the **Global Signature Management** page. This window contains all the globally generated signatures managed by the CSA MC and all the signatures delivered by default in CSA 6.0.

■ Managing Global and Local Signatures

Figure 14-2 Global Signature Management Page

#	Exploit	Enabled	Confidence	Permanent	Source	Last Update
1	Process dns.exe experienced exception processing MSRPC payload on programming interface with GUID=50abc2a4-574d-40b5-9d66-eef4fd5... [details]	Yes	High	Yes	CSA auto-generated	7/13/2007 12:10:50 PM
2	Process lsass.exe experienced exception processing MSLPC payload on port 'LsaAuthenticationPort' and operation=13 [details]	Yes	High	Yes	CSA auto-generated	7/13/2007 12:10:53 PM
3	Process lsass.exe experienced exception processing MSLPC payload on port 'LsaAuthenticationPort' and operation=13 [details]	Yes	High	Yes	CSA auto-generated	7/13/2007 12:10:53 PM
4	Process lsass.exe experienced exception processing MSLPC payload on port 'LsaAuthenticationPort' and operation=13 [details]	Yes	High	Yes	CSA auto-generated	7/13/2007 12:10:53 PM
5	Process lsass.exe experienced exception processing MSRPC payload on programming interface with GUID=dsetetu and API=9 [details]	Yes	High	Yes	CSA auto-generated	7/13/2007 12:10:52 PM
6	Process services.exe experienced buffer_overflow with GUID=srvsvc and API=31 [details]	Yes	High	Yes	CSA auto-generated	7/13/2007 12:10:48 PM
7	Process services.exe experienced exception with GUID=8d9f4e40-a03d-11ce-8f69-0... [details]	Yes	High	Yes	CSA auto-generated	7/13/2007 12:10:52 PM

The Global Signature Management page contains the following columns of information:

- **Exploit** - This column briefly describes the exploit that generated the signature. It provides the process name, the kind of exploit, the interface that was attacked, and the GUID or port name. (MSRPC signature tags are identified by a Global Unique Identifier (GUID) and an API number. LPC signature tags are identified by a port name and an API number.) You can click the **details** link to view the signature tag in an easily readable format along with the common substrings that comprise the signature. See [Viewing Global Signatures, page 14-13](#) for more information about the Attack Details dialog.
- **Enabled** - Enabled signatures are distributed to agents when they poll in. If the **Enable new signatures** in the <Common> area of the Signature Setting page is selected, globally correlated signatures will be enabled after they are created. By default, globally correlated signatures are enabled.
- **Confidence** - When a signature is automatically generated, it is assigned a confidence level of Low. The confidence level indicates the likelihood that the generated signature has been derived from a dangerous attack. You can set the confidence level to Low, Medium, or High using the drop down menu.

24830

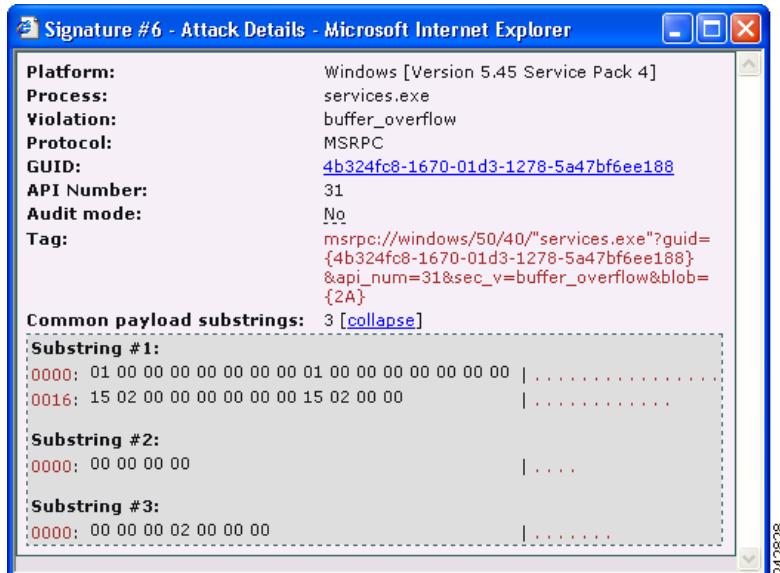
- **Permanent** - Permanent prevents the signature from being deleted at the time defined by the **Expire signatures after X days** field in the <Common> area of the Signature Settings page. If you don't want a signature to be deleted, set Permanent to **Yes**.
- **Source** - This indicates whether the signature was automatically generated by CSA rules or whether it was imported from another source.
- **Last Updated** - This is the date that the signature was added to the global correlation list.

At the bottom of the table is an **Operations** button and a **Refresh** button. See the “[Global Signatures Operations](#)” section on page 14-15 for instructions on how to use these command buttons.

Viewing Global Signatures

To view the details of a global signature follow this procedure:

-
- Step 1** Log on to the CSA MC and switch to **Advanced Mode**.
 - Step 2** From the **Configuration** menu, navigate **Global Settings > Signature Settings**.
 - Step 3** Expand the Tasks menu and click **Manage global signatures**.
 - Step 4** Find the signature you want to examine and click its **details** link. The Attack Details page opens.
 - Step 5** Clicking the signature tag displayed in the Global Signature Management page opens the **Attack Details** pop-up window; it displays the signature in text format.

Figure 14-3 Attack Details pop-up window

The Attack Details pop-up window provides you with this information:

- The signature tag is displayed in an easily readable format in the top section of the Attack Details pop-up window:
 - **Platform:** The operating system and service pack level on which the application was attacked.
 - **Process:** The name of the application or process that was attacked.
 - **Violation:** This identifies the form of attack. Figure 14-3 shows that the form of this attack was by exception handling.
 - **Protocol:** Indicates if the MSRPC or LPC protocol was used for the attack.
 - **GUID:** This is the Globally Unique Identifier (GUID) of the interface under attack. Clicking the link performs an Internet search for information about this GUID using the Google search engine.
 - **Port:** Name of the LPC port being attacked.
 - **API Number:** Displays the method number within the object.
 - **Tag:** This is the label that identifies this signature.

- **Audit Mode:** Indicates whether or not this signatures was found by rules running in audit mode. Mousing-over the **Yes** or **No** link the link tells you how many systems were running in audit mode.
- **Common Payload Substrings:** Shows the number of payloads that have been correlated thus far. Clicking the **Expand** or **Collapse** link displays or hides the payload substrings that have been correlated.
- **Correlating events:** Shows you the events in the Event Log which correlated the signature. Clicking the **View** link displays these events.

Global Signatures Operations

You can also manage the signatures in the Global Signature Management window. To do so, follow this procedure:

-
- Step 1** Log on to the CSA MC as a user with configure privileges and switch to **Advanced Mode**.
 - Step 2** From the **Configuration** menu, navigate **Global Settings > Signature Settings**.
 - Step 3** Expand the Tasks menu and click **Manage global signatures**.
 - Step 4** Click the check box next to the signature(s) you want to manage.
 - Step 5** Click the **Operations** button at the bottom of the Global Signature Management page.
 - Step 6** Select one of these operations and the list box and click **Execute**:
 - **Remove** - This operation deletes the signature from the list.
 - **Enable** - This operation allows the signature to be distributed to all agents. This is the same as selecting **Yes** in the Enable column for that signature.
 - **Disable** - This operation prevents the signature from being distributed to all agents. This is the same as selecting **No** in the Enable column for that signature.
 - **Import** - This adds signatures to the list of global signatures. After selecting **Import**, browse to the location of the signature file. Select **Importing refinable signatures exported from the same MC** if it is appropriate, and click **Execute**

If you don't select the **Importing refinable signatures exported from the same MC**, then the RuleID is stripped from the signature when it is re-imported. This prevents the signature from being further refined.

Do not select **Importing refinable signatures exported from the same MC** when importing signatures generated from one CSA MC to another CSA MC.

If you select **Importing refinable signatures exported from the same MC** then the same CSA MC will be able to continue to refine the re-imported signature definitions if there are more reported instances of the attack.

- **Export** - This exports the selected signatures to the local MC. After you have clicked Execute, and confirmed your intention to export the file, you receive a message saying that the export was successful with a link to download the exported signature. Click the link to locate the signature list and save it. Click **Done** to close the export signature box.



Note If you want to prevent a signature from being further refined by the signature correlation process, export the signature and then re-import it without checking the **Importing refinable signatures exported from the same MC**.

- **Make permanent** - Selecting **Make permanent**, prevents the signature from being deleted at the time defined by the **Expire signatures after X days** field in the <Common> area of the Signature Settings page. This is the same as selecting **Yes** in the Permanent column for a signature.

Permanent signatures can still be manually deleted using the **Remove** operation described previously.

- **Make expiring** - Selecting **Make expiring**, allows the signature to expire after the value of the **Expire signatures after X days** field, in the <Common> area of the Signature Settings page, has been reached. This is the same as selecting **No** in the Permanent column for a signature.

When a signature is changed from Permanent to Expiring, the signature is deleted based on its creation date, not the date that it was changed from Permanent to Expiring.

- **Set confidence** - By selecting **Set confidence**, you can change the confidence level in the signature to Low, Medium, or High. This is the same as choosing Low, Medium, or High in the Confidence column of the signature. When a signature is created, it is automatically given the confidence level of Low.

Clicking **Refresh** in the Global Signature Management screen updates an open screen with the latest correlated global signatures.

Managing Local Signatures

Local signatures can not be managed individually as global signatures can. A signature that has been generated locally can only be deleted by resetting the local agent.



Caution

Resetting the local agent in order to remove local signatures will affect more than just the local signatures; it returns almost all the agent settings to their original state when the agent was installed.

To reset the local security agent, navigate:

Start>Programs>Cisco>Cisco Security Agent>Reset Cisco Security Agent.

Importing, Exporting, and Upgrading Signatures

Signatures can be imported and exported using the operations menu in the Global Signature Management window. See the “[Global Signatures Operations](#)” section on page 14-15 for more information about importing and exporting signatures.

Upgrading to Refined Signatures

As signatures are refined, they are distributed to the local agent when the agent polls in for updates. Generally, the attributes of the signature tag and the signatures permanence setting are retained if a signature is upgraded.

Globally correlated signatures are distributed to agents when they poll in. If a globally correlated signature is distributed and it matches a locally correlated signature already on the agent, the globally correlated signature replaces the locally correlated signature.

Upgrading Signatures Due to CSA MC Upgrade

How signatures are upgraded from one release of CSA MC to another depends on whether or not the System API Control “Set” rules shipped with CSA MC have changed.

A CSA MC upgrade fully compares new rule modules to existing rule modules with all their dependencies. If there are no differences, the CSA MC re-labels a rule module with the latest version and leaves rule ids intact. If there are any differences between rule modules, CSA MC creates a new module with the new kit version number appended to the name, and puts the new rules there.

Your private exceptions modules are not upgraded, so any signatures you generate would stay refineable.

Signature Reporting

You can generate reports that describe various aspects of signature creation and protection using signatures. See the [“Signature Information Detail” section on page 11-19](#) for the various signature detail reports you can create.

Deploying the Signature Feature

The simplest way to deploy the Automatic Signature Generation feature is to deploy the default Windows Desktop or Windows Server agent kits and then evaluate the signatures that are generated. Then elevate legitimate globally correlated signatures to Medium or High confidence and make exceptions for signatures created from false positives. (A false positive occurs when CSA interprets a benign payload as malicious and creates a signature to prevent that payload from being delivered again.)

The System API control rules that deny an action or terminate a process attempting to access system functions from code executing in data or stack space, or run an exception handling routine, are spread throughout other rule modules or are written by you to protect a particular application.

The default Windows Desktops or default Windows Servers agent kits contain the policies that generate locally and globally correlated signatures after one of those System API rules is triggered. These policies are *Firewall - Centrally Managed (desktops)*, *Firewall - Centrally Managed (servers)*, and *Firewall - User Managed*.

Distinguish Legitimate Signatures from False Positives

Global signatures are created with a confidence setting of Low. See (**confidence levels**) for more information. When using the default policies shipped with this release, when a signature of Low confidence is matched to an application's attempt to access system functions from code executing in data or stack space or an application's attempt to handle exceptions, a DACL reports an event but the application's action is allowed.

Use these guidelines to determine if the signature is legitimate or a false positive:

1. Open the CSA MC Event Log and look at the application generating the event. Applications vulnerable to attack are often network servers (for MSRPC) or applications interacting with network servers (for LPC).
2. Examine the information in the matching signature, cross-linked with the Set-Untrusted event. The tag in the Global Signature Management screen (also present in the details of the event) gives you the interface ID (GUID) or LPC interface name, the application name, and the policy violation (exception, buffer overflow, etc). Search the Internet for the GUID to see if it corresponds to a known vulnerability or attack.
3. Return to the CSA MC Event log and examine this host's and this application's other events in close proximity to the signature generation event. Suspicious activity (e.g., an unusual outbound connection or registry modification attempts) suggests that the signature corresponds to a real threat.

After analyzing the events that come from the DACL, if you determine that the signature is legitimate, elevate your confidence in the signature to Medium or High and the application's actions will be denied. See [Global Signatures Operations, page 14-15](#).

If you determine that the signature is a false positive, create an exception to the rule that denied the application's action and disable the global signature. See [Use the Wizard to Create Exceptions for Generated Signatures, page 14-20](#) for these procedures.

If there are signatures that have been correlated on the local agent, you can use the Reset Cisco Security Agent feature to remove it. See the “[Managing Local Signatures](#)” section on page 14-17.

Use the Wizard to Create Exceptions for Generated Signatures

If you feel that a signature, that has been automatically correlated, is stopping benign traffic, you can use the Event Management Wizard to create an exception in order allow the traffic.

Once the signature has been generated, you need to perform two tasks in order to allow the benign behavior:

1. [Use the Event Management Wizard to Allow the Application to Operate, page 14-21](#). This will prevent a signature from being generated.
2. Disable the globally correlated signature. See [Disabling an Unwanted Correlated Signature, page 14-23](#) for more information.

Use the Event Management Wizard to Allow the Application to Operate

Figure 14-4 shows a series of events surrounding a global signature correlation:

Figure 14-4 Signature Generation Event Sequence

11	6/25/2008 9:21:39 AM	client1027	Notice	⊕	The process 'C:\Documents and Settings\Administrator\Desktop\signature_test_utilities\msrpc_s.exe' (as user CLIENT1027 \Administrator) attempted to receive data. The operation was allowed by default (rule defaults). This action was due to global signature matching following global_signature.correlation (2 attacks with similar payload were detected by agent rule 84 on 1 host). Details Rule 84 Wizard 
10	6/25/2008 10:24:10 AM	-	Information	-	The central server has generated a signature for an attack on protocol MSRPC, interface "996b0ce0-c70b-1067-b317-00dd010662da", API 0. The attack was triggered by agent rule 84 on 2 hosts from 4 payloads over a time interval of 864000 seconds. The signature was enabled and distributed to agents. Details Signature Settings Wizard 
9	6/25/2008 9:20:52 AM	client1027	Information	⊕	The process 'C:\Documents and Settings\Administrator\Desktop\signature_test_utilities\msrpc_s.exe' (as user CLIENT1027 \Administrator) attempted to call an exception handling routine. The exception code was '-1073741819'. The specific action was taken to set Data Payload trust status as Untrusted if MSRPC (locally and globally). Details Rule 84 Wizard 
8	6/25/2008 9:20:52 AM	client1027	Alert	✗	The process 'C:\Documents and Settings\Administrator\Desktop\signature_test_utilities\msrpc_s.exe' (as user CLIENT1027 \Administrator) attempted to call an exception handling routine. The exception code was '-1073741819'. The operation was denied. Details Rule 762 Wizard 

- Event 8 shows msrpc_s.exe attempted to call an exception handling routine and the event was denied.
 - Event 9 shows that the data payload was marked as untrusted.
- Events 8 and 9 are the last events in a series (not shown) that lead up to the correlation of a global signature. Making an exception to the rule that triggered Event 8 would “white-list” **msrpc_s.exe** and would prevent any other such actions from creating a globally correlated signature.
- Event 10 reports that the CSA MC has generated a signature for an attack on the MSRPC interface; this is the globally correlated signature.
 - Event 11 shows that msrpc_s.exe attempted to receive data and that the action was not prevented. This form of event was reported because the rule matched the msrpc_s.exe payload to a correlated signature. This event is able to display the data the msrpc_s.exe collected that ultimately causes the exception handling.

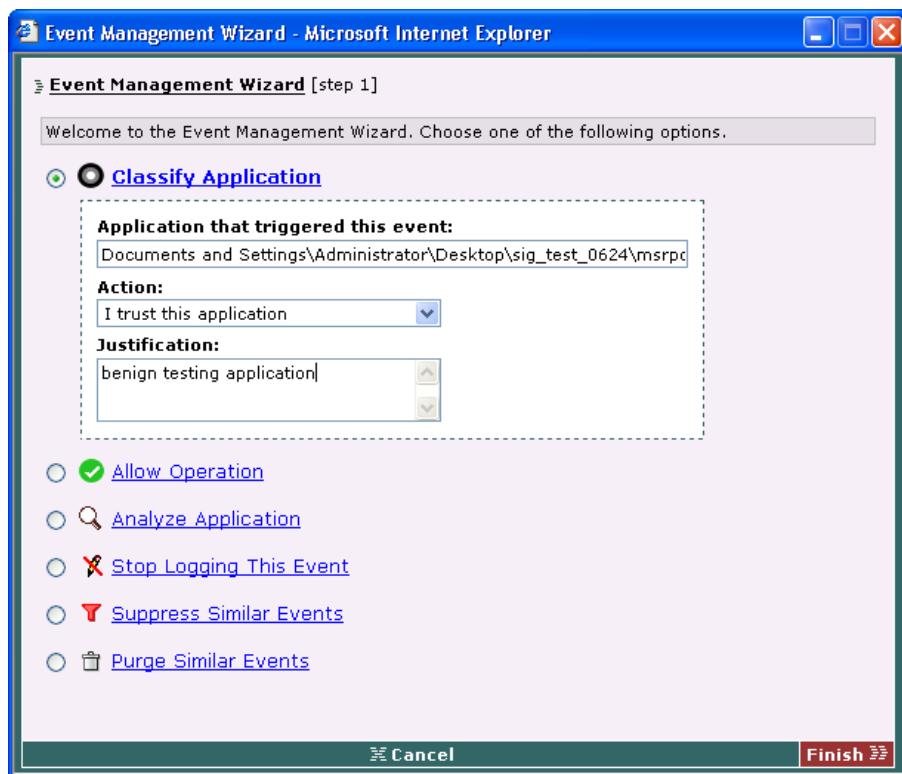
The rule that lead to CSA MC creating a globally correlated signature blocking your application from acting will likely be different from the one in this example. The important thing to remember is to accept the settings suggested by the Event Management Wizard when creating an exception.

Step 1 Log on to the CSA MC as a user with configure privileges.

■ Deploying the Signature Feature

- Step 2** From the **Event** menu, select **Event Log**.
- Step 3** Click the **Wizard** link in the rule that triggered the Alert event. In Figure 14-4, this is rule 762 in Event 8.
- Step 4** In the Event Management Wizard box, accept the choices offered to you by the wizard:
- Select **Classify Application**.
 - The **Application that triggered this event** field shows the path to the application you are going to classify.
 - In the **Action** field, accept the setting **I trust this application**.
 - Enter the reason you are creating this exception in the **Justification** field.

Figure 14-5 Event Management Wizard



- Step 5** Click **Finish**. The global **Application Trust Levels** list view opens and lists the application which you have just added to the “White List.” The application’s white-list status will be recognized after you generate rules and the agents poll in to the CSA MC.

Disabling an Unwanted Correlated Signature

Disabling the global signature in order to prevent it from causing CSA to deny benign or desirable actions is a better strategy than deleting the signature right away.

If you delete the signature you lose the payloads and information associated with it. If the global signature is marked as “Expiring” then CSA MC will delete the signature when it expires in 60 days.

See [Global Signatures Operations, page 14-15](#) for more information about disabling signatures and setting the expiration setting for a signature.

■ Deploying the Signature Feature



CHAPTER **15**

AntiVirus Protection

Overview

The AntiVirus feature provides protection from computer viruses that have been identified by a signature and malware that has been identified by its suspicious or dangerous behavior. Signature-based AntiVirus functions and behavior-based AntiVirus functions provide complimentary protection.

This chapter contains these sections:

- [AntiVirus Basics, page 15-2](#)
 - [Signature-based AntiVirus, page 15-2](#)
 - [Behavior-based AntiVirus, page 15-3](#)
 - [Enabling AntiVirus Protection, page 15-3](#)
 - [How AntiVirus Signatures are Updated, page 15-4](#)
 - [Signature-based Scanning for Viruses, page 15-5](#)
 - [The @virusscan Token, page 15-8](#)
 - [Quarantined Files, page 15-9](#)
 - [Differences Between Signature-based AntiVirus and Automatic Signature Generation, page 15-10](#)
- [Administrative Signature-based AntiVirus Tasks, page 15-10](#)
 - [Scheduling a Background Scan, page 15-11](#)
 - [Performing an On-Demand AV Scan, page 15-12](#)
 - [Identifying a Host AntiVirus Scan Schedule, page 15-13](#)

- Forcing a Signature Update for a Group, page 15-13
- Forcing a Signature Update for a Host, page 15-13
- Creating Exemptions for AntiVirus Tags, page 15-14
- End-user AntiVirus Tasks, page 15-28
- AntiVirus Reporting, page 15-17
- Creating Signature-based AntiVirus Rules and Components, page 15-17
- Configuring Behavior-based AntiVirus Policy, page 15-27
- End-user AntiVirus Tasks, page 15-28

AntiVirus Basics

This section provides an overview of the AntiVirus features.

Signature-based AntiVirus

The signature-based AntiVirus function protects the endpoint by identifying infected files. Once identified, CSA tags these files as infected and then security policies limit the actions of, or the access to, these files.

Virus signatures and the signature-matching infrastructure are supplied by Clam AntiVirus (<http://www.clamav.org>). Clam AntiVirus, or ClamAV™, is an open-source antivirus toolkit. A community of users submit files, infected with viruses to ClamAV, ClamAV creates a signature for the virus and then distributes signature updates back to its user community.

Incorporating a traditional antivirus scanner in CSA provides fast and efficient defense against known viruses along with a low rate of false positives. This feature complements CSA's ability to defeat unknown, day-zero attacks based on identifying malicious behavior.

The signature-matching infrastructure supplied by ClamAV and the CSA policies to restrict infected files are only available for Windows platforms.

Behavior-based AntiVirus

The behavior-based AntiVirus function protects the endpoint by examining an untrusted application's behavior. If an application acts in such a way that is suspicious, malicious, or dangerous, the application receives a behavior-based AntiVirus tag and the application is placed in an application class that reflects its behavior.

As the application continues to act, the end-user is made aware of the application's behavior through pop-up notifications and events in the agent GUI. The user can allow the application to act or prevent the application from acting. As the user prevents an application's actions, the application is placed in application classes that are subject to increasingly restrictive rules or terminated based on the user's selection.

After an application has violated a certain number of different policies, the default rules can severely limit its actions or terminate the application automatically.

There are also some actions that an application may take which are automatically denied and the application is automatically terminated without prompting the user for input.

Behavior-based AntiVirus policies are available for Linux, Unix, and Windows platforms.

Enabling AntiVirus Protection

Signature-based AntiVirus protection is enabled when the *AntiVirus - Signature based* policy is deployed to a group. A group's details page and an individual host's details page indicate that the function is enabled. When signature-based AntiVirus protection is deployed, end-users will be able to perform on-demand scans, manage quarantined files, and manage restored files.



Note

CSA installs a signature database on the host; it is used in identifying infected files. If other antivirus applications are installed on the host, it is likely that they will interpret these signature database files as infected and quarantine them. So that there are no conflicts, we strongly recommend that users uninstall other antivirus applications when using CSA's AntiVirus feature.

Behavior-based AntiVirus protection is enabled when the *AntiVirus - Behavior based* policy is deployed to a group. A group's details page and an individual host's details page indicate that the function is enabled. When behavior-based AntiVirus protection is deployed, end-users will see the AntiVirus pane on their Cisco Security Agent. Users will be able to Restore and Quarantine files with behavioral AntiVirus tags using the AntiVirus screen but they will not be able to perform on-demand scans.

How AntiVirus Signatures are Updated

For signature-based AntiVirus protection, the CSA MC maintains a cached version of the Clam AntiVirus signature files and acts as a proxy server when a signature update is requested by an agent.

Agent requests for signature file updates trigger the CSA MC to obtain and provide virus definitions. When agents request updated virus signature files from the CSA MC, the CSA MC compares the timestamp of the signature files on the Clam AntiVirus server with its cached version of the file. If the timestamp of the files on the Clam AntiVirus server matches the copy of the signature files cached on the CSA MC, the CSA MC provides the agent with the signature updates from its own cache. If the CSA MC's cached version is out of date, the CSA MC passes the agent's request directly to the Clam AntiVirus server and then caches the new version of the signature files when they are returned.

**Note**

In order for the CSA MC to obtain signature updates from ClamAV server (db.local.clamav.net) should be reachable over HTTP either directly or through proxy server.

Two files comprise the virus signature database on the CSA MC:

- Main signature file (main.cvd). This is the main signature file which is stored on the CSA MC and downloaded to every agent. This file is updated with every new release of ClamAV.
- Daily updates file (daily.cvd). This is the database of updated signatures. It is stored on the CSA MC and downloaded to every agent. This file is updated several times a day and stores the latest virus definitions.

On the CSA MC, the virus signature database files are stored here:
Program Files\Cisco\CSA MC\CSAMC60\bin\WebServer\htdocs\clamav

On the agent, the virus signature database files are stored here:
\\Program Files\\Cisco\\CSAgent\\dclass\\csa-av

An agent contacts the CSA MC for signature updates as a result of one of these events:

- **A scheduled request for antivirus updates.** An agent contacts the CSA MC every 24 - 25 hours for updated virus definitions.
- **Forced antivirus updates from a host.** Users can force an antivirus update from the AntiVirus screen of Cisco Security Agent interface.
- **Forced antivirus update for a group.** CSA MC administrators can force an antivirus update for a group from the group's properties page.

If the Cisco Security Agent is standalone, or if the agent can not reach the CSA MC for two days, the agent will try to communicate directly with the internet server, <http://db.local.clamav.net> to get signature updates directly from ClamAV.

Signature-based Scanning for Viruses

For signature-based AntiVirus protection, the goal of virus scanning is to determine if a file is infected or clean. Infected files are tagged with the name of the virus that infects them. Clean files receive an empty tag. Once the files are tagged, rules in the AntiVirus policy protect the host from the infected files.

CSA scans for viruses using these methods

- [Background Scan](#)
- [Scanning Files when Accessed](#)
- [On-demand Scan](#)



Note

These scans do not change a file's modification date.

Background Scan

Administrators can schedule weekly or monthly background scans of all hosts that use the default *AntiVirus - Signature-based* server or desktop policy provided with this release. These policies contain rules that specify which files will be scanned during a background scan. By default, files on fixed local drives are scanned during an AntiVirus background scan.

Background scans happen slowly, at a controlled pace, so as not to affect the user experience. See [Scheduling a Background Scan, page 15-11](#) for more information.



Note

We recommend regular background scans for all hosts.

Scanning Files when Accessed

Scanning for virus signatures occurs when files are opened, closed, or executed. Rules in the *AntiVirus - Signature-based* server or desktop policies determine which files are scanned and under what circumstances.

Files over 3MB in size are scanned slowly and separately from other accessed files. This allows the scanner to keep up with on-access scan requests.

On-demand Scan

If a host is protected by the *AntiVirus - Signature-based* policy, for desktops or servers, then the AntiVirus pane will be visible to the user in the agent user interface. Users start on-demand scans from that screen.

An on-demand scan examines all files on fixed local drives including archive files such as .zip files and mail files, such as .pst. On-demand scans do not scan files based on rules in a policy.

See [AntiVirus Protection, page A-17](#) for the procedure to perform an on-demand scan. Users can view the procedure in the Agent user interface help by clicking the **AntiVirus** task and clicking the help icon associated with that screen.

AntiVirus Tagging

Content files receive AntiVirus tags when virus signatures are found in them. Applications receive AntiVirus tags when they take some action that is considered, suspicious, dangerous, or malicious.

Signature-based AntiVirus Tagging

Once a file is scanned it acquires a tag. Once a file is tagged, rules protect the host from the file based on the file's tag. If a file is infected, it is tagged with the name of the virus that infects it. For example, if a file has been scanned and it is infected with the CodeRed worm, it is tagged: <Virus:Worm.CodeRed>. If a file has been scanned and it is not infected, the file receives an empty tag, “ ”.

If a file has not yet been scanned, it has no tag. While a file is being scanned, it gets the temporary tag, <CSA_SCAN_IN_PROGRESS>. If a file cannot be scanned, it is tagged <CSA_UNSCANNABLE>. An encrypted file is an example of an unscannable file.

There is also a <CSA_SCAN_NOT_ATTEMPTED> tag. Files could receive this tag if the file scanner is not ready to scan a file or if the file scanner does not have permission to open a file, for example. If a file is tagged with <CSA_SCAN_NOT_ATTEMPTED> the file scanner will make additional attempts to scan the file. A file only has the <CSA_SCAN_NOT_ATTEMPTED> tag during the scanning transaction. After the attempted scan, the <CSA_SCAN_NOT_ATTEMPTED> tag is removed from the file.

When CSA scans files, the file scanner checks to see if a file has an existing tag. If the file has an existing tag, and has not been modified since the previous scan, the existing tag is still considered valid and the file is not re-scanned.

“Clean” files, those with empty tags, lose their tags when the file scanner is shut down. This would happen, for example, if the host is rebooted. When a file loses its clean tag, it will be subject to scanning again in the future.

If a file is found to have a virus, it will be listed in the **Quarantined files** tab of the AntiVirus screen, in the agent user interface. Users then have the option of “restoring” their access to Quarantined files.

Behavior-based AntiVirus Tagging

Many types of rules can assign a behavioral AntiVirus tag to an application when the application interacts with another application and attempts a certain activity. Behavior AntiVirus tags are “static.” The tags can be assigned to an application and they can be configured by the administrator but their names cannot be changed.

Based on the kind of interaction, the application can receive one of these tags:

- <Virus:Behavior.Excessive Policy Violations>
- <Virus:Behavior.Malicious Activity>
- <Virus:Behavior.Dangerous Activity>
- <Virus:Behavior.Suspicious Activity>
- <Virus:Behavior.Potential Unwanted Application>

An application can also be specifically assigned “no static tag.” If there are two rules with the same tagging requirements and one rule applies a “no static tag” and one rule applies one of the behavior static tags, the rule with the “no static tag” classification takes precedence and the application does not receive a static tag.

Applications that have an AntiVirus tag can be grouped in with application classes. This allows other rules to allow and restrict the activities of all the applications in a class the same way.

If an application receives a behavior-based AntiVirus tag, it will be listed in the **Quarantined files** tab of the AntiVirus screen, in the agent user interface. Users then have the option of “restoring” their access to Quarantined files.

The @virusscan Token

The **@virusscan** token is used in the content matching field of a file set. All tags, attributed to files because of AntiVirus scanning, are attributes of the **@virusscan** token. The **@virusscan** token allows a rule to refer to a group of files rather than naming them all specifically.

When associating a behavior-based AntiVirus tag with the **@virusscan** token, the syntax is **@virusscan=<behavior_based_tag_name>** For example:

```
@virusscan=<Virus:Behavior.Excessive Policy Violations>
```

See [Content Matching in File Sets, page 2-57](#) for more examples of @virusscan token syntax.

Quarantined Files

Files and applications are quarantined if they receive a signature-based AntiVirus tag or a behavior-based AntiVirus tag. Quarantined files remain in place and are rendered inert by the rules that govern quarantined files; they are not moved to a special directory.

Users see quarantined files in the Quarantined files tab, on the AntiVirus screen, of the agent's user interface. Through that interface, users can remove files from the quarantine list by "restoring" them and they can re-quarantine a file that they once restored. Users can also delete quarantined files.

Quarantined files are automatically deleted from the users system after 60 days if the following conditions are met:

- Automatic deletion only applies to files found to have a signature-based virus.
 - Files found to have behavior-based viruses will not be automatically deleted; they remain in the quarantine state.
 - Applications identified as PUA are not automatically deleted; they remain in the quarantine state. The PUA label is short for Potentially Unwanted Application. These applications are not malicious by themselves but can be used in a malicious or unwanted context. See <http://www.clamav.org/support/faq/> for more information about applications labeled PUA.
- The file is not touched by another user or application for 60 days.
- The file's status remains in quarantine for 60 days. For example, if a file is quarantined, restored, and then moved back to quarantined, the 60 day timer is reset when the file returns to the quarantined state.

After a quarantined file is deleted, an event is sent to the CSA MC.



Because quarantined files are restrained by AntiVirus rules, if security on the agent is turned off, the infected files become uncontrolled. They can be read, modified, or executed.

**Caution**

If the agent is reset, all files in the Quarantined files and Restored files lists are removed.

Differences Between Signature-based AntiVirus and Automatic Signature Generation

Signature-based AntiVirus protection in this release of CSA is a traditional antivirus security feature. It scans the contents of files and compares the content to a library of known virus signatures. If a file contains a virus, the file is rendered inert by CSA policies which prevent the file from being read, written to, or executed.

All local files are scanned periodically. Some files are scanned when they are opened or closed, based on rules in the *AntiVirus - Signature based* policies for desktops and servers. Regular updates of virus signature files are required to ensure that AntiVirus properly identifies the latest known viruses residing in files.

The Automatic Signature Generation feature is designed to protect MSRPC and LPC interfaces from buffer overflow and denial of service attacks. As one of these interfaces is being attacked, the Automatic Signature Generation feature dynamically creates a signature that identifies the attack. That signature is then used by rules to prevent other similar attacks.

Automatically generated signatures are created in real time, this feature does not depend on static signatures which you need to download periodically.

Administrative Signature-based AntiVirus Tasks

This section describes signature-based AntiVirus tasks CSA MC administrators perform.

Scheduling a Background Scan

Administrators can schedule AntiVirus background scans of all hosts that use the default *AntiVirus - Signature-based* provided with this release. These policies contain a rule that specifies which files will be scanned during a background scan. By default, files on fixed local drives are scanned during an AV background scan.

-
- Step 1** Log on the CSA MC as an administrator with configure privileges and switch to **Advanced Mode**.
- Step 2** From the **Systems** menu, in the CSA MC interface, navigate **Host Tasks > Host Scanning Tasks**.
- Step 3** Click **New**.
- Step 4** Give the task a **Name** and a **Description**.
- Step 5** Select **Enabled** if you want to enable this task immediately after rules are regenerated and software updates are distributed to hosts.
- Step 6** In the Configuration area, define the task:
- In the **Run this task** fields, choose to run this task every week and on a particular day of the week, or choose to run this task every month and on a particular day of every month.



Note We recommend weekly background scans of all hosts.



Note If a scan is scheduled on the 31st of the month, the scan will not be performed on months with fewer days.

- In the **At** field, specify the time of day the scan is to run. Time is expressed in twenty-four hour format.
- Check **Perform background AV search on all hosts in group** and select a group from the drop-down list. You can only specify one group for a background scan.

**Note**

Combining an AntiVirus scan with a Data Loss Prevention scan causes two separate system scans.

Step 7 Click **Save**.

You will then need to generate rules for the task to be distributed to all hosts in that group.

Performing an On-Demand AV Scan

An on-demand AV scan searches fixed drives on the host for files with AntiVirus tags. In order for an on-demand AV scan to work you need to have *Signature-based AntiVirus protection* enabled. See [Enabling AntiVirus Protection, page 15-3](#) for more information.

-
- Step 1** Log on to CSA MC as a user with configure or deploy privileges and switch to **Advanced Mode**.
 - Step 2** From the **Systems** menu, click **Hosts**.
 - Step 3** Click the link for the host on which you want to start an immediate scan.
 - Step 4** At the end of the **AV full-scan schedule** row, click **View AV Scan Results**.
 - Step 5** In the Scanning dialog box, click **AV Scan Results** if the tab is not open already.
 - Step 6** Click **Scan Now**. A polling hint is sent to the host, after the host receives the polling hint, the on-demand scan begins automatically. If the host does not receive the polling hint, the scan will begin the next time the host polls.

While the scan is in progress, you can click **Get Results** to receive the information gathered so far. After clicking Get Results, the agent on the host forwards the information it has collected the next time the agent polls.

When the on-demand scan is complete, the agent sends the results to the CSA MC automatically.

The AV Scan Results page refreshes the information it has periodically. Upon refresh, the latest information forwarded from the agent is displayed on the page.

Identifying a Host AntiVirus Scan Schedule

-
- Step 1** Log into the CSA MC as any level of user and switch to **Advanced Mode**.
 - Step 2** From the **Systems** menu, select **Hosts**.
 - Step 3** Click the link for the host you want to investigate.
 - Step 4** Expand the **Host Status** area.
 - Step 5** The **AV Full Scan Schedule** field identifies the scanning schedule for the host.

Forcing a Signature Update for a Group

-
- Step 1** Log into the CSA MC as a user with configure or deploy privileges and switch to **Advanced Mode**.
 - Step 2** From the **Systems** menu, select **Groups**.
 - Step 3** Click the link for the group which will receive the virus signature updates.
 - Step 4** In the Features area, click the link to **Force AV Update**. A green check mark flashes with the word Done to indicate that the agent has been notified to start an update.

Forcing a Signature Update for a Host

-
- Step 1** Log into the CSA MC as an administrator with configure or deploy privileges and switch to **Advanced Mode**.
 - Step 2** From the **Systems** menu, select **Hosts**.
 - Step 3** Click the link for the host for which you want to force a virus signature update.
 - Step 4** Expand the Host status area.
 - Step 5** In the **Time since last AV signature update** row, click the link to **Force AV Update**. A green check mark flashes with the word Done to indicate that the agent has been notified to start an update.

Creating Exemptions for AntiVirus Tags

AntiVirus exemptions can be created for signature-based AntiVirus tags that you have determined to be false positives. Creating an exemption for a tag prevents any files, that have been given the tag, from being restricted by AntiVirus rules that pertain to that tag. Creating an exemption for an individual file, with a particular AntiVirus tag, prevents that file from being restricted by AntiVirus rules that pertain to that tag.

You can create an exception for a virus tag through the **Event Management Wizard** or from scratch using the **AntiVirus Exemptions** page.

Here is an example of how an end-user and a CSA MC administrator would be affected by an AntiVirus exemption: Assume that files have been quarantined on various hosts because they have been tagged with an AntiVirus tag. The CSA MC administrator determines that the tag represents a false positive and then creates an exemption for that tag either using the wizard or by hand. The exemption is then listed on the AntiVirus Exemptions page on the CSA MC. When the administrator is ready, he or she generates rules.

The next time the host's CSA polls in to the CSA MC, it receives the AntiVirus exemption information. Within the next minute, any files with that AntiVirus tag that have already been quarantined are removed from the Quarantined files tab of the agent. The files are not put in the Restored tab. The AntiVirus exemption is global and individual users are not given the opportunity to re-classify the file as Quarantined.

Creating AntiVirus Exemptions Using the Event Management Wizard

-
- Step 1** Log on to the CSA MC as a user with configure privileges. You can perform this task in either Simple Mode or Advanced Mode.
 - Step 2** From the **Events** menu, select **Event Log**.
 - Step 3** Find the event that identifies the virus and quarantines the file because of the presence of the virus. Click the **Wizard** link for the rule.
 - Step 4** Different rules act on a file with an identified virus in different ways. When the wizard launches, accept the suggested action presented by the wizard. When given the option to remove a file from quarantine, you have these options:
 - In the **Remove from AV Quarantine** area, select one of these two radio buttons:

- **All Windows files** - This allows you to exempt every file, with the specified AntiVirus tag, from being restricted by AntiVirus rules that pertain to that tag. This is the default setting offered by the wizard.
- **Only this Windows file** - This allows you to exempt the file identified by the wizard from being restricted by AntiVirus rules because it has the specified tag.

You can modify the file location with two wildcards (**) to generalize where this file might be found. For example:

**\Documents and Settings\Administrator\Desktop

\Temp\virus.doc

indicates the virus.doc file on Administrator's desktop.

**\Desktop\Temp\virus.doc

indicates virus.doc on any desktop.

- In the **Justification** field, explain why you are creating the AntiVirus exemption.
- Under the Justification field is a link to **Report the file as false-positive to Cisco/ClamAV**. Clicking the link opens up the default email client available on the host. See [Reporting ClamAV False Positive Viruses to Cisco, page 15-16](#) for more information.

Step 5 Click **Finish** to exempt the file from further AntiVirus enforcement rules.

Step 6 **Generate rules** after clicking finish to deploy the exemption to the host. The exemption is listed in the global **AntiVirus Exemptions** page on the CSA MC. You can reach this page by mousing-over the **Configuration** menu and navigating **Global Settings > AntiVirus Exemptions**.

After rules are generated, the host receives a polling hint, automatically polls in to the CSA MC, and receives the exemption information for this AntiVirus tag. In this case, the exempted files would be removed from the **Quarantine** tab of their local agent and, because the AntiVirus tag was exempted by the CSA MC, the files are not placed in the Restored files tab.

Creating AntiVirus Exemptions Using the Global AntiVirus Exemptions Page

Step 1 Log on to the CSA MC as a user with configure privileges. You can perform this task in either Simple Mode or Advanced Mode.

Step 2 From the **Configure** menu, navigate **Global Settings > AntiVirus Exemptions**.

Step 3 Click **New**. The **Edit AntiVirus Exemption** dialog box opens.

Step 4 Select one of these two radio buttons:

- **All Windows files** - This allows you to exempt every file, with the specified AntiVirus tag, from being restricted by AntiVirus rules that pertain to that tag. This is the default setting offered by the wizard.
- **Only this Windows file** - This allows you to exempt the file identified by the wizard from being restricted by AntiVirus rules because it has the specified tag.

You can specify wildcards at the beginning of the path to indicate “all drives” but you may not specify wildcards in any other part of the directory path. For example:

```
**\Documents and Settings\Administrator\Desktop\virus.txt
```

Step 5 In the **With content matching virus** field, enter the name of the AntiVirus tag you want to exempt from being placed in quarantine. The name has to match exactly to be exempted. Obtain the virus name from the event text.

Step 6 In the **Justification** field, enter a short explanation of why you are creating an exemption for this virus tag.

Step 7 Click **Save**.

Step 8 **Generate rules** to deploy the exemption. The exemption is listed in the global AntiVirus exemptions page on the CSA MC.

Reporting ClamAV False Positive Viruses to Cisco

You can report ClamAV false positives to Cisco as you create an AntiVirus exemption using the Event Management Wizard. See [Creating AntiVirus Exemptions Using the Event Management Wizard](#), page 15-14 for this procedure. Clicking the link to **Report the file as false-positive to Cisco/ClamAV** opens up the default email client and provides a partially composed email with additional instructions.

The email’s address field is pre-populated with cса-clamav-falsepositive@cisco.com. The false positive report lists the filename “infected” with the false positive, the name of the reported infection, and the version of CSA that found the infection.

Before sending the email, please compress the file “infected” with the false positive virus and attach the compressed file to the email.



- Note** In order to report the ClamAV false positive to Cisco, you must have the email client configured on the host from which you intend to send the email.
- Reporting false positives is best performed from a remote host that can access CSA MC using a web browser. If you attempt to report false positives while logged on to the server on which the CSA MC is installed, you may need to reconfigure the rules in the *CSA Management Center policy* in order to allow the email to be sent.

A false positive occurs when CSA classifies a file or application as being infected by a virus when it is not. When members of the user community report examples of ClamAV false positives to Cisco, these examples are analyzed and if the false positive virus is accepted by the ClamAV signature writers, it is added to ClamAV's database and distributed to the greater ClamAV user community. This makes the AntiVirus scanning faster and more efficient for everyone using ClamAV.

AntiVirus Reporting

You can generate reports that describe the age of signature libraries on hosts, the number and type of viruses infecting hosts, and the location of infected files. See [Clam AntiVirus Reports, page 11-9](#) the for the AntiVirus reports you can generate.

Creating Signature-based AntiVirus Rules and Components

The *AntiVirus - Signature based* policies for desktops and servers are provided by default with this release of CSA. They includes rules that scan files and applications for viruses, and rules to protect the host from files and applications that are infected with viruses.

If you want to create customized rules and file sets for your enterprise, this section provides procedures to do that.

Creating Virus Scanning Rules

There are two types of rules that, when triggered, scan files for viruses:

- File Access Control Rule (FACL)
- Application Control Rule (APCR)

Creating File Access Control Rules to Scan Files

Use file access control rules to trigger AntiVirus scans on files. Generally, by using a FACL, you can trigger a virus scan on a file when an application has opened or closed it, the application has attempted to read or write the file, and the attempt to read or write the file has been allowed or denied by CSA.

**Note**

See [Configuring Rule Modules, page 5-4](#) to create your own rule module into which you will put this rule.

-
- Step 1** To add rules to your module, expand the **Rules** area of the rule module configuration screen and click the **Add** button. A pop-up list of the available rule types appears.
- Step 2** Select **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** In the **Take the following action list box**, select **Set** from the pulldown list.
- Step 5** In the Attributes list box, select **Virus scan on CLOSE** or **Virus scan on OPEN**. See [Attribute: Virus scan on CLOSE, page 5-38](#) or [Attribute: Virus scan on OPEN, page 5-39](#) for descriptions of these set attributes.

Step 6 In the Value field select **NOT being required for this file** to prevent a file from being scanned for viruses or **Being required for this file** to require that the file be scanned for viruses.

Step 7 Enable the **Log** checkbox to turn logging on for this rule. Generally, you will not want to turn logging on for these set rules.

Step 8 When —

- **Applications in any (or all) 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 control. You may also create a new application class by clicking the blue **New** link next to the application class list box. For application class configuration details, see [Chapter 8, “Using Application Classes”](#)

If you choose **Applications in any of the following selected classes** the rule will affect an application that is a member of one of the selected application classes.

If you choose **Applications in all of the following selected classes**, the rule will affect an application that is a member of every application class you select.

- **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. You may also create a new application class by clicking the blue **New** link next to the application class list box.



Note

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

Step 9 Attempt the following operations—In this step, you specify the file operation that the application you are controlling is attempting.

If you are creating a **Scan on OPEN** rule, you must select both the **Read File** and **Write File** operations you are allowing or denying on the files named in the **On any of these files** box. If you are creating a **Scan on CLOSE** rule, you can only select the **Write File** operation.

For either Scan on OPEN or Scan on CLOSE, you can also choose the “Write” directory operation. The Write actions you are allowing or denying are **Create**, **Delete**, and **Rename**. Refer to File and Directory protection in [Using the Correct Syntax, page 2-41](#).

**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 10 On any of these files—In this step you configure the files you want to scan for viruses.

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 2-41](#).

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)
```

For network machines (Windows only), enter:

```
\\\<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 9-12](#).



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 globally quarantined files** link on the Global Event Correlation page. See [Manage Dynamically Quarantined Files and IP Addresses, page 7-10](#) for more information.

Step 11 And — In this area specify, the enforcement action taken by CSA.

Specifying **Allow by default** or **Allow if triggered by a rule** scans files that applications have been allowed to read or write by other rules. Specifying **Terminated** or **Denied by rule** scans files that other applications have been prevented from acting on.

Step 12 When you are finished configuring your File access control rule, click the **Save** button.

This rule is now part of your rule module. It takes effect when the rule module is attached to a policy, the policy is attached to a group and then downloaded by an agent on the network.



Note In order to distribute rules to the correct hosts, you must associate policies with groups and then Generate rules. See [page 5-16](#) for instructions.

Creating Application Control Rules to Scan Files

Use application control rules (APCR) to trigger virus scans on applications. Generally, by using an APCR, you can trigger a virus scan on “Application B” when there is an attempt to run it by “Application A” and the operation has been allowed or denied by CSA.



Note See [Configuring Rule Modules, page 5-4](#) to create your own rule module into which you will put this rule.

-
- Step 1** To add rules to your module, expand the Rules area of the rule module configuration page and click the **Add** button. 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.
- 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** In the **Take the following action list box**, select **Set** from the pulldown list.
- Step 5** In the Attributes list box, select **Virus scan**. See [Attribute: Virus scan, page 5-37](#) for descriptions of this set attribute.
- Step 6** In the Value field select **NOT being required for this application** to prevent a an application from being scanned for viruses or **Being required for this application** to require that the application be scanned for viruses.
- Step 7** Enable the **Log** checkbox to turn logging on for this rule. Generally, you will not want to turn logging on for this set rule.



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 8** **When** — In this step, specify the application that will attempt to run the application that you want to scan. You are not scanning the application you specify in this step.
- **Applications in any (or all) of the following selected classes**

If you want to scan an application running on a system, no matter how it is invoked, allow “All Applications” to remain selected by default.

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).

If you choose **Applications in *any* of the following selected classes** the rule will affect an application that is a member of one of the selected application classes.

If you choose **Applications in *all* of the following selected classes**, the rule will affect an application that is a member of every application class you select.

You may also create a new application class by clicking the blue **New** link next to the application class list box. For application class configuration details, see [Chapter 8, “Using Application Classes”](#)

When your rule is configured, currently selected application classes appear at the top of the list. See [Configuring Static Application Classes, page 8-8](#) 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. You may also create a new application class by clicking the blue New link next to the application class list box.

Step 9 attempt to run — In this step, configure the application that you want to scan for viruses.

- **New applications in *any* of the following selected classes**—Select the application you want to scan if an attempt is being made to run it by the application defined by the **Applications in *any* (or *all*) of the following selected classes** field.

If you choose **New applications in *any* of the following selected classes** the rule will control an application that is a member of one of the selected application classes.

If you choose **New applications in *all* of the following selected classes**, the rule will affect an application that is a member of every application class you select.

If you selected “All Applications” in the top application field, selecting “All Applications” in this second field will cause a scan of any file or application when any application launches any file or application. This will significantly diminish the performance of the host.

- **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 10 And — In this area specify, the enforcement action taken by CSA.

Specifying **Allow by default** or **Allow if triggered** by a rule scans applications that have been allowed to run by other rules. Specifying, **Terminated** or **Denied by rule** scans applications that have been prevented from running by other rules.

Step 11 When you are finished configuring your Application control rule, click the **Save** button. This rule is now part of your rule module. It takes effect when the rule module is attached to a policy, the policy is attached to a group and then downloaded by an agent on the network.

Creating File Sets That Refer to Infected Files

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.

In the case of the AntiVirus feature, the file set defines what files your FACL will scan for viruses. The *File Content - Virus - All signatures* file set, provided by default in this release, represents any file in any directory that has been tagged as containing any virus. If you want to create a file set that represents a specific virus, follow this procedure:

Step 1 From the menu bar **Configuration** drop-down list, mouse over **Variables** and select **File Sets**.**Step 2** Click the **New** button to create a new file set.

Step 3 If you have not configured an operating system preference for your administrator account, click **Windows** in the pop-up box. If you have configured an operating system preference for your administrator account, the new file set will automatically be created for that operating systems. This takes you to the file set configuration view (see [Figure 9-3](#)).

Step 4 In the available edit fields, enter the following information (See [Using the Correct Syntax, page 2-41](#). 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.
- **OS**—Optionally, you can select to target an operating system more narrowly by selecting a specific Windows operating system from the **OS** list box.

Step 5 **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:

Windows example:

```
c:\Program Files\**\*SQL*\bin\**  
\Program Files\**\*SQL*\bin
```



Note See [Using the Correct Syntax, page 2-41](#) for details for information on protecting directory paths and files.

Step 6 **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.

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 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 8 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 7-10](#) for more information.

Step 9 Content matching — The Content matching field allows you to describe a set of files that all have the same AntiVirus tag. The entry for each AntiVirus tag is placed on its own line in the Content matching box and must conform to the syntax for @virusscan tokens described in [Using the Correct Syntax, page 2-41](#).

- a. Next to the Content matching edit fields, click the **Insert content** link. The **File Content Selector** pop-up opens.
- b. In the Scan type field, select **Virus scanning**.
- c. In the Tag field, type the virus tag name and click **OK**.

If you prefer, you can also edit the Content matching field directly by clicking in the edit box. 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. Be sure to follow the syntax guidelines for the @virusscan token described in [Using the Correct Syntax, page 2-41](#).

- d. When you have added all the virus scanning tags, close the File Content Selector pop-up box.

Step 10 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 In the Tasks menu 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.

Configuring Behavior-based AntiVirus Policy

The rules in the rule modules that comprise the *AntiVirus - Behavior based* policies for desktops and servers are complex and have many interdependencies. Instead of creating your own behavior-based AntiVirus rules and components, we strongly recommend that you deploy the *AntiVirus - Behavior based* policies that are provided with this release.

This policy requires a minimal amount of configuration before it is deployed. To configure the policy, follow this procedure:

-
- Step 1** Logon to the CSA MC as a user with configure privileges.
 - Step 2** From the **Configuration** menu, select **Host Security**.
 - Step 3** Expand the Group to which you want to deploy the policy.
 - Step 4** Check the box for the *AntiVirus - Behavior based* policy.
 - Step 5** Click the red **warning** link after the policy name.
 - Step 6** Click the links for the rules you need to configure and save each one after you configure it. If you need help configuring the rules, click the help icons next to the fields that require configuration.
 - Step 7** **Generate** rules. Users will receive the updated policy when they next poll in or when they download the agent kit for the group.

End-user AntiVirus Tasks

End-users have some local control over the AntiVirus feature. Users can perform these tasks if their host is protected with AntiVirus policies:

- Start an On-demand virus scan.
- Change a file's quarantine status.
- Delete quarantined files.
- Force an AntiVirus signature update.

See the “[AntiVirus Protection](#)” section on page A-17 for more information about how users can perform these tasks. Users can also view these procedures by clicking the AntiVirus icon in the Tasks panel of the agent user interface and then clicking the help icon.



CHAPTER **16**

Data Loss Prevention

Overview

Data on network endpoints is increasingly subject to internal policies and external regulations concerning proprietary and confidential information. The process of data classification assists network data security by helping track the existence of sensitive data, its location in the enterprise, how that data is being accessed, and how it must be protected to meet legal and regulatory requirements.

Cisco Security Agent's new Data Loss Prevention (DLP) feature includes these capabilities:

- Classification and tagging of a file based on the result of a content scan or its location on the host system.
- Classification and tagging of a file based on what applications attempt to read or write it.
- User notification when users are working with content that is considered sensitive. Raising awareness of the presence of sensitive data will help prevent accidental data loss.

The DLP feature enables CSA to tag files based on several types of file content, including specific characters or phrases. CSA also provides optimized pattern matching for credit card numbers and Social Security numbers, which are especially sensitive and subject to government regulatory control.

Identification of sensitive data and control over sensitive data can be customized on the CSA MC to assist in the implementation of Data Loss Prevention controls for use of data in compliance with your organization's policies.

This chapter contains these sections:

- [Data Loss Prevention Basics, page 16-3](#)
 - [Enabling Data Loss Prevention Protection, page 16-3](#)
 - [Scanning Data Tags and Static Data Tags, page 16-4](#)
 - [Scanning Data Tag Search Patterns, page 16-5](#)
 - [The @datascan Token, page 16-9](#)
- [Managing Scanning Data Tags, page 16-9](#)
 - [Data Classification - Scanning Data Tags List Page, page 16-9](#)
 - [Built-In Data Scanning Tags, page 16-11](#)
 - [Creating a Scanning Data Tag, page 16-11](#)
 - [Editing a Scanning Data Tag, page 16-12](#)
 - [Cloning a Scanning Data Tag, page 16-13](#)
 - [Deleting a Scanning Data Tag, page 16-14](#)
- [Managing Static Data Tags, page 16-14](#)
 - [Data Classification - Static Data Tags List Page, page 16-14](#)
 - [Adding Descriptions to Static Data Tags, page 16-15](#)
 - [View References to Static Data Tags, page 16-15](#)
- [Data Loss Prevention Scanning Tasks, page 16-16](#)
 - [Scheduling a Background DLP Scan, page 16-16](#)
 - [Performing an On-Demand DLP Scan, page 16-17](#)
 - [Identifying a Host's DLP Scan Schedule, page 16-18](#)
 - [Identifying a Group's DLP Scan Schedule, page 16-18](#)
- [Data Loss Prevention Reporting, page 16-19](#)
- [Creating Data Loss Prevention Rules and Components, page 16-19](#)
 - [Creating File Access Control Rules to Apply Scanning Data Tags, page 16-19](#)
 - [Creating File Access Control Rules to Apply Static Data Tags, page 16-22](#)

Data Loss Prevention Basics

This section describes the basic concepts of CSA's Data Loss Prevention (DLP) feature.

Enabling Data Loss Prevention Protection

The Data Loss Prevention feature is available for Windows desktop platforms only. To enable Data Loss Prevention protection, you need to perform these tasks:

1. Install the DLP license

Before CSA MC distributes data scanning rules to a host, CSA requires a DLP license key in addition to the standard CSA desktop host key. Data Loss Prevention license files are named **DLP Desktop Agent Upgrade** and are available in bundles from 25 to 10,000 seats.

With the license in place, CSA can tag files with scanning data tags and static data tags, CSA can gather information on files with those tags, and CSA can enforce rules that consider a file's tag.

If you have not done so already, you can upload a data loss prevention license to the CSA MC by following this short procedure:

-
- Step 1** Log on to the CSA MC as a user with configure or deploy privileges.
 - Step 2** Click **Home** to go to the Home page.
 - Step 3** Click **Update License Information**.
 - Step 4** Browse to the location of the DLP license file, and click **Upload**.

2. Configure the DLP policies for the groups you want to protect

-
- Step 1** Open the **Host Security** page.
 - Step 2** Expand the Group that you want to protect with DLP. You should find that the Data Loss Prevention policy is listed with your group but its checkbox is probably not checked and may even be grayed-out.

- Step 3** Click the red **warning** link next to the Data Loss Prevention policy name.
- Step 4** Configure and save any rules that require customization.
- Step 5** Click the checkbox for the Data Loss Prevention policy and click **Save** on the Host Security page.
- Step 6** **Generate rules.** After you have configured the DLP license, generate rules. The DLP policy will be distributed to the hosts in the group when they next poll in.

**Tip**

If you want to distribute the Data Leakage Prevention policy quickly, send a polling hint to the group.

Scanning Data Tags and Static Data Tags

There are two types of data tags: scanning data tags and static data tags. Scanning data tags can be assigned to a file based on its contents. Static data tags can be assigned to a file based on what applications use that file.

Scanning Data Tags

A **scanning data tag** is assigned to a file if CSA has scanned the contents of the file and matched a pattern in the file to a pattern defined on the **Data Classification - Scanning Tags** page.

You can create scanning data tags representing any string of characters you decide to search for. (See [Text-matching Search Patterns, page 16-6](#) for more information.) There are also pre-configured, “built-in” scanning tags that are provided by default.

The “built-in” scanning data tags are defined by pre-configured patterns that are used to find Social Security numbers and credit card numbers. CSA uses a special number-scanning algorithm to identify these numbers in files while, at the same time, differentiating them from other large numbers. For example, CSA can distinguish between a file containing nine digit part numbers and a file containing Social Security numbers with a high degree of accuracy.

If more than one type of pattern is found in a file, the file is tagged with more than one scanning tag.

After a file has received a scanning data tag, other rules can govern how users are allowed to interact with that file. Users may also be notified if they are using a file with sensitive information. Making users aware of the kind of files they access helps to prevent accidental data loss.

See [Creating a Scanning Data Tag, page 16-11](#) for an explanation of how to create scanning data tags.

**Note**

There is support in the default Data Loss Prevention policies for the <Regulatory Controlled> and <Proprietary Information> tags. If you assign one of these two tags, then the default Data Loss Prevention policies will restrict the behavior of the tagged files. If you assign a tag other than one of these two, then you must create your own rules that govern the behavior of these tagged files.

Static Data Tags

A **static data tag** can be assigned to a file if a particular application accesses the file. **Static data tags** are built-in data tags distributed with this release and are listed on the **Data Classification - Static Data Tags** page on the CSA MC. You cannot change the names of these tags and you cannot create new static data tags.

You define the rules, based on your enterprise's needs, that assign static data tags to files. There are no Data Loss Prevention policies that come pre-configured to assign static data tags to files.

Static data tagging can be useful if, for example, you have a specialized application. Perhaps your enterprise is a hospital and you know in advance that any file that your specialized application reads falls under HIPAA guidelines. There is a <HIPAA Controlled> static data tag that you can apply to the file. This type of tagging method may also be useful when a file type is not scanable for a text-matching pattern, such as an audio file or a graphics file.

See [Creating File Access Control Rules to Apply Static Data Tags, page 16-22](#) for more information.

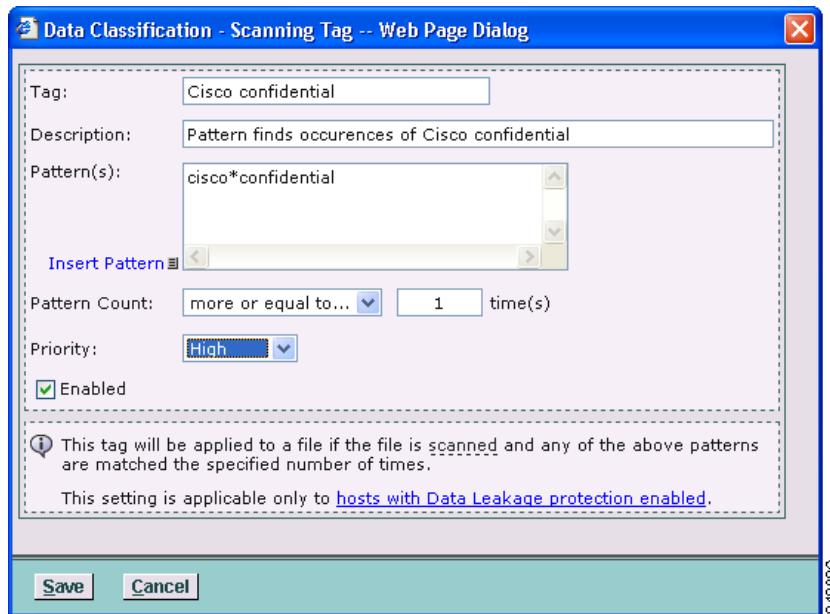
Scanning Data Tag Search Patterns

The **Patterns** field of the **Data Classification - Scanning Tag** pop-up is where you specify the pattern that your content tag represents. See [Figure 16-1](#).

The two types of patterns can be specified in this field:

- Text-matching Search Patterns
- Built-In Scanning Patterns

Figure 16-1 Data Classification - Scanning Tag dialog



Text-matching Search Patterns

Text-matching patterns can contain any strings of characters or numbers specified by the administrator.



Note

In general, long text-matching patterns usually will be more effective than short patterns. Searching for long text-matching patterns prevents CSA from assigning content tags to files that you did not expect or intend to match. For example, by searching for the pattern Company confidential. For internal use only CSA is more likely to find and tag files that are truly confidential than if your pattern was only the word confidential.

These are the syntax requirements for character-matching search patterns:

- CSA's string-searches support English, and languages other than English, whose character sets can be represented by 2-byte UNICODE text-encodings. (Currently, this excludes Asian and Semitic languages.) We also support accented Latin, Greek, and Cyrillic characters, as long as each letter and its accents are included within a single two-byte character.



Note In order to match strings with accented characters, the string must be entered twice using both the “combined encoding” and the “pre-composed encoding” UNICODE formats.

- Text-matching patterns are not case sensitive. For example, the pattern `cisco` will match `Cisco` and `cisco`.
- A text-matching pattern can be no more than 256 characters long including wildcards. For example, the pattern: `confidential*` is 13 characters long.
- The smallest text-matching pattern you can search for, not including wildcards, is two characters long.
- A text-matching pattern, by default, can only match a whole word or phrase, and not part of a word. Therefore, a pattern such as `confidential` will not match the word `nonconfidential` in a file.
- Wildcards, represented by a `*`, can be used to match prefixes and suffixes of a word as well as character strings in between other strings. Here are some other examples:
 - The pattern `*confidential` matches `nonconfidential`.
 - The pattern `confidential*` matches `confidentiality`.
 - The pattern `*confidential*` matches `nonconfidentiality`.
 - The pattern `confidential` does not match `nonconfidential`, `confidentiality`, or `nonconfidentiality`.
- If multiple words are specified, and they are included on the same line in the Patterns field, they must appear in the same order in the target file to be considered a match. If words are entered on separate lines, the presence in the file of any of the lines in the Patterns field, in any order, is considered a match.

- A wildcard can be used in the middle of a string with more than one word. In this case the wildcard breaks the pattern into three parts: the string before the wildcard, the wildcard, and the string after the wildcard.
CSA will match the pattern, `Cisco*confidential`, to a string that begins with `Cisco`, ends with `confidential` and has no more than 50 characters in between `Cisco` and `confidential`. For example `Cisco*confidential` will match `Cisco Security Agent - Company Confidential` because “`Security Agent - Company`” is only 26 characters long.
- Numeric strings are matched like alphabetic strings. The whole string in the Patterns field must be matched exactly in the file to record a match; if there is more than one number on a line in the Patterns field, that entire string must be present in the target file to make a match; and wildcards may be used to match longer strings of numbers.

**Tip**

Though wildcards can be used to match strings of numbers, if you use wildcards, you may end up matching other alpha-numeric strings that you did not expect or intend to match with your string. Entering exact strings of numbers in the Patterns field will produce the most accurate results.

These are examples of using wildcards with numbers:

- The pattern `9785551234` will only match `9785551234`.
- The pattern `5551234` will not match `9785551234`.
- The pattern `*5551234` will match `9785551234`.
- The pattern `*8555123*` will match `1234978555123456789`.
- The pattern `978*` will match `9785551234` as well as many other alpha-numeric string that you may not have intended on matching.

Built-In Scanning Patterns

CSA contains two “built-In” scanning patterns, `@ssn` and `@credit_card`. These patterns use special number-scanning algorithms contained in CSA. The `@ssn` search pattern is optimized to identify patterns of valid Social Security numbers issued by the United States federal government. The `@credit_card` pattern is optimized to identify valid credit card numbers used by major credit card issuers. These search patterns also distinguish Social Security numbers and credit card numbers from other long numbers to limit the number of false matches.

The @datascan Token

The **@datascan** token is used in the **Content matching** field of file sets and the **Data Classification** area of system state sets to identify files that have received a scanning data tag or static data tag. Using the **@datascan** token allows rules to refer to a group of files rather than individual files. The syntax for defining a scanning classification tag for these variables is in [Data Classification \(DLP\) Tag Token Syntax, page 2-58](#).

Managing Scanning Data Tags

Scanning Data Tags are managed through the CSA MC. The **Data Classification - Scanning Data Tags** list page is accessible from the menu bar by navigating **Configuration > Global Settings > Data Classification - Scanning Data Tags**.

This page lets you manage scanning data tags that are applied to files after a rule matches a text-matching search pattern or a built-in search pattern. Some built-in scanning data tags are provided by default with this release.

You can perform several administrative tasks from this page. See these procedures for more information:

- [Creating a Scanning Data Tag, page 16-11](#)
- [Editing a Scanning Data Tag, page 16-12](#)
- [Cloning a Scanning Data Tag, page 16-13](#)
- [Deleting a Scanning Data Tag, page 16-14](#)

Data Classification - Scanning Data Tags List Page

The **Data Classification - Scanning Data Tags** list page describes tags by displaying these columns of information:

- **Tag:** This is the name of the tag that identifies a pattern of text. The tag is applied to a file that contains the pattern of text specified for the tag. This tag name will be visible to you when creating variables such as file sets or system state sets.

- **Pattern:** This field displays the string of text that CSA searches for when performing a data scan. Once the pattern is located, the tag that identifies this pattern is applied to the file that contains the pattern.
- **Occurrences:** Describes the number of times a pattern has to be found in a file for the file to be tagged as having that pattern.

For built-in numeric patterns such as @ssn or @credit_card, CSA uses a proprietary algorithm to determine if a file has a legitimate concentration of social security numbers or credit card numbers and not other kinds of long numbers. This strives to prevent, for example, a database of part numbers as being mistaken for a database of social security numbers or credit card numbers.

- **Description:** Displays the description for your tag for informational purposes.
- **Version:** Displays the version of CSA with which the tag was supplied. By clicking the column heading, the entries can be filtered to show tags from all versions, only those tags that have been user-defined, or those from a particular release.
- **Priority:** If the CSA database has entries for many tagged files and the database is getting too big, the entries for the files tagged with the high-priority tags remain in the database and the entries for the files with the lowest priority tags are discarded.
- **Status:** A data tag is either “enabled” and CSA actively scans for it, or it is “disabled” and CSA does not scan for it.
- **In Use:** A data tag is in use if it is specifically referenced by at least one variable such as a file set or a system state set. If the tag is only referenced by variables that reference all data tags, for example, @datascan=<*>, the tag is not considered to be in use.

To find out which variable uses the tag, click in the row that describes the data tag, click the **Tasks** button in the **Data Classification - Scanning Tag** dialog, and click **View references**. A list of file sets is displayed.

A data tag that is “In Use” cannot be deleted without first deleting the variable that references the tag.

Built-In Data Scanning Tags

Files are given scanning data tags if CSA has scanned the file and matched pattern in the file. CSA provides these built-in data scanning tags by default:

- **<credit_card>**: The <credit_card> tag uses @credit_card, which is a number scanning search pattern built into CSA. The @credit_card search pattern is optimized to identify patterns of valid credit card numbers used by major credit card issuers.
- **<Proprietary Information>**: The <Proprietary Information> tag is assigned to a file if CSA matches the exact phrase “Company Confidential” or “Internal Use Only” a certain number of times, in a scanned file. However, before files can be tagged with the <Proprietary Information> tag, your CSA administrator needs to edit the pattern to make sure it is appropriate for your enterprise, before enabling the tag.
- **<SSN>**: The <SSN> tag uses @ssn, which is a number scanning search pattern built into CSA. The @ssn search pattern is optimized to identify patterns of valid Social Security numbers issued by the United States federal government. A <SSN> tag is assigned to scanned data if CSA finds valid Social Security numbers in the data.
- **<Regulatory Controlled>**: The <Regulatory Controlled> tag is assigned to files in which the @credit_card or @ssn patterns are found. A <Regulatory Controlled> tag is assigned to scanned data if CSA finds valid credit card numbers or Social Security numbers in the data.

Creating a Scanning Data Tag

This kind of tag would be applied to a file after a “Data scan on OPEN” or “Data scan on CLOSE” FACL triggers a scan on a file and CSA finds the pattern specified by the data classification tag.

-
- Step 1** Log on to the CSA MC as a user with configure privileges. This procedure may be done by either a Simple Mode or Advanced Mode user.
- Step 2** From the **Configuration** menu, navigate **Global Settings > Scanning Data Tags**.
- Step 3** Click **New**. The **Data Classification - Scanning Tag** dialog opens.

- Step 4** In the **Tag** field, enter a tag name. Only alphanumeric characters, underscores, hyphens, parentheses and periods may be used in a tag name.
- Step 5** Optionally, in the **Description** field, enter a description of the pattern.
- Step 6** In the **Patterns** field, enter a combination of a text string, a numerical string, or a built-in pattern chosen by clicking **Insert Pattern** (@credit_card and @ssn are the preselected patterns available). The pattern list cannot be empty. See “[Scanning Data Tag Search Patterns](#)” section on page 16-5 for how to enter a string in the Patterns field.

**Note**

In order to match strings with accented characters, the string must be entered twice using the “combined encoding” and the “pre-composed encoding” UNICODE formats.

- Step 7** In the **Pattern Count** field, specify the number of times the pattern must be found in a file for the file to receive the tag.
- Step 8** In the **Priority** field, select a priority for the scanning data tag. If the CSA database has entries for many tagged files and the database is getting too big, the entries for the files tagged with the high-priority tags remain in the database and the entries for the files with the low priority tags are discarded.
- Step 9** Select the **Enabled** check box to enable the tag.
- Step 10** Click **Save** to save the tag. The tag will be available after rules are generated and distributed to hosts when they poll in to the CSA MC.

Editing a Scanning Data Tag

- Step 1** Log on to the CSA MC as a user with configure privileges. This procedure may be done by either a Simple Mode or Advanced Mode user.
- Step 2** Click the link for an existing scanning data tag. The **Data Classification - Scanning Tag** dialog opens.
- Step 3** If a tag is not in use, you can change its name. If a Tag is “in use” then it is referenced by some other component or rule. In that case, you must click **Allow tag change** to rename the tag. Only alphanumeric characters, underscores, hyphens, parentheses and periods may be used in a tag name.

**Note**

Changing the name of the tag on this page does not change the name of the tag globally. If you want the components and rules that use the old tag name to use the new tag name, you need to edit those items individually.

- Step 4** Optionally, in the **Description** field, enter a description of the pattern.
- Step 5** In the **Patterns:** field, enter a combination of a text string, a numerical string, or a pre-selected pattern chosen by clicking on **Insert Pattern** (@credit_card and @ssn are the pre-selected patterns available). The pattern list cannot be empty. See “[Scanning Data Tag Search Patterns](#)” section on page 16-5 for how to enter a string in the Patterns field.

**Note**

In order to match strings with accented characters, the string must be entered twice using the “combined encoding” and the “pre-composed encoding” UNICODE formats.

- Step 6** In the **Pattern Count** field, specify the number of times the pattern must be found in a file for the file to receive the tag.
- Step 7** In the **Priority** field, select a priority for the scanning data tag. If the CSA database has entries for many tagged files and the database is getting too big, the entries for the files tagged with the high-priority tags remain in the database and the entries for the files with the low priority tags are discarded.
- Step 8** Select the **Enabled** check box to enable the tag, clear the Enabled check box to disable the tag.
- Step 9** Click **Save** to save your changes. The tag will be available after rules are generated and distributed to hosts when they poll in to the CSA MC.

Cloning a Scanning Data Tag

- Step 1** Log on to the CSA MC as a user with configure privileges. This procedure may done by either a Simple Mode or Advanced Mode user.
- Step 2** Click the link for an existing scanning data tag. The **Data Classification - Scanning Tag** dialog opens. Select the checkbox to the left of the tag to be cloned. Only one tag may be cloned at a time.

- Step 3** Click “Clone”, then select “OK”. A new tag will appear in the Data Classifications - Scanning Tags screen, with a <new> marker next to the tag name. The cloned tag may then be edited by following the steps in [Creating a Scanning Data Tag, page 16-11](#).

Deleting a Scanning Data Tag

-
- Step 1** Log on to the CSA MC as a user with configure privileges. This procedure may done by either a Simple Mode or Advanced Mode user.
- Step 2** Select the checkbox to the left of the tag(s) to be deleted.
- Step 3** Click **Delete**, then select **OK** if you are sure you want the tag(s) to be deleted.



Note

Scanning data tags that are “In Use” can not be deleted without first deleting the variable that references the tag.

Managing Static Data Tags

Static Data Tags are assigned to files based on what group of applications attempt to access them.

The Static Data Tags list page is accessible from the menu bar by navigating **Configuration > Global Settings > Static Data Tags**. This page helps you identify in what rules and variables these static data tags have been referenced.

You can perform two administrative tasks from this page. See these procedures for more information:

- [Adding Descriptions to Static Data Tags, page 16-15](#)
- [View References to Static Data Tags, page 16-15](#)

Data Classification - Static Data Tags List Page

The **Data Classification - Static Data Tags** list page describes tags by displaying these columns of information:

- **Tag:** This is the name of the tag given to the file after a particular application has accessed it. This tag name will be visible to you when creating variables such as file sets or system state sets.
- **Description:** Displays the description for your tag for informational purposes.
- **In Use:** A data tag is **in use** if it is specifically referenced by at least one variable such as a file set or a system state set. If the tag is only referenced by variables that reference all data tags, for example, @datascan=<*>, the tag is not considered to be in use.

To find out which variable uses the tag, click in the row that describes the data tag, click the **Tasks** button in the Data Classification - Scanning Tag dialog, and click **View references**. A list of file sets is displayed.

The attributes of a static tag are defined by a file access control rule that you create. See [Creating File Access Control Rules to Apply Static Data Tags, page 16-22](#) for a procedure to define the attributes of a static tag.

Adding Descriptions to Static Data Tags

- Step 1** Log on to CSA MC and switch to **Advanced Mode**.
- Step 2** From the **Configuration** menu, navigate **Global Settings > Static Data Tags**.
- Step 3** In the **Data Classification - Static Tags** list page, click the link for the static data tag you want to describe.
- Step 4** Enter your description in the **Description** field and click **Save**.

View References to Static Data Tags

- Step 1** Log on to CSA MC and switch to **Advanced Mode**.
- Step 2** From the **Configuration** menu, navigate **Global Settings > Static Data Tags**.
- Step 3** In the **Data Classification - Static Tags** list page, click the link to the static data tag for which you want to view references.
- Step 4** Expand the **Tasks** menu and click **View References**.
- Step 5** Click a link to follow the reference.

Data Loss Prevention Scanning Tasks

Data Loss Prevention scans can be scheduled or performed “on-demand.”

**Note**

Background and on-demand scans do not change a file’s modification date.

Scheduling a Background DLP Scan

Administrators can schedule weekly or monthly background scans of all hosts that use the default **Data Loss Prevention - desktops** policy provided with this release. This policy contains a rule that specifies which files will be scanned during a background scan. By default, files on fixed local drives are scanned during a DLP background scan.

Background scans happen slowly, at a controlled pace, so as not to affect the user experience.

Follow this procedure to create your own DLP background scanning task or enable the DLP background scanning task provided with this release.

-
- Step 1** Log on to the CSA MC as a user with configure or deploy privileges and switch to **Advanced Mode**.
 - Step 2** From the **Systems** menu, in the CSA MC interface, navigate **Host Tasks > Host Scanning Tasks**.
 - Step 3** Click **New**.
 - Step 4** Give the task a **Name** and a **Description**.
 - Step 5** Select **Enabled** if you want to enable this task immediately after rules are regenerated and software updates are distributed to hosts.
 - Step 6** In the Configuration area, define the task:
 - In the **Run this task** fields, choose to run this task every week and on a particular day of the week, or choose to run this task every month and on a particular day of every month.



Note If a scan is scheduled on the 31st of the month, the scan will not be performed on months with fewer days.

- In the **At** field, specify the time of day the scan is to run. Time is expressed in twenty-four hour format.
- Check **Perform background DL search on all hosts in group** and select a group from the drop-down list. You can only specify one group per background scan task.



Note Combining an AntiVirus scan with a Data Loss Prevention scan causes two separate system scans.

Step 7 Click **Save**.

You will then need to generate rules for the task to be distributed to all hosts in that group.

Performing an On-Demand DLP Scan

An on-demand DLP scan searches fixed drives on the host for files with data scanning tags. In order for an On-demand DLP Scan to work you need to have Data Loss Prevention enabled. See [Enabling Data Loss Prevention Protection, page 16-3](#) for more information.

-
- Step 1** Log on to CSA MC as a user with configure or deploy privileges and switch to **Advanced Mode**.
- Step 2** From the **Systems** menu, click **Hosts**.
- Step 3** Click the link for the host on which you want to start an immediate scan.
- Step 4** At the end of the **DL full-scan schedule** row, click **View DL Scan Results**.
- Step 5** In the Scanning dialog box, click **DL Scan Results** if the tab is not open already.
- Step 6** Click **Scan Now**. A polling hint is sent to the host, after the host receives the polling hint, the on-demand scan begins automatically. If the host does not receive the polling hint, the scan will begin the next time the host polls.

■ Data Loss Prevention Scanning Tasks

While the scan is in progress, you can click **Get Results** to receive the information gathered so far. After clicking Get Results, the agent on the host forwards the information it has collected the next time the agent polls.

When the on-demand scan is complete, the agent sends the results to the MC automatically.

The DL Scan Results page refreshes the information it has periodically. Upon refresh, the latest information forwarded from the agent is displayed on the page.

Identifying a Host's DLP Scan Schedule

To identify a host's Data Loss Prevention scan schedule, follow this procedure:

-
- Step 1** Log into the CSA MC and switch to **Advanced Mode**.
 - Step 2** From the **Systems** menu, select **Hosts**.
 - Step 3** Click the link for the host you want to investigate.
 - Step 4** Expand the Host Status area.
 - Step 5** The **DL Full Scan Schedule** field identifies the data loss prevention scanning schedule for the host.

Identifying a Group's DLP Scan Schedule

To identify a group's Data Loss Prevention scan schedule, follow this procedure:

-
- Step 1** Log into the CSA MC and switch to **Advanced Mode**.
 - Step 2** From the **Systems** menu, select **Groups**.
 - Step 3** Click the link for the group you want to investigate.
 - Step 4** In the Features area, look for **Data Loss Prevention**.
 - Step 5** Click the link for Background Scan: On (Off). The pop-up box displays the time of the regularly scheduled background scan or indicates that DL background scanning is disabled.

Data Loss Prevention Reporting

You can generate reports that describe the number of files tagged with scanning data tags and the location of those files. See “[Data Loss Prevention Reports](#)” section on page 11-14 for the various Data Loss Prevention reports you can generate.

Creating Data Loss Prevention Rules and Components

This release provides policies which seek to prevent data loss. These policies include rules that trigger scans for text patterns and built-in data patterns and warns users of possible data loss activities.

If you want to create customized rules and file sets for your enterprise, this section provides procedures to do that.

Creating File Access Control Rules to Apply Scanning Data Tags

Use file access control rules to trigger data scans on files. Generally, think of a file access control rule triggering a data scan after testing this kind of statement: “Perform a data scan on a file, if an application attempts to read or write that file, and the attempt was allowed (or denied).”

**Note**

Unless this rule applies a static tag when the application’s actions are allowed by default, you will also need to create a separate rule that allows (or denies) the applications attempt to access the file.

Follow this procedure when creating a FACL to trigger a data scan:

**Note**

See [Configuring Rule Modules, page 5-4](#) to create your own rule module into which you will put this rule.

-
- Step 1** Log on to the CSA MC as a user with configure privileges and switch to Advanced Mode.
- Step 2** Open the rule module to which you want to add this rule.
- Step 3** Expand the **Rules** area of the rule module configuration screen and click the **Add** button. A pop-up list of the available rule types appears.
- Step 4** Select **File access control** rule. This takes you to the configuration view for this rule type.
- Step 5** 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 6** In the **Take the following action list box**, select **Set** from the pulldown list.
- Step 7** In the Attributes list box, select the kind of scan you want to perform: **Data scan on CLOSE** or **Data scan on OPEN**. See [Attribute: Data scan on CLOSE, page 5-29](#) or [Attribute: Data scan on OPEN, page 5-30](#) for descriptions of these set attributes.
- Step 8** In the Value field select **NOT being required for this file** to prevent a file from being scanned for information or **Being required for this file** to require that the file be scanned for information.
- Step 9** Enable the **Log** checkbox to turn logging on for this rule. Generally, you will not want to turn logging on for these set rules, except for testing or debugging a new rule.
- Step 10** **When**—
- **Applications in any (or all) 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 control. You may also create a new application class by clicking the blue **New** link next to the application class list box. For application class configuration details, see [Chapter 8, “Using Application Classes”](#)

If you choose **Applications in *any* of the following selected classes** the rule will affect an application that is a member of one of the selected application classes.

If you choose **Applications in *all* of the following selected classes**, the rule will affect an application that is a member of every application class you select.

- **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. You may also create a new application class by clicking the blue **New** link next to the application class list box.



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

Step 11 Attempt the following operations—In this step, you specify the file operation that the application, you are controlling, is attempting.

If you are creating a **Scan on OPEN** rule, you must select both the **Read File** and **Write File** operations you are allowing or denying on the files named in the **On any of these files** box. If you are creating a **Scan on CLOSE** rule, you can only select the **Write File** operation.

The **Write directory** operation is not a valid choice for **Data scan on OPEN** or **Data scan on CLOSE** actions.



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 be very specific in your path string and understand the resulting behavior.

Step 12 On any (or all) of these files—In this step you configure the file sets on which you want to perform data scans.

- If you choose, **On any of these files**, the rule will trigger a file-scan on a file that is a member of any one of the file sets you specify.
- If you choose, **On all of these files**, the rule will trigger a file-scan on a file that is a member of all of the file sets you specify.

Click the **Insert File Set** link to enter a pre-configured file set from a list of available file sets. In the Insert File Set list box, you may also click the blue **New** link, at the top of the list, to create a new file set for the rule. Finally, you can also 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 2-41](#).

Step 13 And — In this area specify, the enforcement action taken by CSA.

Specifying **Allow by default** or **Allow if triggered by a rule** triggers a scan on files that applications have been allowed to access. Specifying **Terminated** or **Denied by rule** scans files that other applications have been prevented from accessing.

Step 14 When you are finished configuring your File access control rule, click the **Save** button.

This rule is now part of your rule module. It takes effect when the rule module is attached to a policy, the policy is attached to a group and then is downloaded by an agent on the network.

Creating File Access Control Rules to Apply Static Data Tags

You can use file access control rules to assign a static data tag to a file without having scanned its contents. Generally, think of this rule as classifying a file after testing this kind of statement: “Assign to a file this static data tag if an application attempts to modify the file, and the attempt was allowed (or denied).”



Note

Unless this rule applies a static tag when the application’s actions are allowed by default, you will also need to create a separate rule that allows (or denies) the applications attempt to access the file.

Static data tags are applied to files after they have been modified and closed.

Follow this procedure when creating a FACL to trigger a data scan:



Note See [Configuring Rule Modules, page 5-4](#) to create your own rule module into which you will put this rule.

-
- Step 1** Log on to the CSA MC as a user with configure privileges and switch to Advanced Mode.
- Step 2** Open the rule module to which you want to add this rule.
- Step 3** Expand the Rules area of the rule module configuration screen and click the **Add** button. A pop-up list of the available rule types appears.
- Step 4** Select **File access control** rule. This takes you to the configuration view for this rule type.
- Step 5** 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 6** In the **Take the following action list box**, select **Set** from the pulldown list.
- Step 7** In the Attributes list box, select **file Data Classification**. See [Attribute: file Data Classification, page 5-34](#) for a description of this setting.
- Step 8** In the **Value** field, select “**include the tag <Tag Name>**.” In the value field's pulldown menu, there are several static tags for you choose from. You should choose a Tag Name that is related to the kind of application that is accessing the file. As delivered in the default policies, these static tags arrive unused and unconfigured.
The static tags' names were chosen to guide and support the tags' intended use. For example, if your end-users run medical application software, then some of your FACL rules might set the static tag **<HIPAA Controlled>** for any files that your medical software touches. Note, though, that a file cannot take on more than one static tag. If two “Set file Data Classification” rules fire on the same file, then the tag that appears first in the **Value** field of the **file Data Classification** set action will be applied.

For example, if rule 100 is written to apply the <Confidential Information> static tag and rule 200 is written to apply the <HIPAA controlled> tag, if both rules are triggered for the same file, the file will be tagged with the <HIPAA Controlled> static tag because it appears higher in the list of **file Data Classification** set values.

Step 9 Enable the **Log** checkbox to turn logging on for this rule. Generally, you will not want to turn logging on for these set rules, except for testing or debugging a new rule.

Step 10 When —

- **Applications in any (or all) 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 control. You may also create a new application class by clicking the blue **New** link next to the application class list box. For application class configuration details, see [Chapter 8, “Using Application Classes”](#)

If you choose **Applications in any of the following selected classes** the rule will affect an application that is a member of one of the selected application classes.

If you choose **Applications in all of the following selected classes**, the rule will affect an application that is a member of every application class you select.

- **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. You may also create a new application class by clicking the blue **New** link next to the application class list box.



Note

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

Step 11 Attempt the following operations—In this step, you specify the file operation that the application you are controlling is attempting. You can only specify Write File.

Refer to File and Directory protection in [Using the Correct Syntax, page 2-41](#).

**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 be very specific in your path string and understand the resulting behavior.

Step 12 On any (or all) of these files—In this step you configure the file sets which contains the files you want to tag.

- If you choose, **On any of these files**, the rule will tag a file that is a member of any one of the file sets you specify.
- If you choose, **On all of these files**, the rule will tag a file that is a member of all of the file sets you specify.

Click the **Insert File Set** link to enter a pre-configured file set from a list of available file sets. Click **Show All** to expand the list of file sets to choose from. In the Insert File Set list box, you may also click the blue **New** link, at the top of the list, to create a new file set for the rule. Finally, you can also 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 2-41](#).

Step 13 And — In this area specify, the enforcement action taken by CSA.

Specifying **Allow by default** or **Allow if triggered by a rule** triggers a scan on files that applications have been allowed to access. Specifying **Terminated** or **Denied by rule** scans files that other applications have been prevented from accessing.

Step 14 When you are finished configuring your File access control rule, click the **Save** button.

This rule is now part of your rule module. It takes effect when the rule module is attached to a policy, the policy is attached to a group and then downloaded by an agent on the network.

In order to distribute rules to the correct hosts, you must associate policies with groups and then Generate rules. See [page 5-16](#) for instructions.

■ Creating Data Loss Prevention Rules and Components



CHAPTER **17**

Cisco Partner and 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 IPS Integration Support, page 17-2](#)
- [Cisco MARS Integration Support, page 17-3](#)
- [netForensics Integration Support, page 17-3](#)

Cisco IPS Integration Support

You can configure Management Center for Cisco Security Agents to send host posture events and quarantined IP address events to Cisco Intrusion Prevention System 6.0. Refer to the Cisco Intrusion Prevention System 6.0 documentation on Cisco.com

To configure CSA MC to send information to IPS, do the following:

-
- Step 1** Navigate to the CSA MC **Events>Status Summary** page. Click the **No** link beside **Host history collection enabled** in the Network Status section. A new pop-up window appears. Click the **Enable** button in this window.
Note that this enables host history collection globally for the system. This feature is disabled by default as the MC log file tends to fill quickly when it's turned on.
 - Step 2** Navigate to **Systems>Groups** and create a new group (with no hosts) to use in conjunction with administrator account you will next create.
 - Step 3** Create a new CSA MC Administrator account to provide IPS access to the MC system. Navigate to **Maintenance>Administrators>Account Management**. Create a new account with the role of **Monitor**. This maintains the security of the MC by not allowing this new account to have Configure privileges.
Note the username and password given to this administrator account as you will need them when you configure IPS.
 - Step 4** Navigate to **Maintenance>Administrators>Access Control** to further limit this administrator account. In the Access Control window, select the administrator you created previously and select the group you created previously. When you save this configuration, you have further limited the MC access of this new administrator account. Again, the purpose is to maintain security on CSA MC.
That is all the configuration needed for the CSA MC side of this integration.

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 MARS Integration Support

MARS is a Security Information Management (SIM) appliance. It delivers a range of information about your networks' health as seen through the "eyes" and "ears" of the reporting devices, sessionizes them across different devices, fires default rules for incidents, determines false positives, and delivers consolidated information through diagrams, charts, queries, reports and rules.

To integrate events generated by the Cisco Security Agent with the MARS appliance, refer to Chapter 3 of your MARS User Guide documentation.

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.

■ netForensics Integration Support



CHAPTER **18**

Using the Scripting Interface (CSAAPI)

Overview

The Management Center for Cisco Security Agents provides the ability for administrators to write scripts to perform a subset of configuration actions on the MC.

Sample scripts are provided with the MC and it is recommended that you use these samples for writing your own scripts.

This section contains the following topics.

- [Overview, page 18-1](#)
- [CSAAPI/Scripting Overview, page 18-2](#)
 - [API Function Summary, page 18-3](#)
- [Scripting Interface Fundamentals, page 18-4](#)
 - [Before You Begin, page 18-4](#)
 - [WSDL/SOAP, page 18-5](#)
 - [Choosing a Scripting Language, page 18-6](#)
 - [Sample Scripts and README Files, page 18-7](#)
 - [Encryption and Authentication, page 18-8](#)

- Object Expressions, page 18-9
- Object Types, page 18-10
- Supported Names per Object Type, page 18-10
- Object Expression Values, page 18-12
- Object Type Names, page 18-16
- Wildcarding, page 18-17
- Using the Escape Character, page 18-17
- Using the Limit Name to Prevent Unwanted Actions, page 18-19
- Blocking vs. Non-blocking, page 18-19
- API Function Descriptions, page 18-21
 - Getting the Status of Functions and Waiting for Functions to Complete, page 18-21
 - Testing Object Expressions, page 18-23
 - Modifying the State of the Overall System, page 18-24
 - Host Group Assignment, page 18-27
 - Manipulating Hosts, page 18-29
 - Getting Host Information, page 18-30
 - Getting Overall System Information, page 18-32
 - Getting Event Information, page 18-33
 - Getting Reports, page 18-33

CSAAPI/Scripting Overview

The Management Center for Cisco Security Agents provides administrators with the ability to use scripts for performing some very specific functions locally on the MC or from a remote system. This scripting interface is called CSAAPI and it allows you to write your scripts in any language and run your scripts on any operating system.

API Function Summary

The CSA MC scripting interface lets you execute a variety of functions, which include manipulating hosts and retrieving host information. The following is a list of actions that are possible:



Note

Before attempting to run the functions listed here, read through the [Scripting Interface Fundamentals, page 18-4](#) and [API Function Descriptions, page 18-21](#) sections so that you understand the general concepts and individual API functions listed here.

Non-blocking Functions

- Integer GenerateRules ()
 - Integer GenerateReport (String reportName, String emailAddress)
 - Integer Import (String filename)
 - Integer Export (String filename, String desc, String emailAddress, StringArray objects)
 - Integer RunHostTask (String hostTaskName)
 - Integer BackupConfig ()

Blocking Functions

“Get” Functions

- ```
- StringArray GetHostInfo (String hostExpression)
- StringArray GetLastIpAddrs (String hostExpression)
- StringArray GetDiagnosticInfo (String hostExpression)
- StringArray GetMostActive (String objType,
 Integer numOfObjects,
 String timespan)
- Integer GetLastDayEventCount ()
- StringArray GetLatestEvents (String objType,
 String objExpression,
 Integer numOfEvents)
- StringArray GetLatestAudit (Integer numOfEvents)
- String GetConfigVar (String name)
```

- Integer GetObjectCount (String objType, String objExpression)
- StringArray GetNames (String objType, String objExpression)
- StringArray GetReportNames ()
- StringArray GetHostTaskNames ()

#### “Set/Update” Functions

- Boolean AddHostsToGroups (String hostExp, String groupExp)
- Boolean RemoveHostsFromGroups (String hostExp, String groupExp)
- Boolean MoveHosts (String hostExp, String fromGroupExp, String toGroupExp)
- Boolean DeleteHosts (String hostExp)
- Boolean SendHint (String hostExp)
- Boolean ResetAgent (String hostExp, Integer resetMask)
- Boolean SetConfigVar (String name, String value)

#### “Housekeeping” Functions

- Integer GetStatus (Integer processID)
- String GetStatusMessage (Integer processID)
- Integer WaitForProcess (Integer processID, Integer timeout)

# Scripting Interface Fundamentals

The following sections provide information you need to use the scripting interface.

## Before You Begin

Before you attempt to write scripts that use the CSA MC scripting interface, it is critical that you take some time to familiarize yourself with a number of important concepts described in the next several sections, including:

- WSDL/SOAP
- Choosing a scripting language
- Using the Sample Scripts and README files
- Encryption and Authentication
- Object Expressions
- Wildcarding
- Using the Escape Character
- Using the LIMIT token to prevent unwanted actions
- Blocking vs. Non-blocking Functions
- Getting the status of functions and waiting for functions to complete
- Getting to know each scripting interface function

Bear in mind that the scripting interface is a powerful tool that allows you to execute actions that can have serious consequences. For example, the scripting interface allows you to perform tasks such as deleting hosts, resetting agents, generating rules and modifying host/group assignments. As such, it makes sense to exercise caution while using the scripting interface and take the time to understand its intricacies.

## WSDL/SOAP

The CSA MC scripting interface infrastructure relies upon WSDL (Web Services Description Language) and SOAP (Simple Object Access Protocol) for its function. WSDL and SOAP allow you to use widely-available, non-proprietary libraries to write scripts for most operating systems in a variety of different languages. In short, SOAP and WSDL allow you to write distributed applications without having to understand the complexities of the communication between your scripts and the CSA MC server.

That said, before writing your scripts, it is recommended that you take a few moments to familiarize yourself with the basics of WSDL and SOAP. The sample scripts will be easier to follow and debugging may be easier with just a few moments devoted to WSDL and SOAP.

WSDL is a specification for defining web services/APIs with a common XML grammar. WSDL is powerful because it abstracts out details relating to specific operating systems and computer languages. CSA MC contains a WSDL file (csaapi<csa mc version number>.wsdl, for example csaapi60.wsdl) that describes which functions are available, what parameters they take, and what values they return. This WSDL file can be used by a variety of freely-available utilities to generate script “stubs” that can be quickly modified into working scripts. (Or you can just start with the sample scripts provided with CSA MC – more on this later.)

Good information on WSDL can be found here:

<http://www.w3.org/TR/wsdl>

<http://www.oreilly.com/catalog/webservess/chapter/ch06.html>

<http://en.wikipedia.org/wiki/WSDL>

SOAP is an XML-based protocol for object exchange (usually over HTTP). While WSDL is used to describe web services, SOAP is a protocol for encapsulating messages (requests and responses, usually) in an “envelope” that is communication-protocol independent. SOAP has been widely adopted and there are a variety of good SOAP implementations (for example, Perl’s SOAP::Lite) that make writing web-based scripts easier than you would think.

Good information on SOAP can be found here:

<http://www.w3.org/TR/soap12-part1/>

<http://www.w3.org/TR/2003/REC-soap12-part0-20030624/>

[http://en.wikipedia.org/wiki/Simple\\_Object\\_Access\\_Protocol](http://en.wikipedia.org/wiki/Simple_Object_Access_Protocol)

## Choosing a Scripting Language

As is stated above, WSDL and SOAP allow you to write scripts in any language that supports WSDL and SOAP, for any platform on which the appropriate libraries are available.

That being said, there are sample scripts provided for you in the following languages: Perl, Java and C++. It is *highly* recommended that you start with the sample scripts and understand their workings before attempting to move onto other languages (for example, C# or PHP). It’s recommended that you start with the sample scripts because the scripts contain examples of many different

techniques, from asking for passwords, to using the LIMIT clause, to checking the status of functions and getting status messages, to using wildcards and escape characters, to using object expressions (all of which are explained here).

Furthermore, if you do not have a language preference, it's recommended that you choose Perl for your first workings with the scripting interface. The Perl infrastructure, including its encryption libraries, is easy to install and use. Perl, as an interpreted language, lends itself to fast prototyping and has nice features for running in debug mode that make debugging easier than in the other languages.

Finally, please bear in mind that Cisco TAC can assist you if there is a problem with the scripting interface infrastructure, but *Cisco TAC will not help you debug your own scripts*.

## Sample Scripts and README Files

CSA MC installs with sample scripts which you should use to model your own scripts. These samples scripts appear in a separate folder for each scripting language. These folders also contain other files that are meant to help you write your scripts, including a detailed readme file. The sample scripts can be found in the “samples\csaapi” directory of your CSA MC installation directory, for example:

```
C:\Program Files\Cisco\CSAMC\CSAMC60\samples\csaapi
```

This directory contains a README.txt file that contains general information on the Scripting Interface. Furthermore, this directory contains “Perl”, “Java” and “CPP” directories that contain sample scripts for each language. Note that each language directory contains its own README.txt file that contains important information specific to each language.



### Caution

It is critical that you read these README.txt files before attempting to create or run a script. The readme files contain specific information for setting up your MC server environment and your client environment. This information is not provided anywhere else and you must follow the instructions provided in the readme for your scripts to work as expected.

## Encryption and Authentication

In order to ensure that the CSA MC scripting interface is not used in an unauthorized manner, the scripting interface mandates the use of encryption and authentication.

Encryption is provided by the use of the *https* protocol. In the sample scripts, you will see an URL embedded with “*https*” as the protocol. Do not try to change this protocol as the scripts will not work.

Authentication is provided outside the CSA MC user-interface login system. The scripting interface does not have knowledge of existing administrator accounts on the MC. Before you can use the scripting interface, you must create a new userid and password using the instructions provided in this section in order to use a script to configure the MC. The userid and password you create to access the MC with your script will have no bearing on the CSA MC user interface access and will only apply to the scripting interface.

Before you use the scripting interface, you **must** run through the following steps to provide the scripting interface infrastructure with userid and password information:

First, go to the apache directory by typing:

```
cd <CSAMC_base_directory>\apache2
```

For example:

```
cd Program Files\Cisco\CSAMC\apache2
```

Then run the *htpasswd* utility with the following syntax:

```
bin\htpasswd.exe -c conf\csaapiUsers<csa mc version number>.pwd <username>
```

You will be prompted to enter that user's password two times.

To add additional users, type the following:

```
bin\htpasswd conf\csaapiUsers<csa mc version number>.pwd <next user name>
```

Note the file MUST be named *csaapiUsers.pwd*.

Once this is done, your scripts must provide one of these userid/password combinations. See the *README* files in the *csaapi* directory and the sample scripts for details.

# Object Expressions

Many functions in the CSA MC scripting interface require you to specify which objects to act on. For example, the “DeleteHosts” function requires you to specify which hosts to delete.

**Note**

An “object”, for the purposes of the scripting interface, is an entry in the CSA MC database corresponding to an entity like a host, group, policy, rule module, rule, etc.

To provide maximum power to describe groups of objects, the CSA MC scripting interface uses an “object expression” syntax, which is simply a set of name/value pairs with the format:

```
NAME='VALUE' NAME='VALUE' NAME='VALUE'
```

For example, consider the following scripting interface function:

```
StringArray DeleteHosts (String hostExpression)
```

To delete all Windows hosts in Learn Mode, for example, you would call the function with the following argument:

```
DeleteHosts ("OS='Windows' LEARN_MODE='true'");
```

The object-expression syntax is basically an “SQL Lite” system that is both flexible and independent of the CSA MC database schema. Multiple Name/Value pairs are logically ANDed together. In other words, the example above would apply only to hosts that are both Windows AND in Learn Mode.

If an invalid expression is passed to any function, the function will return an error code, and the caller can use the `GetStatus()` and `GetStatusMessage()` functions to get more information.

Now that the syntax has been explained, let’s take a look at what names are valid, and what values are valid for each name.

# Object Types

There are some general issues to note when using a scripting interface to access CSA MC. You cannot create new configuration items using the scripting interface. You can only manipulate existing items and you can also generate rules. This next section provides information, universal to all scripting languages, on the CSA MC functions (object types) that are available for configuration via scripting. Each object is specified in terms of name/value pairings. The following is a list of supported object types:

```
HOST
GROUP
POLICY
RULE_MODULE
RULE
APP_CLASS
VAR
```

## Supported Names per Object Type

The following describes which names are valid for which object types:

### *Object Type: Hosts*

#### *Names:*

```
HOST_NAME
IP_ADDR
GROUP_NAME
POLICY_NAME
RULE_MODULE_NAME
OS_TYPE
OS_ARCHITECTURE
OS_DESC
ACTIVE
TEST_MODE
LEARN_MODE
```

### *Object Type: Groups*

#### *Names:*

```
GROUP_NAME
POLICY_NAME
```

HOST\_NAME  
VERSION  
TEST\_MODE  
LEARN\_MODE  
OS\_TYPE  
OS\_ARCHITECTURE

### ***Object Type: Policies***

#### ***Names:***

POLICY\_NAME  
GROUP\_NAME  
RULE\_MODULE\_NAME  
VERSION

### ***Object Type: Rule Modules***

#### ***Names:***

RULE\_MODULE\_NAME  
POLICY\_NAME  
VERSION  
TEST\_MODE  
LEARN\_MODE  
OS\_TYPE  
TARGET\_OS

### ***Object Type: Rules***

#### ***Names:***

RULE\_ID  
RULE\_NAME  
RULE\_TYPE  
ACTION  
RULE\_MODULE\_NAME

### ***Object Type: Application Classes***

#### ***Names:***

APP\_CLASS\_NAME  
VERSION  
OS\_TYPE  
TARGET\_OS

### ***Object Type: Variables***

***Names:***

VAR\_NAME  
VAR\_TYPE  
VERSION  
OS\_TYPE  
TARGET\_OS

## Object Expression Values

Valid values for each of the names listed in the previous section are listed here. The use of wildcard characters is supported in all value entries unless otherwise specified:

**HOST\_NAME**

A string expression of a host name would appear as follows. Value examples:

bugtrack.amer.cisco.com  
bugtrack\*  
bugtrack.????.cisco.com

Note that host name values are NOT case sensitive.

**IP\_ADDR**

A string expression of an IP address would appear as follows. Value examples:

1.1.1.1  
1.1.1.\*  
15?.\*.\*.\*

**GROUP\_NAME**

A string expression of a group name would appear as follows. Value examples:

Desktops - All types  
Servers - \* deployed

Note that group name values are NOT case sensitive.

**POLICY\_NAME**

A string expression of a policy name would appear as follows. Value examples:

Email client - Linux  
Email client \*

**RULE\_MODULE\_NAME**

A string expression of a rule module name would appear as follows. Value examples:

```
Email Client Module - Low Security
Email Client Module - ? Security
```

**RULE\_ID**

A string expression of a rule ID would appear as follows. Value examples:

```
"51"
```

**RULE\_NAME**

A string expression of a rule name would appear as follows. (Note that rules, technically, do not have names. RULE\_NAME gives you the ability to query against the Description field that is displayed in the MC UI for an individual rule.) Value examples:

```
Email worm
```

**RULE\_TYPE**

This field lets you identify a rule by its type. Since there is a specific name for each rule type, a rule type value you enter must match one of the following strings:

```
Agent service control
Agent UI control
Application control
Buffer overflow
Clipboard access control
COM component access control
Connection rate limit
Data access control
File access control
Global event log
Global IP address quarantine
Global network scan
Global virus scan
Kernel protection
Network access control
Network interface control
Network shield
NT Event log
Registry access control
```

```
Resource access control
Rootkit / kernel protection
Service restart
Sniffer and protocol detection
Syslog control
System API control
```

Rather than trying to match the string exactly, you can also use wildcards to match types. For example, the following would be less likely to be foiled by a typo:

```
RULE_TYPE='Rootkit*'
than this entry:

RULE_TYPE=' Rootkit / kernel protection'
```

#### ACTION

The following string values are allowed for this name. Since there are a specific number of action types, the value you enter must match one of the following strings. Any other value results in an error:

```
PRIORITY_TERMINATE
PRIORITY_DENY
PRIORITY_ALLOW
QUERY
TERMINATE
DENY
MONITOR
SET
```

Note that wildcards are not supported for ACTION types.

#### VERSION

A string expression of a CSA MC release version would appear as follows.  
Value examples:

```
5.2 r578
5.2*
5.2.? r6??
```

#### OS\_TYPE

This allows you to specify either ‘WINDOWS’ or ‘UNIX’. Generally, this field correlates to the “ostype” field in the various database tables.

**OS\_ARCHITECTURE**

This field provides a way to specify more granularity than with the OS\_TYPE field. This field can be applied to objects of type HOST and GROUP. The valid values are 'WINDOWS', 'SOLARIS', and 'LINUX'. In general, the field corresponds to the "architecture" field in the database.

**TARGET\_OS**

This field provides a way to specify more granularity than with the OS\_TYPE field. This field can be applied to objects of type RULE\_MODULE, APP\_CLASS and VAR. The valid values are 'ALL', 'XP', 'SOLARIS', and 'LINUX'. In general, the TARGET\_OS field corresponds to the "osflavor" field in the database

**OS\_DESC**

This field lets you query directly on the host's "os" database field. This contains descriptions such as "Windows 2003" that could allow you to differentiate between Windows 2000 and Windows 2003.

**ACTIVE**

For this name, you can enter a boolean value ('TRUE' or 'FALSE') corresponding to whether the machine is active. 'YES' and 'NO' are also acceptable values.

**TEST\_MODE**

For this name, you can enter a boolean value ('TRUE' or 'FALSE') corresponding to whether the machine is active. 'ON' and 'OFF' are also acceptable values.

**LEARN\_MODE**

For this name, you can enter a boolean value ('TRUE' or 'FALSE') corresponding to whether the machine is active. 'ON' and 'OFF' are also acceptable values.

**APP\_CLASS\_NAME**

A string expression of an application class name would appear as follows.  
Value examples:

FTP applications  
Software installer invoked applications

**VAR\_NAME**

A string expression of a variable name would appear as follows. Value examples:

Apache executables  
Ephemeral port ranges

**VAR\_TYPE**

The following string values are allowed for this name. Since there are a specific number of variable types, the value you enter must match one of the following strings. Accepted values are:

COM  
DATA  
FILE\_UNIX  
FILE\_WINDOWS  
NETWORK\_ADDRESS  
NETWORK\_SERVICE  
QUERY  
REGISTRY

Note that wildcards are not supported for VAR\_TYPE.

## Object Type Names

There are several functions in the scripting interface that are generic and that can be run for objects of any type (`GetNames()`, `GetMostActive()`, etc.). The scripting interface uses a string variable typing system to indicate to these generic functions the type of object being acted upon. The following are accepted values:

HOST  
GROUP  
POLICY  
RULE\_MODULE  
RULE  
APP\_CLASS  
VAR

The listed object type values are special because they can be passed separately into functions requiring an “object type” string, but they can also be combined with the name “OBJ\_TYPE” in a name/value pair for any object type. For example, to get a list of names of Application classes associated with Linux, you could create the following name/value expression:

```
"OBJ_TYPE='APP_CLASS' OS='Linux'"
```

The OBJ\_TYPE designation can be omitted for any function in which the object type is implied by the function itself (for example, GetHostInfo) or any function that takes as a parameter an object-type string that is separate from the object expression (for example, GetObjectCount).

## Wildcarding

The scripting interface provides wildcard support similar to what is available through SQL, although with slightly different syntax. The following wildcard characters are supported:

- \* Matches any string of zero or more characters
- ? Matches any one character

## Using the Escape Character

Although this will be rare, there may be times when you want to specify a wildcard character (or the single-quote character) literally. In other words, when you want to express a string that has the wildcard character in it, for example:

Bob's Group

In order to support expressions like this, there are four characters that must be “escaped” with the “\” escape char. These characters are:

- \*
- ?
- ' (single quote)
- \ (backslash)

Therefore, if you wanted to specify a Group Name of:

Bob's Group

You would need to place a backslash before the single-quote, for example:

GROUP\_NAME='Bob\'s Group'

Literal backslash characters also require a backslash. For example, to specify the Group Name C:\foo, you would need to enter:

GROUP\_NAME='C:\\foo'

As a final example, if you wanted to specify a string ending in a question mark, the user would need to enter:

GROUP\_NAME='\*\\?'

In the above example, the asterisk is a wildcard, but the question mark is used literally.

It should be noted that CSA MC provides restrictions on which characters can be present in names of groups, hosts, etc. As such, you will rarely have to use a wildcard character literally. But the escape-character functionality exists in the event that CSA MC naming restrictions are lifted in the future.



**Note**

Note to Perl Script Writers: Perl provides an extra hurdle when using the backslash character. In order to embed the backslash character in a string in Perl, you must unfortunately specify two backslashes. So, in Perl, to specify the group name Bob's Group, you must actually provide text like this:

```
my $objExp = "GROUP_NAME='Bob\\\\'s Group'"
```

In a more painful example, to specify C:\foo, you will actually need to specify four (4) backslashes, as in:

```
my $objExp = "GROUP_NAME='C:\\\\\\foo'"
```

This is an unfortunate consequence of having to escape the backslash character twice – once for Perl and once for the scripting interface. For more details, see the Scripting Interface README files.

## Using the Limit Name to Prevent Unwanted Actions

There is one name token that can be applied to objects of any type. That token is called **LIMIT**. The **LIMIT** construct allows the caller to specify that a function must terminate immediately if the number of objects returned by the function's object expression exceeds the specified limit.

For example, if you want to delete all hosts that begin with the string "server", but your assumption is that no more than two hosts meet this description, you could run the following:

```
DeleteHosts ("HOST_NAME='bugtrack*' LIMIT='2'")
```

This call would delete no hosts if more than two hosts started with the string "server".

This **LIMIT** construct in effect allows you to call the **GetObjectCount** method within a called function, saving an extra call. It should be noted that the **LIMIT** token has no effect if placed within the **GetObjectCount** function.

In the event of a failure of a function that has an object expression that contains a **LIMIT** statement, call the **GetStatus()** function (described below). If the error code is "200", then this means that the number of objects described by the object expression exceeds the **LIMIT** value.

## Blocking vs. Non-blocking

Generally, Scripting Interface functions can be split into two groups: Those that "block" and those that don't. The following section describes the difference and how this difference relates to return values and getting status information.

### Blocking Functions

When a blocking function is executed, the server waits until the function is complete before returning a value. All but a handful of functions in the API are blocking.

Generally, blocking functions that implement a “set/update” operation (for example, `AddHostsToGroups`) return a boolean value (`false` on failure and `true` otherwise). Blocking functions that implement a “get” operation (for example, `GetLastIpAddrs`) return the data type of whatever data is being retrieved (string, string array, integer, etc).

Detailed status/error information of a blocking function can be retrieved by calling one of the status functions (`GetStatus` and `GetStatusMessage`) with the Process ID of 0. See the section *Getting the Status of Functions and Waiting for Functions to Complete* for more information.

### Non-blocking Functions

Non-blocking functions return control back to the client script before the function is complete. Generally, functions that can take a long time to complete are the non-blocking functions. Non-blocking functions return control back to the client script immediately to ensure that the connection between the client and server does not time out. The current list of non-blocking functions is as follows:

```
GenerateRules()
GenerateReport()
Import()
Export()
RunHostTask()
BackupConfig()
```



---

**Note** All other functions in the scripting interface block.

---

When a non-blocking function runs, the scriptinginterface server basically tells the client script “I got your request, and I am working on it. Please check back with me later to learn how it went.” All non-blocking functions return an integer Process ID that can be used to get the status of the function later.

Client scripts can use the `WaitForProcess` function to wait until a non-blocking function is complete and can use the status functions (`GetStatus` and `GetStatusMessage`) to check on a non-blocking function’s status. See the section *Getting the Status of Functions and Waiting for Functions to Complete* for more information.

# API Function Descriptions

The following sections provide more information for each individual API function.

## Getting the Status of Functions and Waiting for Functions to Complete

The CSAMC Scripting Interface provides a comprehensive infrastructure for retrieving the status of functions that have recently been executed. This section describes the infrastructure's main elements, which include numeric *status codes*, *process IDs*, and *functions* that return status information and wait for non-blocking functions.

### Status Codes

The Scripting Interface uses numeric status codes to communicate the status of a function that has been executed by a client. In general, a status code of zero reflects success, a status code greater than zero reflects failure, and a status code of less than zero indicates that nothing has happened.

The complete list of status codes is given below:

| Success |             | Failure |                      | No Action |                 |
|---------|-------------|---------|----------------------|-----------|-----------------|
| ID      | Description | ID      | Description          | ID        | Description     |
| 0       | SUCCESS     | 1       | GENERIC ERROR        | -1        | PENDING         |
|         |             | 100     | UNKNOWN PROCESS      | -100      | NO ACTION       |
|         |             | 200     | ILLEGAL OBJECT EXPR. | -200      | NO OBJECT MATCH |
|         |             | 300     | DB OPEN FAILURE      | -201      | NO OBJECT MATCH |
|         |             | 301     | DB READ FAILURE      | -300      | LIMIT EXCEEDED  |

Most of these status codes are self explanatory, but a few require elaboration, below.

If you pass to a function an improperly formed object expression, then this situation is an error condition and the status code for that situation will be 200.

If, on the other hand, you pass to a function an object expression that happens to match no objects (for example, if your object expression is "HOST\_NAME='A\*' " but you have no hosts that begin with the letter 'A'), then you will receive the status code -200 (negative 200), which is not an error code – it's a no-action code. In general, *the scripting interface does not consider a request to do nothing to be an error.*

Similar to the situation above, if you specify a LIMIT clause in an object expression and the number of objects described by the object expression exceeds the limit specified in the LIMIT clause, then the return code will be -300 (negative 300), which, again, is not an error code but rather an no-action code.

### Process IDs: Identifying the Execution of a Function

Each time you run a function, a Process ID is associated with the execution of that function. This Process ID can then be used to get the status code association with the function execution.

The Process ID for a non-blocking function (see the [Blocking vs. Non-blocking](#) section for details) is the integer returned by the function.

The Process ID for a blocking function is always zero. In other words, getting the status code for the process with a Process ID of zero is the same as getting the status code for the last blocking function that was run.

### Getting a Status Code for an Execution of a Function

Once you have the Process ID for a function you have run, getting the status of that function is simply a matter of passing the Process ID to the following function:

- Integer GetStatus (Integer processID)

This API function asks the scripting interface server for the appropriate status code. The argument is the Process ID, and the returned value is the status code.

### Getting a Detailed Status Message

To get text information about the specific nature of an error, call the following function:

```
- String GetStatusMessage (Integer processID)
```

This function returns the status message of the process with the passed-in ID. If the passed-in ID is zero, then `GetStatusMessage` returns the status message of the last API function that was called.

If the process with the passed-in ID is still running, then the returned value will be “PENDING”. If the process succeeded, then the returned value will be “SUCCESS”.

`GetStatusMessage` is often helpful when attempting to receive additional information about why a function failed.

### Waiting for a Non-blocking Function to Complete

```
- Integer WaitForProcess (Integer processID, Integer timeout)
```

This function *blocks* until the specified process is complete or until the timeout (expressed in seconds) expires, whichever comes first. This function returns the Status Code of the specified function if the function finishes before the timeout or -1 otherwise. This function provides a handy way of blocking for function completion without having to write a loop.

## Testing Object Expressions

Object expression strings are used to describe a set of objects and are passed to functions as arguments. But some functions can have devastating effects if run against the wrong set of objects. The following two menu functions provide “sanity-checks” that allow scripts to determine what objects are returned by a particular expression before running an operation on that expression.

```
Integer GetObjectCount(String objType, String
objExpression)
```

`GetObjectCount` returns the number of objects referenced by the object expression. For example:

```
GetObjectCount("HOST", "OS='WINDOWS'")
```

would return the number of Windows hosts.

**Note**

The LIMIT token has no effect in this function and generally you should avoid including it in the object expression for this function.

```
StringArray GetNames(String objType, String objExpression)
```

GetNames returns a string array containing the names of all the objects matching the object expression. For example:

```
GetNames ("HOST", "OS='LINUX' ACTIVE='FALSE' ")
```

would return a list of hostnames of all inactive Linux boxes.

**Note**

For the object type “RULE”, this function returns the string form of the rule ID because rules do not technically have names.

## Modifying the State of the Overall System

The following functions modify the state of the overall system. Each function kicks off a process that executes the intended action and then immediately returns a Process ID. These functions do NOT block until their work is done.

```
Integer GenerateRules ()
```

GenerateRules() simply generates rules. This function does not block. It returns a Process ID that can be used by GetStatus to determine whether the rule generation was successful.

```
Integer Import (String filename)
```

Import() imports objects from the specified file. A full pathname must be provided. Import does not block. It instead returns a Process ID. Note that wildcards are NOT supported in the filename.

**Note**

You cannot import from files on remote drives. Import files must reside locally on the CSA MC system.

```
Integer Export (String filename, String desc, String emailAddr, StringArray objExpressions)
```

The `Export()` function exports objects to a file. The exported file is saved to the default CSAMC export directory and the file is accessible through the Exports page on the CSAMC GUI. If an optional email address is provided, then a copy of the export file is sent in an attachment to the email address.

The objects are specified by providing an array of object expressions. Each object expression is in the form of the name/value pairs described in the *Object Expressions* section.

Important: It is critical that each object expression provide an object type (for example, “`OBJ_TYPE='POLICY'`”). An error will result otherwise.

A sample array to export all Windows Application Classes would be:

```
sampleArray[] = { "OBJ_TYPE='APP_CLASS' OS_TYPE='W'" };
```

Export does not block; rather, it returns a Process ID.

Important Note: Not all possible object expressions are permissible in the `Export()` function. You cannot export objects of type HOST or RULE. Also, the only permissible name following an object of type VAR is VAR\_TYPE. In other words, you cannot export variables by name, version or OS\_TYPE or OS\_FLAVOR. The only way variables can be exported is by VAR\_TYPE.

Note: In order for this function to send email, the scripting interface must be informed of the name of the server to which to send emails. To do this, use the `SetConfigVar` function to set the “`csaapi.email_server`” parameter to the name of the email server. Note that this must be done only once.

Note: To allow the scripting interface to send email, you must first make a minor modification to the CSAMC rule that governs permissible web server actions. Please see the scripting interface sample script `README.txt` files for details.

**Note**

---

To email an export file to multiple addresses, separate the email addresses with a semicolon (‘;’). For example: `joe@company.com;jane@company.com`

---

```
Integer RunHostTask (String hostTaskName)
```

`RunHostTask()` executes a Host Managing task. `RunHostTask` does not block; rather, it returns a Process ID. `RunHostTask` supports the CSA MC scripting interface wildcarding mechanism.

```
Integer BackupConfig()
```

`BackupConfig()` executes a backup task. `BackupConfig` does not block; rather, it returns a Process ID. Note that `BackupConfig` will fail unless the user has previously specified a backup type and a Directory name on the Maintenance>Backup Configuration screen in the CSA MC UI.

```
Boolean SetConfigVar(String name, String value)
```

`SetConfigVar()` performs the same function as the “`set_config.csapl`” script on the CSA MC machine. `SetConfigVar()` allows you to modify a number of system-wide, persistent CSA MC configuration variables. In general, documentation of the valid config variable names and their associated values is located elsewhere in the CSA MC documentation, but the following two config variables are documented here because of their importance for all scripting interface functions that send emails:

`csaapi.email_server`

`csaapi.orig_email_addr`

The first config variable is used to specify to which address e-mails are sent by the scripting interface. The second config variable is used to specify the originator’s email address for emails sent by the scripting interface.

For example, to tell the scripting interface to send all emails (say, from `GenerateReport`) to the server `myserver.cisco.com`, make the following call:

```
SetConfigVar ("csaapi.email_server",
"myserver.cisco.com")
```

Again, please note that the email server MUST be set before running any scripting interface function that generates an email.

Note: Wildcards are NOT supported in any of these string parameters.

Note: All configuration variables set with this function are persistent in the CSA MC database. In other words, you only need to set them once.

```
String GetConfigVar (String name)
```

`GetConfigVar` returns the value of any configuration variable stored in the CSA MC configuration database. It returns the same values as the “`set_config.csapl`” script on the CSA MC machine.

See the `SetConfigVar` documentation, above, for more information about these CSA MC configuration variables.

Note: An empty string can be returned as the result of three distinct situations: Either the value is indeed the empty string in the database, or the value is not set at all in the database, or an error occurred in the Scripting Interface. To distinguish between these three cases, call `GetStatus`. A zero return code (success) indicates that the value is indeed the empty string in the database. A negative return value (no action) indicates that there was no matching record in the database. A positive return value (failure) indicates that there was an error in the Scripting Interface, and that `GetStatusMessage` should be called to learn more about the error.

## Host Group Assignment

The following functions change the Host/Group assignment. In all of the following functions, TRUE is returned on success and FALSE is returned on failure. Also, for all these functions, a failure with any part of the function will result in a rollback of any changes made. In other words, either all hosts matched by the hostExpression will be properly manipulated, or none will.

These functions block until the operation is complete. Note that these functions do not generate rules. That must be done separately.

For all of these functions, it is not considered an error/failure if the host or group expressions return no hosts/groups. In this case, the functions simply return TRUE (success) and do nothing. The reasoning for this is that scripts may simply want to manipulate certain hosts that meet certain criteria, but it may be common for no hosts to meet the object expression criteria at any given time.

If a script wants to detect the case in which no hosts were manipulated because no objects matched the object expressions, the script can call the `GetStatus` function.

```
Boolean AddHostsToGroups (String hostExp, String groupExp)
```

This function adds ALL the hosts matched by the host expression to ALL the groups matched by the group expression. This function does not remove the hosts from any groups. It just adds.

The following example adds all hosts in the group 'Group Test' to the Windows 'Desktops - All types'.

```
AddHostsToGroups("GROUP_NAME='Group Test'",
"GROUP_NAME='Desktops - All types' OS_TYPE='WINDOWS'
VERSION='5.0 r173'")
```

If a host to be added has an operating system different from that of a group matching the group object expression, then the host will not be moved into the group. This will not generate an error condition – the host will simply be skipped.

```
Boolean RemoveHostsFromGroups (String hostExp, String
groupExp)
```

This function removes ALL the hosts matched by the host expression from ALL the groups matched by the group expression. This function does not add the hosts to any groups. It just removes.

The following example removes all hosts in the group 'Group Test' from the Windows 'Desktops - All types'.

```
RemoveHostsFromGroups ("GROUP_NAME='Group Test'",
"GROUP_NAME='Desktops - All types' OS_TYPE='WINDOWS'
VERSION='5.0 r173'")
```

```
Boolean MoveHosts (String hostExp, String fromGroupExp,
String toGroupExp)
```

This function removes ALL the hosts matched by the host expression from ALL the groups matched by the "from group expression" and adds these hosts to ALL the groups matched by the "to group expression".

It is worthwhile to note that `MoveHosts` could theoretically have different results from running `AddHostsToGroups` and then `RemoveHostsFromGroups`. The reason for this is that `MoveHosts` calculates the "from" and "to" groups *before* doing any adding, whereas running the latter combination will cause the `Remove`'s "from" to be calculated *after* hosts have already been added. In almost all practical cases, however, the two approaches will be identical.

The following example moves all hosts from the group 'Group Test' to the Windows 'Desktops - All types'.

```
MoveHosts ("GROUP_NAME='Group Test' ",
 "GROUP_NAME='Desktops - All types' OS_TYPE='WINDOWS'
 VERSION='5.0 r173' ")
```

This function will fail if the “from group” matches groups but the “to group” does not. This is because this would result in the deletion of hosts from the “from group”, and this is probably not what the caller had intended. This function will also fail if one or more hosts cannot be moved due to an OS incompatibility.

```
Boolean DeleteHosts (String hostExpression)
```

This function sends all hosts that match the host expression to the CSA MC Recycle Bin. Obviously, this function should be used with caution.

## Manipulating Hosts

The following functions manipulate hosts in some way. All these functions take as a parameter a host expression (object expression).

Note that for all these functions, it is not considered an error/failure if the host expression returns no hosts. The reasoning for this is that scripts may simply want to manipulate certain hosts that meet certain criteria, but it may be common for no hosts to meet the object expression criteria at any given time.

If a script wants to detect the case in which no hosts were manipulated because no hosts matched the hosts expression, the script can call the GetStatus function.

```
Boolean SendHint (String hostExp)
```

This function sends a hint to all hosts that match the host expression.

This function does not block until all the hosts receive hints. Rather, the scripting interface infrastructure simply places “tags” in the CSA MC database that tell the CSA MC hint infrastructure to give priority to the appropriate hosts. Depending upon a number of factors, including the speed of the processor, the number of hosts to be hinted, etc., there may be some delay before the hints are sent. Bear in mind this delay exists to ensure that the polling server is not overwhelmed by polls.

This function returns true on success and false on failure.

```
Boolean ResetAgent (String hostExp, Integer resetMask)
```

This function resets the Cisco Security Agent. It works in a manner similar to the corresponding function in the CSA MC UI. When the function is run, the scripting interface infrastructure sets a flag in the CSA MC database that tells the CSA MC to reset the appropriate agents the next time these agents poll.

Callers of this function should calculate the reset mask by adding the desired values from the list below:

- 1 – Cached Responses and Logging
- 2 – Local Firewall Settings
- 4 – Learned Information
- 8 – System Security
- 16 – System State
- 32 – Untrusted Applications
- 64 – User Query Responses
- 128 – AntiVirus Tags
- 256 – Data Classification (DLP) Tags
- 512 – Local Signatures

For example, to reset the “System Security” and “System State” only, the mask should be 24, which is the addition of 8 and 16.

**Important Note:** This function blocks until the CSA MC database flags have been set, and then it returns true on success and false on failure. Note that the return of this function does not mean that all the agents have been reset – it simply means that the CSA MC has been configured to reset the agents the next time they poll, whenever that may be. Note that you may be able to expedite the polling of the agents by calling the `SendHint` function after calling the `ResetAgent` function.

## Getting Host Information

The following functions return information about the specified host(s). For each of these functions, an empty string array is returned either on error or if there are no matching hosts. `GetStatus` will return 0 on success, 1 if the host expression yields no hosts, or another number for other kinds of failure.

```
StringArray GetHostInfo (String hostExpression)
```

Each string in the returned array contains the information from the Hosts page on the CSA MC system for a given host.

```
StringArray GetLastIpAddrs (String hostExpression)
```

This function can be used to get the IP address history of one or more hosts. The format of each string in the array is as follows:

```
<ip addr> <hostname> <ACTIVE | INACTIVE>
```

For example:

```
1.1.1.1 host1 ACTIVE
1.1.1.2 host2 ACTIVE
10.10.10.10 host3 ACTIVE
10.10.10.11 host4 INACTIVE
10.10.10.12 host5 INACTIVE
```

```
StringArray GetDiagnosticInfo (String hostExpression)
```

This function can be used to get diagnostic information from the hosts that match the host expression argument.

Because of the way diagnostic information is collected and stored by the CSA MC server, this function behaves a little differently from other CSAAPI functions that get host information.

When the `GetDiagnosticInfo` function is run, the CSA MC system does two things.

1. The server sends back to your script whatever diagnostic information exists currently in the database for the appropriate hosts. If there is no existing diagnostic information in the database for a particular host, then for that host your client script will receive a string asking you to check back later for updated diagnostic information.
2. The server asks the Cisco Security Agent(s) on the appropriate host(s) to send new diagnostic information to the CSA MC system. Each host will send new diagnostic information to the CSA MC system the next time it polls (default interval is ten minutes) and this information will be stored in the CSA MC database.

Therefore, in order to get the latest diagnostic information for a particular host, it is recommended that you call the `GetDiagnosticInfo` function *twice*. This first call is made simply to ask the host for the latest information – the return value can simply be discarded. The second call is made after either calling `SendHint` or waiting for the polling interval to elapse. The returned string array from the second call will represent the latest diagnostic information available from the host.

## Getting Overall System Information

The following functions return information about the overall system.

```
StringArray GetMostActive (String objType, Integer
numOfObjects, String timespan)
```

This function returns the ‘n’ most active objects over the specified time span. This function provides the same information provided on the Status Summary page of the CSA MC UI.

Important Note: The only two object types currently supported by this function are HOST and RULE.

Important Note: The only legal values for the “timespan” variable are: DAY, WEEK, and ALL.

For hosts, the returned array will be a list of strings with a format like this:

```
myhost [W] - 174 events
```

For rules, the returned array will be a list of strings with a format like this:

```
File access control [id=266], CSA MC Security Module [W,
V5.2 r0] - 6 events
```

Examples:

To get a list of the 10 most active hosts over the past 24 hours, use the syntax:

```
GetMostActive ("HOST", 10, "DAY")
```

To get a list of the 20 most active rules over the past week, use the syntax:

```
GetMostActive ("RULE", 20, "WEEK")
```

```
Integer GetLastDayEventCount ()
```

This function returns the number of events generated in the past 24 hours.

```
StringArray GetReportNames ()
```

This function returns a list containing the names of all currently defined reports.

```
StringArray GetHostTaskNames ()
```

This function returns a list containing the names of all currently defined Host Management Tasks.

## Getting Event Information

The following functions return information about events.

```
StringArray GetLatestEvents (String objType, String objExpression, Integer numOfEvents)
```

This function returns the latest events corresponding to the objects matching the expression.

Important Note: This function does not support all the defined object types. The following types are supported: HOST, GROUP, POLICY, RULE\_MODULE, RULE. The following types are NOT supported: CLASS, VAR.

```
StringArray GetLatestAudit (Integer numOfEvents)
```

This function returns last ‘n’ audit trail events.

## Getting Reports

```
Integer GenerateReport (String reportName, String emailAddress)
```

This function generates a report. If an *empty* email address is provided, then the report is simply placed in the default report directory on the CSA MC. If, on the other hand, a legitimate email address is provided, then the report is emailed to the appropriate address and is removed from the default report directory on the CSA MC.

This function does not block until the report is created. Instead, this function creates a process that creates the report. This function returns a Process ID that can be used with GetStatus to determine when/whether the report was successfully generated.

Note: In order for this function to send email, the scripting interface must be informed of the name of the server to which to send emails. To do this, use the SetConfigVar function to set the “csaapi.email\_server” parameter to the name of the email server. Note that this must be done only once.

Note: To allow the scripting interface to send email, you must first make a minor modification to the CSA MC rule that governs permissible web server actions. Please see the scripting interface sample script README.txt files for details.

**Note**

---

To email a report to multiple addresses, separate the email addresses with a semicolon (';'). For example: joe@company.com;jane@company.com

---



# APPENDIX A

## 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](#)
- [The Agent User Interface, page A-8](#)
  - [Agent User Interface Control Rule, page A-8](#)
  - [Agent User Interface Screens, page A-9](#)
  - [Assigning Sounds to Agent Events, page A-29](#)
- [Cisco Security Agent Diagnostics, page A-29](#)
- [Resetting Cisco Security Agent, page A-30](#)
- [Cisco Security Agent Shortcut Menu, page A-30](#)
- [Turn Agent Security Off, page A-31](#)

- [Installing the Windows Agent, page A-32](#)
- [Uninstalling the Windows Agent, page A-33](#)
- [Agent Interaction with Windows Security Settings, page A-33](#)
- [Common Windows Cisco Security Agent Error Codes, page A-34](#)
- [Installing the Solaris Agent, page A-35](#)
- [Uninstalling the Solaris Agent, page A-36](#)
- [UNIX Agent csactl Utility, page A-37](#)
- [Installing the Linux Agent, page A-39](#)
- [Uninstall Linux Agent, page A-40](#)
  - [Command line method, page A-40](#)
  - [GUI method, page A-41](#)

## 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 Management Center for the Cisco Security Agent (CSA MC). This URL will allow them to see all kits that are available. That URL is:

`https://<CSA MC name>/csamc60/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 on which agents are installed must meet the following requirements:

**Table A-1 Agent Requirements (Windows)**

| System Component  | Requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Processor         | <p>Intel Pentium 200 MHz or higher</p> <p><b>Note</b> Uni-processor, dual processor, and quad processor systems are supported.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Operating Systems | <ul style="list-style-type: none"> <li>• Windows Vista Business and Enterprise editions with service pack 0 or 1.</li> <li>• Windows Server 2003 (Standard, Enterprise, Web, or Small Business Editions)</li> <li>• Windows XP (Professional, Tablet PC, or Home Edition) with Service Pack 0, 1, 2, or 3.</li> <li>• Windows 2000 (Professional, Server or Advanced Server) with Service Pack 0, 1, 2, 3, or 4</li> <li>• All Windows, Internet Explorer 4.0 or higher required.</li> </ul> <p><b>Note</b> Citrix Metaframe and Citrix XP are supported. Terminal Services are supported on Windows XP and Windows 2000.</p> <p>Supported language versions are as follows:</p> <ul style="list-style-type: none"> <li>• For Windows 2003, XP, and 2000, all language versions, except Arabic and Hebrew, are supported.</li> </ul> |
| Memory            | <p>256 MB minimum—all supported Windows 2003 R2, Windows XP, and Windows 2000 platforms</p> <p>512 MB minimum—for Windows Vista.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Hard Drive Space  | <p>60 MB or higher</p> <p><b>Note</b> This included program and data.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Network           | <p>Ethernet or Dial up</p> <p><b>Note</b> Maximum of 64 IP addresses supported on a system.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

**■ Downloading and Installing****Note**

The Cisco Security Agent uses approximately 30 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><b>Note</b> Uni-processor, dual processor, and quad processor systems are supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Operating Systems | Solaris 9, 64 bit, patch version 111712-11 or higher installed.<br>Solaris 8, 64 bit 12/02 Edition or higher (This corresponds to kernel Generic_108528-18 or higher.)<br><b>Note</b> If you have the minimal Sun Solaris 8 installation (Core group) on the system to which you are installing the agent, the Solaris machine will be missing certain libraries and utilities the agent requires. Before you install the agent, you must install the "SUNWlibCx" library which can be found on the Solaris 8 Software disc (1 of 2) in the /Solaris_8/Product directory. Install using the pkgadd -d . SUNWlibCx command. |
| Memory            | 256 MB minimum                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Hard Drive Space  | 50 MB or higher<br><b>Note</b> This includes program and data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Network           | Ethernet<br><b>Note</b> Maximum of 64 IP addresses supported on a system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## ■ Downloading and Installing

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><b>Note</b> Uni-processor, dual processor, and quad processor systems are supported. |
| Operating Systems | RedHat Enterprise Linux 4.0 WS, ES, or AS<br>RedHat Enterprise Linux 3.0 WS, ES, or AS                                  |
| Memory            | 256 MB minimum                                                                                                          |
| Hard Drive Space  | 50 MB or higher<br><b>Note</b> This includes program and data.                                                          |
| Network           | Ethernet<br><b>Note</b> 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.

Once users install agents on their systems, they are asked if they want to perform a reboot. (if Automatic reboot is not selected at kit creation time). Whether a system is rebooted or not, the agent service starts immediately and the system is protected.

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**, when no reboot occurs after install, the following caveats exist

- 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-37](#) for details. The Cisco Security Agent user interface appearance is the same on all Windows and Linux platforms.

## Agent User Interface Control Rule

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 6-6](#). 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>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.)
- **SUPPRESS taskbar notifications**—Selecting this check box in the Agent UI control rule, greatly reduces CSA notifications to the user. If the option is selected, user interaction with CSA is changed in these ways:
  - The user no longer receives balloon messages.
  - The flag icon in the system tray no longer pulses.
  - The user no longer receives tool-tip text in the task bar icon.
  - The user will no longer hear sounds for security events.

**Note**

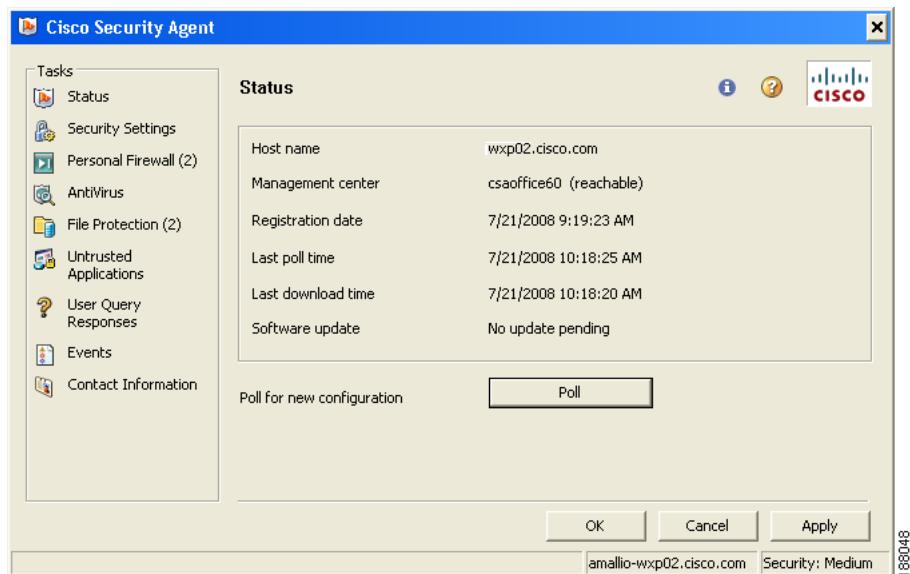
Users also have control over suppressing taskbar notifications. On the agent shortcut menu, users can select “Suppress Taskbar Notifications.” If users choose to suppress taskbar notifications, then they gain control over turning this function on or off in the future. If an administrator changes the Suppress taskbar notifications check box in this rule after a user changes the setting, the administrator’s action will have no affect on that user.

## Agent User Interface Screens

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 Status screen shows users basic information about the Cisco Security Agent and provides users with information about software updates.

**Figure A-1 Agent Status Screen**

- **Host name:** The host name of the machine on which this agent is installed.
- **Management Center:** The name of the CSA MC server with which the agent is registered and from which the agent receive policies.

Whether the CSA MC is “reachable” or “unreachable” is noted next to the name of the CSA MC. If the CSA MC is considered “reachable” it means that the host is on a network that would normally allow it to reach its CSA MC, such as the corporate network. Assuming the CSA MC is up and running, if the CSA MC is considered “reachable”, the host can receive software and policy updates. If the CSA MC is considered “unreachable” the host is not on a network that would normally be able to reach its CSA MC, such as a guest network at a customer site.

Different security policies can be enforced based on whether the CSA MC is considered “reachable” or “unreachable.” A computer running CSA may be allowed or denied access to different resources depending on whether or not the CSA MC is “reachable.”

- **Registration date:** The date and time the agent registered with CSA MC.
- **Last poll time:** The date and time when the agent last polled in to CSA MC (data is not downloaded each time the agent polls).

- **Last download time:** The date and time the agent last downloaded data from CSA MC.
- **Software update:** 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.

## Installing Software Updates

Occasionally, software updates are provided for agents. Administrators configure the central server to distribute the appropriate software updates to specified agents across the network. If there is a software update available for an agent, the agent will receive the update the next time it polls in. If the administrator has configured the update to prompt users before installing, users are notified when an update is available. Users can update at that time or postpone the update.

On Windows agents, after an update has taken place, users may be required to reboot their system within 5 minutes time. They cannot stop this reboot. They have 5 minutes to save any open documents.

On Linux agents, if the update requires a system reboot, a broadcast message will appear informing users that their system will be rebooted in 5 minutes.

See [Modify Groups With Hosts That Meet a Search Criteria, page 3-48](#) for CSA MC configuration details.



### Note

---

Use the csactl utility (see [page A-37](#)) on Solaris systems to check for updates and install them.

---

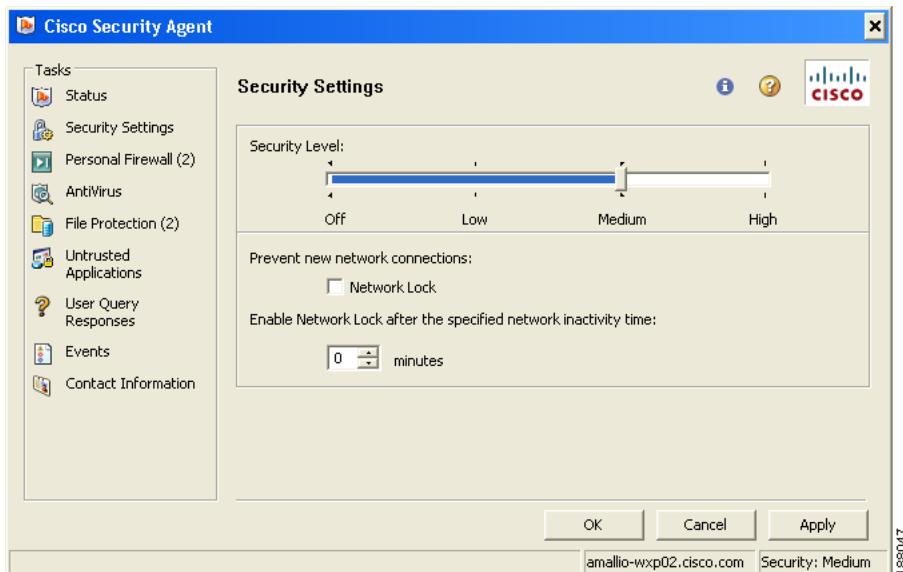
## Poll for New configuration

Clicking the **Poll** button 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. Administrators may advise users to implement this fast polling if new rules are being deployed and tested.

## Security Settings

The Security Settings screen allows users to manage their agent's security level, some aspects of its network connections, and its behavior following a local installation or uninstallation of software.

**Figure A-2 Agent Security Settings Screen**



### Security Level

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 administrators have not defined different levels of security states for the agents, moving the sidebar between security levels will not alter their security.

Some examples of how administrators might define various configuration levels are as follows:

A **High** 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 you the option of allowing them via a query user pop-up box (as might be available in lower settings).

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 you to be presented with more query pop-up boxes to ensure that the action taking place is intended by you and not a type of attack.

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, you could be queried as to whether the detected action should be allowed or not.

The **Off** security setting disables all agent security.

**Caution**

---

In all cases, whether you have states defined for all security levels or not, moving the sidebar to Off will disable all agent security. When security is disabled, a red “x” appears over the agent flag.

---

## Preventing New Network Connections

When the **Network Lock** checkbox is enabled, the agent will not allow any new network connections on the system. Disabling the checkbox disables the network lock.

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. 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.

**Note**

---

If you have the Network Lock enabled and you reboot your system, Network Lock is no longer turned on after the reboot. (All other agent settings, except temporary query response caching, remain constant across reboots.)

---

## Install / Uninstall Detected

The Cisco Security Agent temporarily suspends certain security settings when users are installing or uninstalling software that was downloaded over the network. If users select “Yes” when they are queried whether to allow an installation to proceed, an additional **Resume** button appears in the Security Settings window. If the agent doesn't automatically detect that the install has completed, users can click the Resume button to inform the agent when the install or uninstall process has finished. This way, the agent knows the process is done and it can reinstate all suspended security immediately. If users do not click the Resume button, the agent automatically reinstates suspended security after a certain period of time.

If the install/uninstall requires you to reboot the system when it completes, all agent security settings suspended during that time are reinstated at boot time whether users answered the agent installation completion query or not before rebooting.

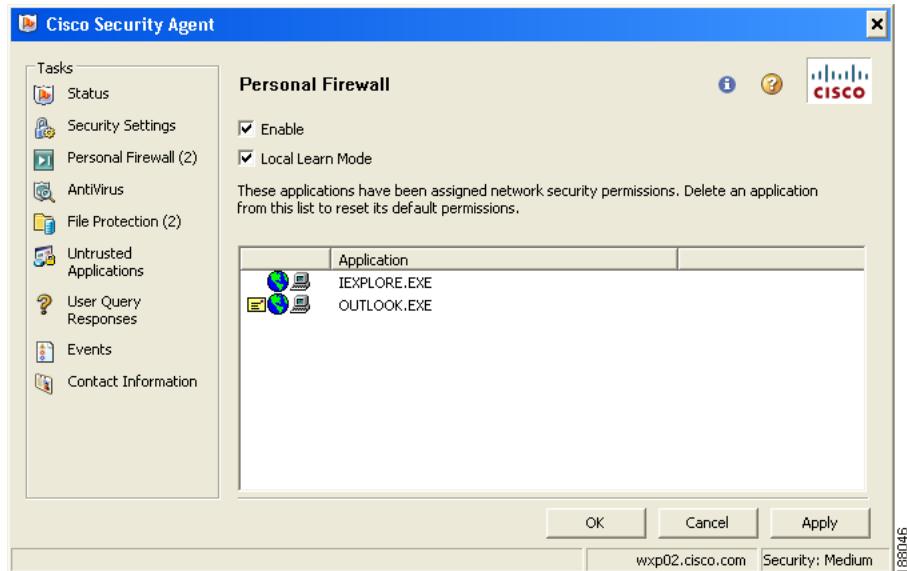


### Note

In some cases, a virus can appear to be an install or uninstall program by attempting to delete or modify executables or other system files. When you install and uninstall software, the agent queries you to ensure that you are indeed altering a configuration intentionally and that some other unintended action is not taking place.

## Personal Firewall

Personal Firewall settings restrict certain applications from making certain types of network connections.

**Figure A-3 Agent Personal Firewall Screen**

The Personal Firewall feature gives users the ability to add restrictions to the security policies created by system administrators. It is not possible to use this functionality to make security policies more permissive.

To use the Personal Firewall, click the **Enable** checkbox. If Local Learn Mode is not checked, then each time a new application attempts to connect to the network, users will be asked whether this connection should be permitted. If they respond no, then connections of this type will be denied in the future. If they respond yes, then future connections of this type will be allowed, assuming that they are not denied by other security policies.

After Enabling the Personal Firewall, users may find that they get a lot of query dialogs. By clicking the **Local Learn Mode** checkbox, users instruct CSA to assume that all network connections not otherwise denied by CSA policies are permitted. The application list on this screen will be populated and will indicate that these applications are allowed to make certain connections. In effect, the Local Learn Mode checkbox allows users to bypass the query boxes while CSA learns what connections are permissible. After a certain period of time, though, users should uncheck the Local Learn Mode box so that they will be queried when applications they use infrequently attempt to access the network.

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. An application can have up to 4 permission types assigned to it. Refer to the [Permission Key](#) below for a description of each possible network service graphic.

If users want to change the assigned permissions of a given application, they select it in the edit box and press the **Delete** key. When they click the **Apply** button, the delete takes effect on the system. When users next invoke the application, they will be queried. They should respond to the query accordingly to reset permissions for the application.

On Windows systems, users can remove items or choose a sorting order by right-clicking in the personal firewall window.

**Note**

Users may be prompted several times in order for email applications to receive the various network permission types it optionally uses. In some cases, an email may have http links within it. If so, the agent prompts users to allow or deny your email application http access to the network. While waiting for your response, the agent pends the http request. As a result, even if users answer Yes to this permission, the http access may fail on the first attempt. If so, users should close their email application and open it again. Now the http permission for their email application will function normally.

**Note**

If a host belongs to a group operating in Audit Mode, local firewall settings are ignored.

**Table A-4      Permission Key**

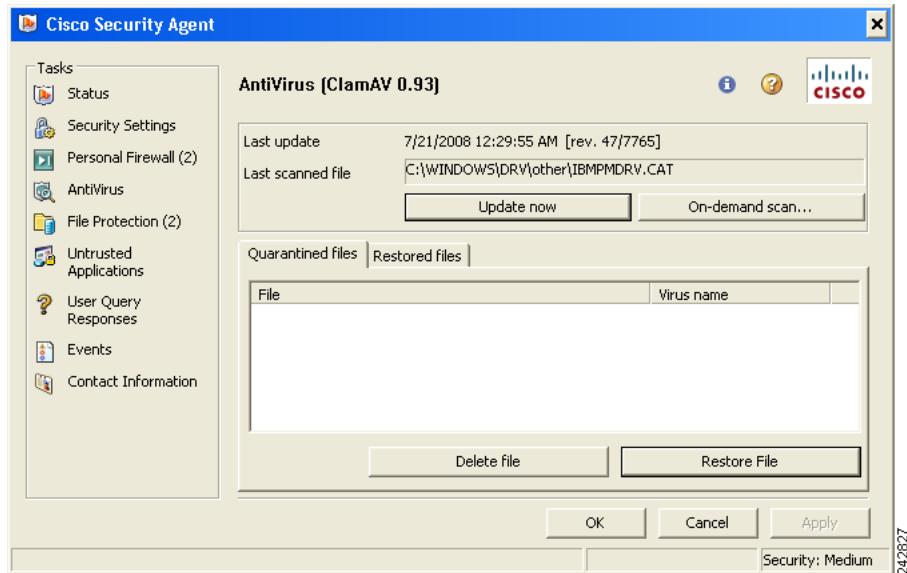
| <b>Symbol</b>                                                                     | <b>Description</b>                                                                     |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
|  | This indicates whether or not an application has email network permissions.            |
|  | This indicates whether or not an application has http network permissions.             |
|  | This indicates that an application can or cannot make network connections as a client. |
|  | This indicates that an application can or cannot make network connections as a server. |

## AntiVirus Protection

The AntiVirus screen allows users to update their local signature database, perform on-demand virus scans, and manage quarantined files.

## The Agent User Interface

**Figure A-4 Agent AntiVirus Screen**



### Updating Signature Database

The AV signature update field indicates the last time that local signature database was updated. <Never> indicates that the local signature database installed with the agent has not been updated.

Clicking **Update now** manually retrieves updates to the signature database.

### Last scanned file

The Last scanned file field shows the path to the last file scanned as a result of a CSA rule triggering the virus scan. The last file scanned after an On-demand scan does not appear in this field.

### On-demand Scan

Clicking On-demand scan opens the AntiVirus On-demand scan window. To configure an on-demand scan, follow this procedure:

- 
- Step 1** Specify directories to be scanned: Click **Add**, browse to the drive or directory you want to scan for viruses and click **OK**. The path is added to the Directories to be scanned window. Repeat this step until you have specified all the locations you want to scan.



**Note** Directory scans are recursive. That is, all the subdirectories in the directory you specify will be scanned in addition to the directory you specify.

---



**Note** You can remove a directory from Directories to be scanned list by selecting the path and clicking **Remove**.

---

- Step 2** Specify the scan speed:

- **Fast:** Performs the scan the most quickly and uses the most CPU resources. It may prevent you from performing other tasks.
- **Normal:** Performs the scan at a moderate pace and uses a moderate amount of CPU resources. It may impact other operations.
- **Slow:** Performs the scan at a slow pace and uses the least amount of CPU resources. It has the least impact on other operations.

- Step 3** Click **Start scan**.

The Scan progress area displays the directory and file being scanned and a summary of the number of files scanned, files found to be infected, and elapsed time of the scan. When the scan is complete, the tile bar of the window will read, “AntiVirus On-demand scan [complete].”



**Note** If you want to stop the scan while it is running, click **Stop scan**. If you restart the scan, the scan will begin again at the beginning of the list of directories to be scanned.

---

## Quarantined Files Window

If a file is found to have a virus after being scanned, it is quarantined in place and listed in the Quarantined files window. Users can delete quarantined files by selecting them from the list and clicking **Delete file(s)**. If a quarantined file is deleted from their computer for any reason, it is also removed from the Quarantined files list.

If users feel a file has been quarantined erroneously, they can move it to the Restored files list by selecting the file and clicking **Restore File**.

## Restored Files Window

The files in the **Restored files** list were originally quarantined and then Restored by the local user. If a Restored file is deleted from the computer for any reason, it is also removed from the Restored files list.

If users feel a file has been Restored erroneously, they can move it to the Quarantined files list by selecting the file and clicking **Quarantine File**.

## File Protection

Through some simple configuration, the agent can protect specified local files and directories on your system from all network access. This is useful if you have sensitive personal information stored on your system. Entering the name of the file or directory that you want protected cuts off all network access to that resource.

You can add files and folders to the file protection window by browsing for them or by entering them in the edit field using the proper syntax. Note that if a network application attempts to access a protected file, you are queried. In some instances, you may want to allow this access.

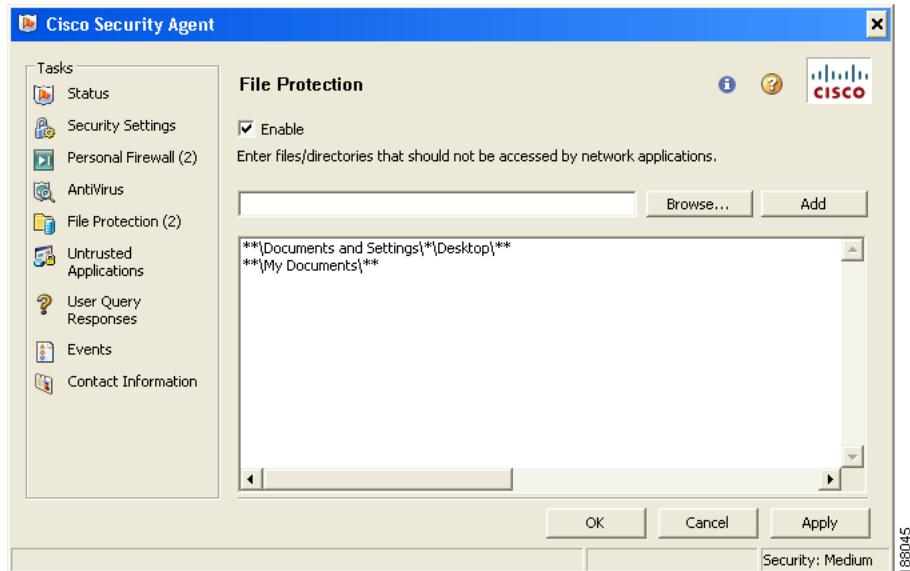


### Note

---

Files and directory names must be added to the File Protection window using a specific syntax. That syntax is explained to end-users in the Cisco Security Agent online help.

---

**Figure A-5 File Protection**

## Selecting Files for Protection

- 
- Step 1** Select **Enable** check box. This turns on File Protection.
  - Step 2** Click **Browse**.
  - Step 3** Select the file you want to protect; it appears in the edit box.
  - Step 4** (Optional) Using the required syntax, edit the path displayed in the edit box. This will allow you to specify folders instead of files or generalize the location of a file.
  - Step 5** Click **Add**. The information in the edit box is now added to the file protection window and protected from all network access. (Note that if a network application attempts to access a protected file, you are queried. In some instances, you may want to allow this access.)
  - Step 6** Click **Apply**.
  - Step 7** When you are done adding files and folders to the file protection window, click **OK**.

## Entering Files and Folders For Protection

- 
- Step 1** Check the **Enable** check box. This turns on file protection.
  - Step 2** In the edit field, type the name of the file or folder you want to protect. Be sure to use the required syntax explained in the agent help.
  - Step 3** Click **Add**. This file or directory added to the file protection window and is now protected from all network access.
  - Step 4** Click **Apply**.
  - Step 5** When you are done adding files and folders to the file protection window, click **OK**.

## Removing File Protection

- 
- Step 1** Right-click the file name or directory name in the file protection window.
  - Step 2** Select **Remove**.
  - Step 3** Click **Apply**.
  - Step 4** When you are done removing files and folders from the file protection window, click **OK**.

## Disabling File Protection

To disable File protection, uncheck the Enable checkbox in the File protection screen. The File Protection window is grayed out.

The contents of the File Protection window are saved for when you want to turn file Protection on again.

To remove file protection, users select the file name or directory name in the edit field and press the **Delete** key. When they click the **Apply** button, the delete takes effect on the system.

## Untrusted Applications

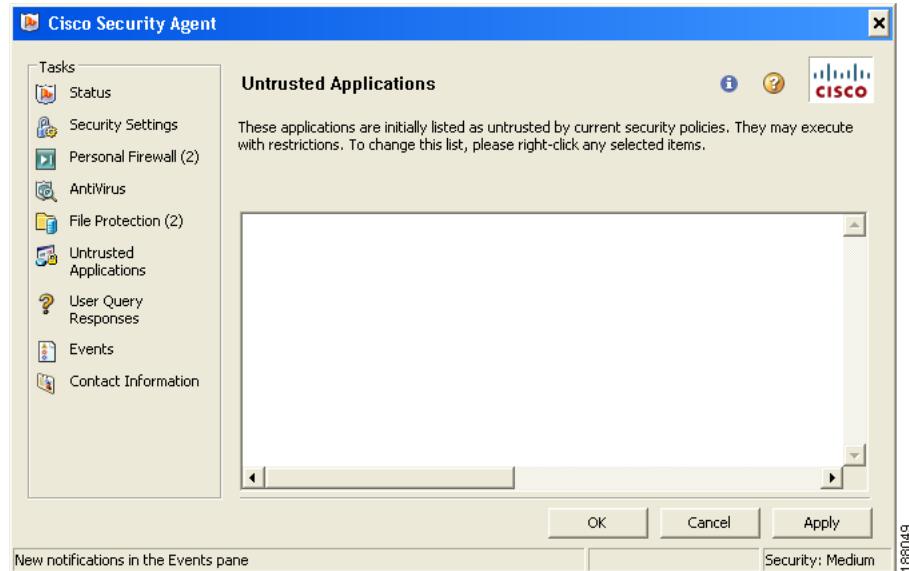
The Cisco Security Agent can keep track of downloaded files that are either applications or that could contain programmatic content such as scripts or macros. Depending on how the agent was configured by the system administrator, these files are considered Untrusted and their filenames are displayed in the Untrusted

Applications edit box. The consequences of being labeled Untrusted are defined by the system administrator, but in general files listed here continue to operate, but under restrictions greater than those of trusted files. For example, untrusted applications may not be able to write to system executables or to registry keys that are typically targeted by viruses.

**Note**

With the default Windows handling for file extensions, a .txt file would not be considered executable, and would not be marked as an Untrusted file.

**Figure A-6** Agent Untrusted Applications Screen



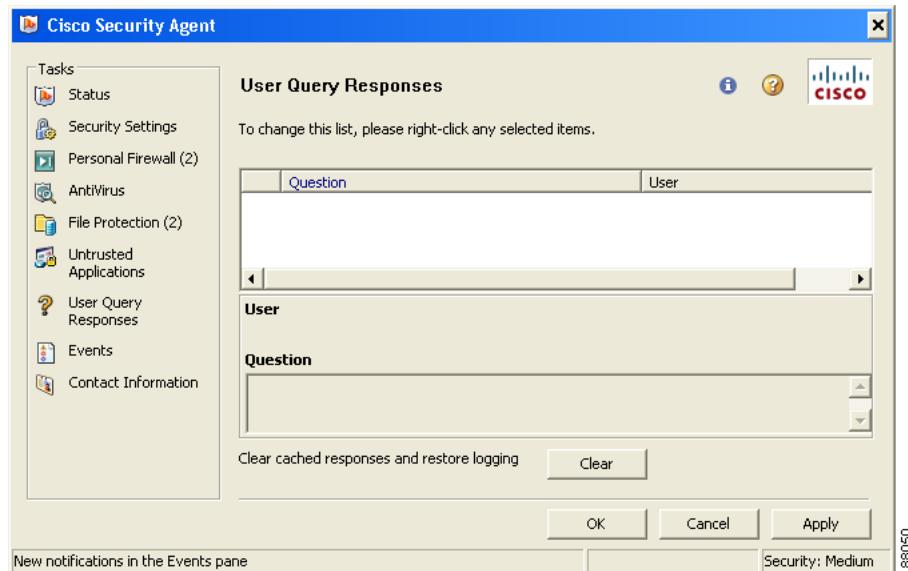
For Windows agents, if users want to remove a file or program from the list of untrusted applications in the Untrusted Applications window, they right-click on the selected entry in the edit box and select **Mark As Trusted**. This removes the application from the untrusted list, making it trusted.

For Linux agents, if users want to remove a file or program from the list of untrusted applications in the Untrusted Applications window, they select the entry in the edit box and press the **Delete** key. When they click the Apply button, the delete takes effect on the system.

## User Query Responses

This screen allows you to manage your responses to user queries.

**Figure A-7 Agent User Query Responses Screen**



## Responding to Pop-up Query Boxes

The management center administrator can create rules that prompt users to allow or deny an action, or terminate a process, when an attempt is made by a process, to access resources on their system. In this case, if the rule in question is triggered, a pop-up box appears prompting users to select from several possible radio buttons and click **Apply** as follows:

- **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.

**Default Action** - If users do not respond to the query within 5 minutes, an administrator-determined default action is automatically taken.

**Don't ask again** - The administrator can optionally display a “Don't ask again” checkbox on the query so that the user's response is remembered. If users select that checkbox when responding to the query, and the same query is triggered on the system, the remembered response is automatically taken and they are not queried again.

**Query challenge** - For added security, the administrator can optionally issue a query challenge on the query pop-up box. This ensures that the local user is answering the query and not a malicious remote user or program. To pass the challenge, users simply enter the information displayed in a graphic on the pop-up box itself.

## Remembering and Caching Query Responses

When users are queried, the agent can remember their response permanently or temporarily. This way, if the same query is triggered again, the action is allowed, denied, or terminated based on what they answered previously without a pop-up query box appearing again either permanently, or for some period of time. In order to reduce the number of queries users must respond to, it is generally advantageous for them to permanently remember query responses.

For example, if users are queried as to whether an application can talk on the network and they respond by selecting the **Yes** radio button, clicking the **Don't ask me again** checkbox, and then clicking **Apply**, the Yes response is remembered permanently and that response appears in the edit field in this window. But if users are queried as to whether setup.exe can install software on their system and they respond by clicking the **Yes** radio button, but there is no **Don't ask me again checkbox** or it is there but they do not select it, this response is remembered temporarily and it does not appear in the edit field. It is the **Don't ask me again checkbox** that controls whether a query response is remembered permanently. The administrator decides whether or not users have the option to choose **Don't ask me again**.



### Note

Permanent responses are remembered across reboots. Temporarily cached responses are not remembered across reboots.

**Note**

A query response is tied to the user who responded. On multi-user machines, multiple users may be asked the same question.

---

**Note**

On Windows agents, users can sort User Query Responses in the edit field by right-clicking within in the edit field and selecting one of many Sort options.

---

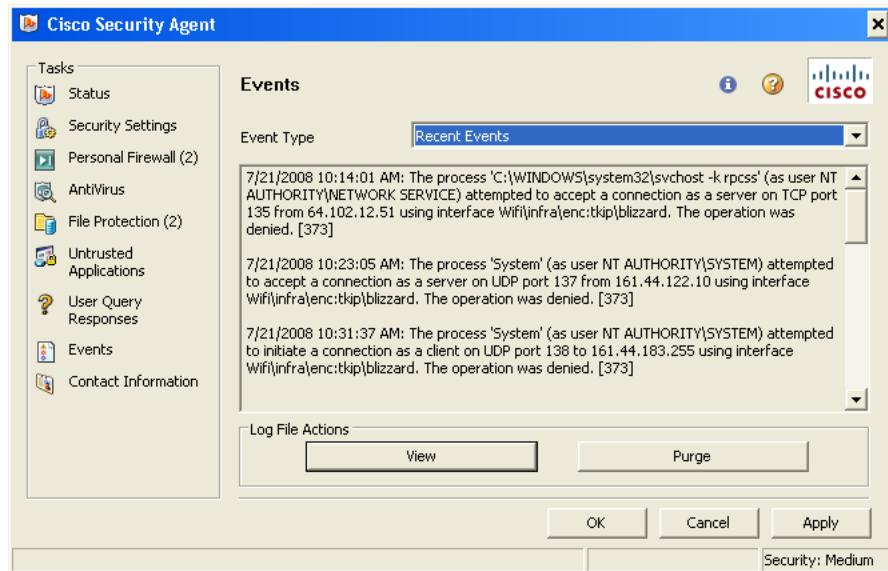
## “Undoing” or Deleting Your Response to a Query

If a response is only cached temporarily (for approximately an hour) users can click the **Clear** button in this window to delete all temporarily cached responses.

On Windows agents, to clear permanent responses listed in the agent User Query Responses window edit field, users right-click on a selected response in the edit field and select **Remove**. On Linux agents, to clear permanent responses listed in the agent User Query Responses window edit field, users select the response in the edit field and press the **Delete** key. When they click the **Apply** button, the delete takes effect on the system.

## Events

The Events window displays security-related messages, system errors, and system status messages generated by Cisco Security Agent.

**Figure A-8 Agent Events Screen**

188044

To view events, follow this procedure:

- 
- Step 1** Click **Events** in the Tasks area of the Cisco Security Agent interface.
- Step 2** Select the set of events to display from the **Event Type** list box.
- Selecting **Recent Events** displays important security-related messages received by the agent beginning at the last time the agent interface was launched.
  - Selecting **All Logged Security Events** displays all security-related messages received by the agent, including those generated before the agent interface was launched.
  - Selecting **All Logged Events & Debug Messages** displays all security-related messages, system errors, and system status messages generated by Cisco Security Agent, including those generated before the agent interface was launched.

Clicking the **View** button launches a text file containing more detailed information than the event type you have chosen to display.

## The Agent User Interface

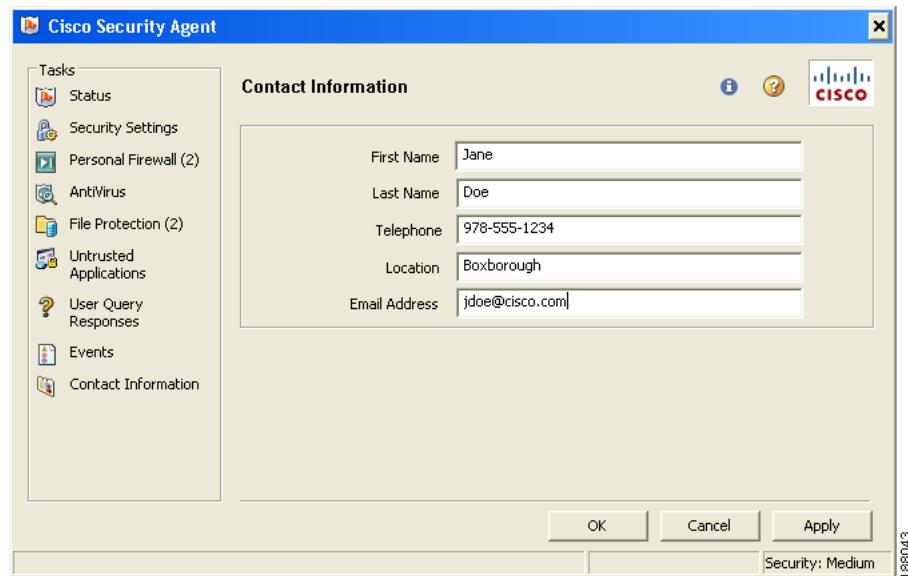
Clicking the **Purge** button clears the messages displayed by the Recent Events or All Logged Security Events event types. You can not purge the messages displayed by the All Logged Events & Debug Messages event type.

## Contact Information

This window allows you to provide contact information to the administrator, including your name, telephone number, location, and email address. If your system administrator has requested that you enter this information, do so here and click the **Apply** button.

CSA MC receives this contact data and the administrator can now quickly locate you if your agent indicates that there is a problem.

**Figure A-9 Agent Contact Information Screen**



## Assigning Sounds to Agent Events

Different sounds can be assigned to different agent events on Windows systems. Through your Windows operating system's Sounds and Multimedia Properties window, accessible from the Start>Settings>Control Panel window, you can assign specific sounds to Cisco Security Agent events. In the Sounds and Audio Devices Properties window, users scroll through the list of Sound Events in the Sounds tab to locate Cisco Security Agent and the list of available sound event assignments.

As an example, users can configure their system to generate a sound when the flag in the system tray begins flapping because a rule has been triggered. They can also have a sound occur when a Query User pop-up window appears and then have another sound occur when the countdown to respond to this query is down to 1 minute. Users must have a sound card installed to play these sounds.

## Cisco Security Agent Diagnostics

This feature allows the agent to gather self-describing diagnostic information about the agent and about the system on which the agent runs. Generally, users should only select this if the administrator has requested that they do so. It may take some time to collect this data. Cisco Security Agent Diagnostics are available for Windows, Solaris, and Linux platforms.

On **Windows** systems, this setting is available from the **Start>Programs>Cisco>Cisco Security Agent** menu when the agent is installed. Selecting **Cisco Security Agent Diagnostics** causes the agent to gather information on the system and on the agent itself. When the collection is complete, a “csa-diagnostics.zip” file is created in the user’s system temp directory. They should send this file to their administrator.

Host diagnostics are available locally to the **Solaris** and **Linux** end user by executing the ./diag shell script from the /opt/CSCOcsa/bin directory. This creates a csa-diagnostic.gz file in the /tmp directory.



### Note

The same data can be collected remotely from the CSA MC. Only ask users to manually gather this data if for some reason remote diagnostics is not working.

# Resetting Cisco Security Agent

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 Firewall Settings or File Protection settings are enabled, they are disabled after a reset as this is the default factory setting. The information entered into the edit boxes for these features is not lost.

On Windows systems, this setting is available from the **Start>Programs>Cisco>Cisco Security Agent** menu on systems where the agent is installed. On Linux systems, this setting is available from the **Red Hat Application Menu>Cisco Security Agent** menu on systems where the agent is installed.

# Cisco Security Agent Shortcut Menu

Right-click the CSA icon in the system tray to view the agent's shortcut menu. These are the menu items and their functions:

| Menu item                                                | Description                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Open Agent Panel</b>                                  | Launches Cisco Security Agent user interface. You can also do this by double-clicking the CSA icon.                                                                                                                                                                                                                                                                                      |
| <b>Suppress Taskbar Notifications</b><br>(Windows only.) | Selecting this menu item changes your interaction with CSA in these ways: <ul style="list-style-type: none"> <li>• The flag icon in the system tray on longer pulses.</li> <li>• You no longer receive tool-tip text for the task bar icon.</li> <li>• You no longer hear sounds for security events.</li> <li>• You no longer receive balloon message, such as the one below</li> </ul> |
| <b>Security Level</b>                                    | Allows you to set the security level to Off, Low, Medium, or High. This is equivalent to using the slide bar on the Security Settings screen.                                                                                                                                                                                                                                            |

| Menu item                   | Description                                                                                                                              |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Network Lock</b>         | Prevents new network connections to the host. This is the same as enabling the network lock on the Security Settings screen.             |
| <b>Help</b><br>(Linux only) | Launches Help for the CSA Agent Panel.                                                                                                   |
| <b>About</b>                | Displays the version number of CSA that is installed on your computer. This is the same as clicking the icon.                            |
| <b>Exit Agent Panel</b>     | Closes the Cisco Security Agent user interface. Though the interface has been closed, CSA is still running and protecting your computer. |


**Note**

On Linux systems, the CSA icon is not visible in the system tray until you run it from the applications menu. Navigate **Applications>Cisco Security Agent>Cisco Security Agent** to run Cisco Security Agent.

## Turn Agent Security Off

Provided there is not an Agent service control rule or Agent UI control rule (See [Agent Service Control, page 6-3](#) and [Agent UI Control, page 6-6](#) 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 sidebar (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.

## ■ Installing the Windows Agent

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 csagent
net start csagent
```



### Note

On Windows Vista desktops, standard users must elevate their privileges to “administrator” in order to run these commands.

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 the Windows Agent

The Windows agent kit is a self-extracting executable. You can save the agent kit to disk and install it from there by double-clicking on the file, or you can choose to install it over the network from CSA MC.

Follow the installation prompts, clicking **Next** when appropriate. You can install to the default directory Program Files\Cisco\CSAgent or you can choose another directory.

Agent kits may be configured to require a reboot after the agent is installed, otherwise users are given the option to reboot. Some security is provided immediately after the agent is installed and before the machine is rebooted.

The following functionality is available only after the system has been rebooted:

- Network Shield rules are not applied.

- 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. To benefit from all the security features of CSA, users should reboot their computer after the agent is installed.

See also [Manual Agent Data Filter Installation, page 12-11](#) if you are installing a web server on the same server as the Windows agent.

See also [Agent Interaction with Windows Security Settings, page A-33](#) for descriptions of how the agent interacts with the Windows Firewall and the Windows Security Center.

## Uninstalling the Windows Agent

To uninstall the Cisco Security Agent, do the following:

- 
- Step 1** From the Start menu, go to **Programs>Cisco>Cisco Security Agent>Uninstall Cisco Security Agent**.
- Step 2** Reboot the system when the uninstall is finished.

## Agent Interaction with Windows Security Settings

The Cisco Security Agent automatically disables the Windows firewall and CSA's status will not be visible in the Windows Security Center if the host is joined to a domain.

## Agent Disables Windows Firewall

The Cisco Security Agent automatically disables the Windows XP and Windows 2003 firewall. This is done per recommendation of Microsoft in their HELP guide for their firewall. If you want to read this recommendation, you can access the "Windows Security Center" console from a Windows XP or Windows 2003 installation, click on "Windows Firewall", and select "on." The firewall

## ■ Common Windows Cisco Security Agent Error Codes

status will warn you as follows: “Two or more firewalls running at the same time can conflict with each other. For more information see Why you should only use one firewall.”

Because the Cisco Security Agent, in part, utilizes firewall-like components, the agent disables the Windows firewall per the recommendation from Microsoft.

If Cisco Security Agent is uninstalled, the Windows Firewall is automatically re-enabled.

## Agent Status is not Reported in the Security Center

If Cisco Security Agent is installed on a computer that **is not** joined to a domain, then the Windows Security Center provides a status message about CSA in the Firewall Programs status area. The message indicates if Cisco Security Agent is on or off.

If Cisco Security Agent is installed on a computer that **is** joined to a domain, then the Windows Security Center does not provide status messages about CSA.

If the system administrators for your enterprise want users to see status messages in the Windows Security Center about CSA, they will need to set this node to “on” in the Group Policy Object Editor (Gpedit.msc.):

```
Computer Configuration\Administrative Templates\Windows Components\Security Center
```

## Common Windows Cisco Security Agent Error Codes

The following are the most commonly seen error codes for Windows agent installations.

2029 - OKENA\_STATUS\_DB\_ERROR. This message usually indicates that the database is down or busy.

2030 - OKENA\_STATUS\_LICENSE\_REACHED\_LIMIT.

2031 - OKENA\_STATUS\_REGISTRATION\_NOT\_ALLOWED. This indicates that the CSA MC registration control is actively denying agent registration.

2035 - OKENA\_STATUS\_INVALID\_LICENSE. This indicates that the license is corrupt or expired.

2037 - OKENA\_STATUS\_REGISTRATION\_BACKOFF. This indicates that an agent with the same IP address has already registered with CSA MC in the past hour.

# 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. After 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. (In the following example, **CSA-Server\_6.0.0.265-setup.tar** is the name of the agent kit.)

```
tar xf CSA-Server_6.0.0.265-setup.tar
```

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

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

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.
```

**Step 4** 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

## ■ Uninstalling the Solaris Agent

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.



**Note** 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.

---



**Note** See also [Manual Agent Data Filter Installation, page 12-11](#) if you are installing a web server on the same server as the Solaris agent.

---

# Uninstalling the Solaris Agent

To uninstall the agent, follow this procedure:

**Step 1** Log on to the server as the superuser.

**Step 2** Open a console in single user mode.

**Step 3** At the prompt, enter this command:

# pkgrm CSCOcsa

**Step 4** Enter y when asked if you want to uninstall CSA.

**Step 5** Enter y when asked if you want to continue to remove the package.

**Step 6** Reboot the server when done.



- 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 6-3](#) 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.<br>(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.<br>(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. |

**■ UNIX Agent csactl Utility**


---

|                |                                                                                                                                                                                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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: 2006-11-20 15:19:16
Host id: {FG9DA858-6131-46E9-18BD-EE32BA2D0676}
Last download time: 2006-11-20 15:19:23
Last poll time: 2006-11-20 15:20:42
Software update: newer version is available
```

For example, to perform a software update:

```
/opt/CSCOcsa/bin/csactl swupdate
```




---

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_V5.2.0.218-lin-setup-1a969c667ddb0a2d2a8da3e7959a30b2.t
ar /tmp
```

- Step 2** Untar the file.

```
$ cd /tmp
$ tar xvf
CSA-Server_V5.2.0.218-lin-setup-1a969c667ddb0a2d2a8da3e7959a30b2.t
ar
```

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

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

- Step 4** Run script install\_rpm.sh as root.

```
./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.)

**Note**

See also [Manual Agent Data Filter Installation, page 12-11](#) if you are installing a web server on the same server as the Linux agent.

## Uninstall Linux Agent

Cisco Security Agent can only be uninstalled by the “root” user. You can uninstall Cisco Security Agent through a command line or GUI interface.

**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 system are not changed to restrict this access.) See [Agent Service Control, page 6-3](#) for details on this rule type.

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

## Command line method

**Step 1** Log on to the computer as the root user.

**Step 2** Open a Terminal window.

**Step 3** Find the correct version number of the CSA rpm by running this command:

```
rpm -qf /opt/CSCOcsa/bin/ciscosecd
```

The name of the rpm is displayed in this form: CSAagent-6.0-5228

**Step 4** Remove the rpm by running an rpm -ev command referencing the correct package name. This is an example of that command:

```
rpm -ev CSAagent-6.0-5228
```

**Step 5** Reboot the machine after the uninstallation has completed.

## GUI method

- 
- Step 1** Log on to the computer as the root user.
  - Step 2** From the Red Hat menu, navigate **Cisco Security Agent > Uninstall Cisco Security Agent**.
  - Step 3** When prompted, respond to the challenge to disable security for Cisco Security Agent by selecting **Yes** and clicking **Apply**.
  - Step 4** Enter the text in the challenge window and click **OK**. Cisco Security Agent is uninstalled.
  - Step 5** Press **Enter** to exit the Terminal window.
  - Step 6** Reboot the machine after the uninstallation has completed.

■ Uninstall Linux Agent



# APPENDIX **B**

## 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.

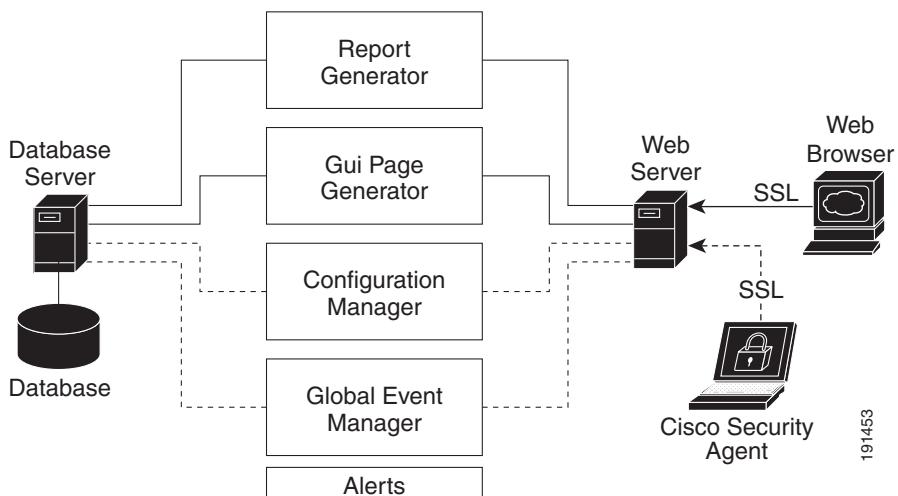
This section contains the following topics.

- [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

191453

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.

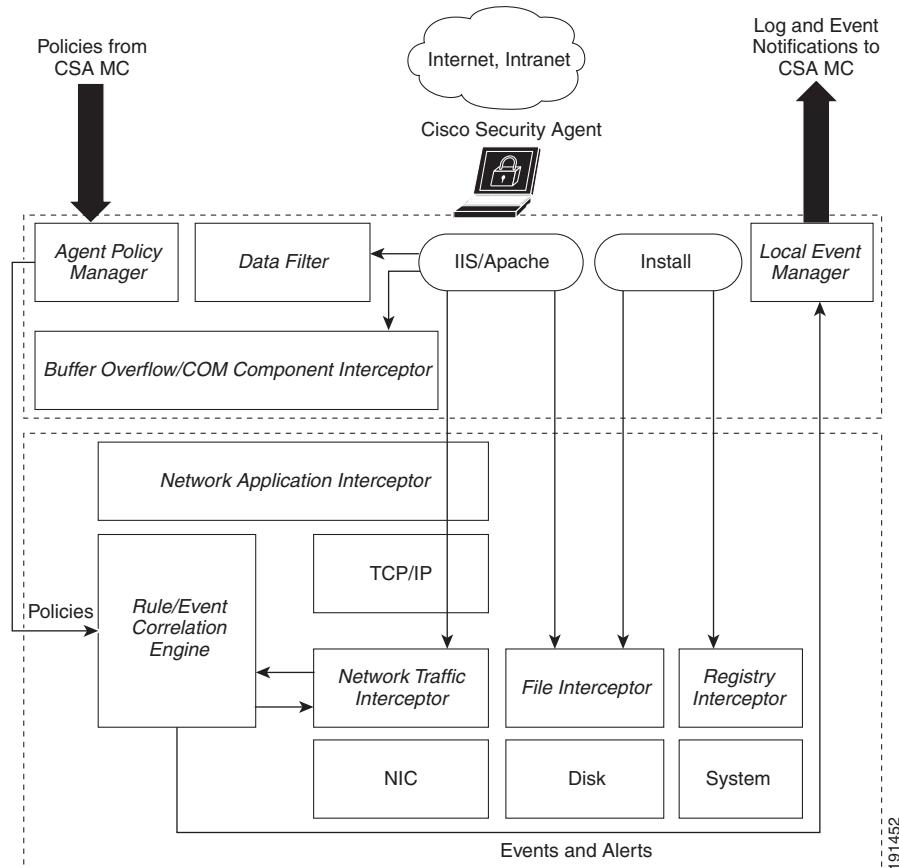
All information (rule configurations, event logs, etc.) passed between CSA MC and the agents distributed across your enterprise is encrypted providing a secure communication channel for the exchange of data.

# 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)**

## Cisco Security Agent Windows Architecture



191452

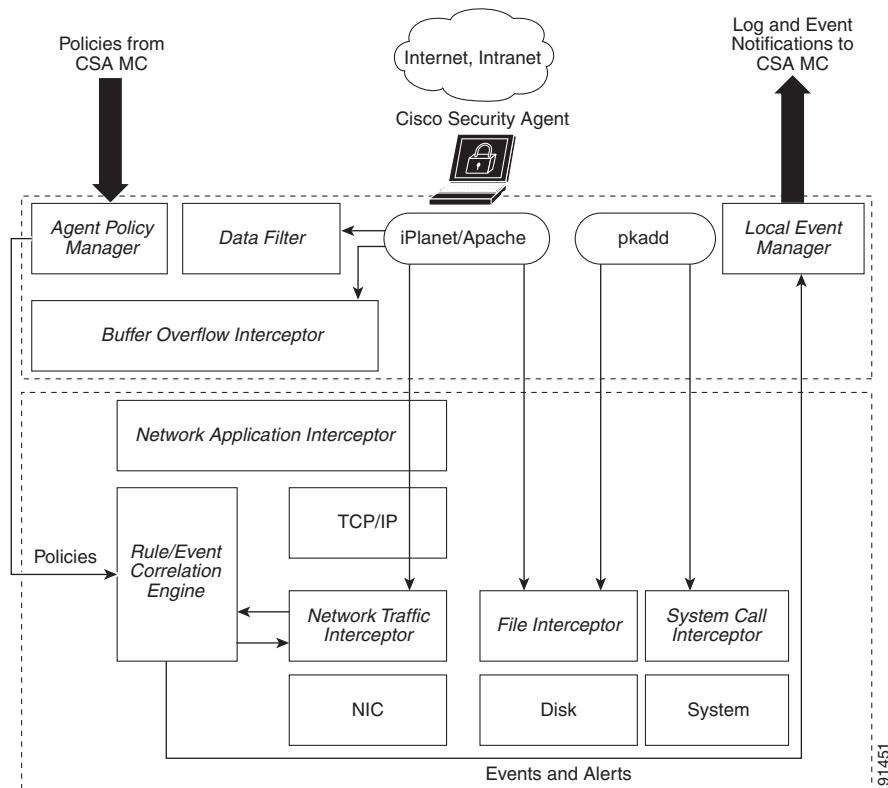
Starting from the left side of the diagram, the agent **policy manager** receives the rules configured by the administrator from CSA MC. These rules are sent to the agent's **rule/event correlation** engine. If a rule set already exists there, those rules are updated or replaced with the newest rule 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.

## Agent Components

**Figure B-3 Cisco Security Agent Components (UNIX)****Cisco Security Agent UNIX Architecture**



# C APPENDIX

## Open Source License Acknowledgements and Third Party Copyrights

---

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

The following acknowledgements pertain to this software license.

- [OpenSSL/Open SSL Project](#), page C-2
- [Apache \[version 2.0.59\]](#), page C-5
- [TCL license](#), page C-9
- [Perl](#), page C-10
- [Socket6](#), page C-10
- [libpcap](#), page C-11
- [CMU-SNMP Libraries](#), page C-12
- [Open Market FastCGI](#), page C-13
- [CGIC License](#), page C-14
- [Mozilla 1.xx \(libcurl\)](#), page C-14
- [MICROSOFT SOFTWARE LICENSE TERMS](#), page C-15
- [.Net Framework 2.0](#), page C-19
- [MarshallSoft Computing SMTP/POP3 Email Engine](#), page C-20

- Jasper Reports V1.2.0 and JFreeChart V1.0.5, page C-21
- iText version 1.3.1, page C-32
- Java Runtime Environment JRE 1.5.0.06, page C-42
- The GNU General Public License (GPL), page C-46

## 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](mailto:openssl-core@openssl.org).

### OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

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

1. Redistributions of source code must retain the 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](mailto: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](mailto:eay@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

#### **Original SSLeay License:**

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

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

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

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

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

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

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

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

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

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

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF

SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

## Apache [version 2.0.59]

### Xerces 2.7 and AxisCpp 1.6

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

Apache License

Version 2.0, January 2004

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

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

#### 1. Definitions.

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

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

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

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

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

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

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

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

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

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

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

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.
4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
  - (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
  - (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
  - (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
  - (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within

Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

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

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. Trademarks. This License does not grant permission to use the tradenames, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for

loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

#### END OF TERMS AND CONDITIONS

## TCL license

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

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

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

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

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

## Perl

Copyright 1987-2005, Larry Wall

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

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

## Socket6

Copyright (C) 2000-2005 Hajimu UMEMOTO <ume@mahoroba.org>. All rights reserved.

Socket6.pm and Socket6\_xs are based on perl5.005\_55-v6-19990721 written by KAME Project.

gai.h, getaddrinfo.c and getnameinfo.c are based on ssh-1.2.27-IPv6-1.5 written by KIKUCHI Takahiro <kick@kyoto.wide.ad.jp>.

Copyright (C) 1995, 1996, 1997, 1998, and 1999 WIDE Project. All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

**THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT 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.**

# libpcap

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

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

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

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

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

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

## CMU-SNMP Libraries

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

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

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

## Open Market FastCGI

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

Open Market permits you to use, copy, modify, distribute, and license this Software and the Documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this Software and Documentation may be copyrighted by their authors and need not follow the licensing terms described here. If modifications to this Software and Documentation have new licensing terms, the new terms must be clearly indicated on the first page of each file where they apply.

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

## CGIC License

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

## Mozilla 1.xx (libcurl)

### COPYRIGHT AND PERMISSION NOTICE

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

All rights reserved.

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

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

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

# MICROSOFT SOFTWARE LICENSE TERMS

## MICROSOFT SQL SERVER 2005 EXPRESS EDITION

## MICROSOFT SQL SERVER 2005 EXPRESS EDITION WITH ADVANCED SERVICES

## MICROSOFT SQL SERVER 2005 EXPRESS TOOLKIT

## MICROSOFT SQL SERVER 2005 MANAGEMENT STUDIO EXPRESS

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

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

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

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

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

### 1. INSTALLATION AND USE RIGHTS.

- a. Installation and Use. You may install and use any number of copies of the software on your devices.
- b. Included Microsoft Programs. The software contains other Microsoft programs. These license terms apply to your use of those programs.

### 2. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.

- a. Distributable Code. You are permitted to distribute the software in programs you develop if you comply with the terms below.
  - i. Right to Use and Distribute. The software is "Distributable Code."
- Distributable Code. You may copy and distribute the object code form of the software. You may not modify the software, and your programs must include a complete copy of the software, including set-up.

**MICROSOFT SOFTWARE LICENSE TERMS**

- Third Party Distribution. You may permit distributors of your programs to copy and distribute the Distributable Code as part of those programs.
    - ii.** Distribution Requirements. For any Distributable Code you distribute, you must
      - add significant primary functionality to it in your programs;
      - require distributors and external end users to agree to terms that protect it at least as much as this agreement;
      - display your valid copyright notice on your programs;
      - indemnify, defend, and hold harmless Microsoft from any claims, including attorneys' fees, related to the distribution or use of your programs; and
      - if the software is Microsoft SQL Server 2005 Management Studio Express or Microsoft SQL Server 2005 Express Toolkit, distribute it with either:
        - Microsoft SQL Server 2005 Express Edition or
        - Microsoft SQL Server 2005 Express Edition with Advanced Services.
    - iii.** Distribution Restrictions. You may not
      - alter any copyright, trademark or patent notice in the Distributable Code;
      - use Microsoft's trademarks in your programs' names or in a way that suggests your programs come from or are endorsed by Microsoft;
      - distribute Distributable Code to run on a platform other than the Windows platform;
      - include Distributable Code in malicious, deceptive or unlawful programs; or
      - modify or distribute the source code of any Distributable Code so that any part of it becomes subject to an Excluded License. An Excluded License is one that requires, as a condition of use, modification or distribution, that
        - the code be disclosed or distributed in source code form; or
        - others have the right to modify it.
3. INTERNET-BASED SERVICES. Microsoft provides Internet-based services with the software. It may change or cancel them at any time.

4. SCOPE OF LICENSE. The software is licensed, not sold. This agreement only gives you some rights to use the software. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. You may not
  - disclose the results of any benchmark tests of the software to any third party without Microsoft's prior written approval;
  - work around any technical limitations in the software;
  - reverse engineer, decompile or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;
  - make more copies of the software than specified in this agreement or allowed by applicable law, despite this limitation;
  - publish the software for others to copy; or
  - rent, lease or lend the software.
5. BACKUP COPY. You may make one backup copy of the software. You may use it only to reinstall the software.
6. DOCUMENTATION. Any person that has valid access to your computer or internal network may copy and use the documentation for your internal, reference purposes.
7. TRANSFER TO A THIRD PARTY. The first user of the software may transfer it and this agreement directly to a third party. Before the transfer, that party must agree that this agreement applies to the transfer and use of the software. The first user must uninstall the software before transferring it separately from the device. The first user may not retain any copies.
8. EXPORT RESTRICTIONS. The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users and end use. For additional information, see [www.microsoft.com/exporting](http://www.microsoft.com/exporting).
9. SUPPORT SERVICES. Because this software is "as is," we may not provide support services for it.

**MICROSOFT SOFTWARE LICENSE TERMS**

10. ENTIRE AGREEMENT. This agreement, and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the software and support services.
11. APPLICABLE LAW.
  - a. United States. If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.
  - b. Outside the United States. If you acquired the software in any other country, the laws of that country apply.
12. LEGAL EFFECT. This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.
13. DISCLAIMER OF WARRANTY. THE SOFTWARE IS LICENSED "AS-IS." YOU BEAR THE RISK OF USING IT. MICROSOFT GIVES NO EXPRESS WARRANTIES, GUARANTEES OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT EXCLUDES THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.
14. LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. \$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.

This limitation applies to

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

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

# .Net Framework 2.0

## End-User License Agreement

### MICROSOFT SOFTWARE SUPPLEMENTAL LICENSE TERMS

#### MICROSOFT .NET FRAMEWORK 2.0

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

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

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

1. SUPPORT SERVICES FOR SUPPLEMENT. Microsoft provides support services for this supplement as described at [www.support.microsoft.com/common/international.aspx](http://www.support.microsoft.com/common/international.aspx).
2. MICROSOFT .NET FRAMEWORK BENCHMARK TESTING. This supplement includes the .NET Framework component of the Windows operating systems ("NET Component"). You may conduct internal benchmark testing of the .NET Component. You may disclose the results of any benchmark test of the .NET Component, provided that you comply with the following terms: (1) you must disclose all the information necessary for replication of the tests, including complete and accurate details of your benchmark testing methodology, the test scripts/cases, tuning parameters applied, hardware and software platforms tested, the name and version number of any third party testing tool used to conduct the testing, and complete source code for the benchmark suite/harness that is developed by or for you and used to test both the .NET Component and the competing

implementation(s); (2) you must disclose the date (s) that you conducted the benchmark tests, along with specific version information for all Microsoft software products tested, including the .NET Component; (3) your benchmark testing was performed using all performance tuning and best practice guidance set forth in the product documentation and/or on Microsoft's support web sites, and uses the latest updates, patches and fixes available for the .NET Component and the relevant Microsoft operating system; (4) it shall be sufficient if you make the disclosures provided for above at a publicly available location such as a website, so long as every public disclosure of the results of your benchmark test expressly identifies the public site containing all required disclosures; and (5) nothing in this provision shall be deemed to waive any other right that you may have to conduct benchmark testing. The foregoing obligations shall not apply to your disclosure of the results of any customized benchmark test of the .NET Component, whereby such disclosure is made under confidentiality in conjunction with a bid request by a prospective customer, such customer's application(s) are specifically tested and the results are only disclosed to such specific customer. Notwithstanding any other agreement you may have with Microsoft, if you disclose such benchmark test results, Microsoft shall have the right to disclose the results of benchmark tests it conducts of your products that compete with the .NET Component, provided it complies with the same conditions above.

## MarshallSoft Computing SMTP/POP3 Email Engine

### License for Use and Distribution

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

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

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

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

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

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

[END]

## Jasper Reports V1.2.0 and JFreeChart V1.0.5

**jTDS version 1.2**

**JFreeChart version 1.0.5**

**GNU LESSER GENERAL PUBLIC LICENSE**

Version 2.1, February 1999

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

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

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

### Preamble

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

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we

suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

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

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

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

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

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

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

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

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

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

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

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

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

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

## GNU LESSER GENERAL PUBLIC LICENSE

### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

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

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

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

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

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

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

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

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

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

- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

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

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

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

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

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

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

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

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

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

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

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

Section 6 states terms for distribution of such executables.

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

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

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

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

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

- a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
- b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.
- c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

- e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

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

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

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

- a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

- b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

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

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

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

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

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

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

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

#### NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

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

LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

#### END OF TERMS AND CONDITIONS

#### How to Apply These Terms to Your New Libraries

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

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

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

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

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

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

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

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

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

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

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice  
That's all there is to it!

## iText version 1.3.1

### MOZILLA PUBLIC LICENSE Version 1.1

#### 1. Definitions.

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

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

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

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

1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable" means Covered Code in any form other than Source Code.

1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License" means this document.

1.8.1. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

- A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.
- B. Any new file that contains any part of the Original Code or previous Modifications.

1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

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

## 2. Source Code License.

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

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

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

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

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

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

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

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

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

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

### 3. Distribution Obligations.

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

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

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

### 3.4. Intellectual Property Matters

(a) Third Party Claims. If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in

Section 3.2, Contributor shall promptly modify the **LEGAL** file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

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

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

**3.5. Required Notices.** You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

**3.6. Distribution of Executable Versions.** You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under

a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

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

#### 4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the **LEGAL** file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

#### 5. Application of this License.

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

#### 6. Versions of the License.

##### 6.1. New Versions.

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

##### 6.2. Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any

subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

### 6.3. Derivative Works.

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

## 7. DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS, MERCHANTABILITY, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

## 8. TERMINATION.

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

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

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

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

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

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

## 9. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY

PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

#### 10. U.S. GOVERNMENT END USERS.

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

#### 11. MISCELLANEOUS.

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

#### 12. RESPONSIBILITY FOR CLAIMS.

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

### 13. MULTIPLE-LICENSED CODE.

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

#### EXHIBIT A -Mozilla Public License.

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

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

The Original Code is \_\_\_\_\_.

The Initial Developer of the Original Code is \_\_\_\_\_.

Portions created by \_\_\_\_\_ are Copyright (C) \_\_\_\_\_  
\_\_\_\_\_. All Rights Reserved.

Contributor(s): \_\_\_\_\_.

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

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

# Java Runtime Environment JRE 1.5.0.06

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

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

1. DEFINITIONS. "Software" means the identified above in binary form, any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Sun, and any user manuals, programming guides and other documentation provided to you by Sun under this Agreement. "Programs" mean Java applets and applications intended to run on the Java Platform, Standard Edition (Java SE) on Java-enabled general purpose desktop computers and servers.

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

3. RESTRICTIONS. Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that Licensed Software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun Microsystems, Inc. disclaims any express or implied warranty of fitness for such uses. No right, title

or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.

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

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

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

**7. TERMINATION.** This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Either party may terminate this

Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon Termination, you must destroy all copies of Software.

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

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

10. U.S. GOVERNMENT RESTRICTED RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government primecontractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

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

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

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

## SUPPLEMENTAL LICENSE TERMS

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

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

B. License to Distribute Software. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README file, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software, (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

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

**The GNU General Public License (GPL)**

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

E. Third Party Code. Additional copyright notices and license terms applicable to portions of the Software are set forth in the

THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions in paragraphs 5 and 6 of the Binary Code License Agreement shall apply to all Software in this distribution.

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

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

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

## The GNU General Public License (GPL)

The source code needed to build our Clam AntiVirus components is provided with the CSA MC kit. These Clam AntiVirus components are **csaclamutil**, which was developed by Cisco to scan files, and its supporting libraries: **ClamAV** and **GMP**. The source code is stored in the \OpenSource directory in the sources.zip file.

### Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.  
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

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

## Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

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

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

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

## TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

**0.** This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

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

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

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

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

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

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

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

**3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:**

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

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

**4.** You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

**5.** You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

**6.** Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

**7.** If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

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

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

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

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

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

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of

any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

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

### **NO WARRANTY**

**11.** BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

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

END OF TERMS AND CONDITIONS

**How to Apply These Terms to Your New Programs**

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

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

One line to give the program's name and a brief idea of what it does.

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

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

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 A PARTICULAR PURPOSE. See the GNU General Public License for more details.

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

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

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

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

Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.

**The GNU General Public License (GPL)**

signature of Ty Coon, 1 April 1989  
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.



# INDEX

---

## Symbols

.Net Framework 2.0 license acknowledgement [C-19](#)  
@blacklist [7-4](#)  
@CD [2-46](#)  
@credit\_card [16-10](#)  
@csanode [5-34](#)  
@datascan [16-9](#)  
@desktop [2-47](#)  
@desktopdirectory [2-47](#)  
@dynamci [2-45](#)  
@dynamic [2-52, 6-27, 7-10, 9-14, 9-19, 15-21, 15-26](#)  
@external [2-46](#)  
@fixed [2-43, 6-55, 6-88](#)  
@floppy [2-46](#)  
@greylist [7-4](#)  
@highrisk\_signatures [6-20, 14-4, 14-7](#)  
@local [6-31](#)  
@mydocuments [2-47](#)  
@network [6-55, 6-88](#)  
@program\_files [2-47](#)  
@recent [2-52](#)  
@reg [2-45, 2-52, 2-54](#)  
@remote [2-53](#)

@removable [2-46, 6-55, 6-88](#)  
@safemode [6-56](#)  
@signatures [6-20, 14-4, 14-7](#)  
@smb-null-session [2-54](#)  
@ssn [16-10](#)  
@startmenu [2-47](#)  
@startup [2-47](#)  
@subnet [2-53](#)  
@system [2-45](#)  
@virusscan [15-8, 15-27](#)  
@whitelist [7-4](#)  
@windows [2-45](#)

---

## A

ActiveX  
    preventing download [6-74](#)  
Address set syntax [2-50](#)  
Add to application class [5-18](#)  
Administrator [2-21](#)  
    LDAP authentication [2-21](#)  
    manage login sessions [2-20](#)  
    role-based access [2-19](#)  
    role-based administration [2-14](#)  
    roles [2-14](#)

- set/change password [2-18](#)
- webmgr utility [12-10](#)
- Agent
  - architecture [1-6](#)
  - kits [3-12](#)
  - scripted silent installs [3-26](#)
- Agent (Linux)
  - commands [A-37](#)
  - csasctl utility [A-37](#)
  - installing [A-39](#)
  - uninstalling [A-40](#)
- Agent (Solaris)
  - commands [A-37](#)
  - csasctl utility [A-37](#)
  - installing [A-35](#)
  - uninstalling [A-36](#)
- Agent (UNIX)
  - check status [A-37](#)
  - polling [A-37](#)
  - re-enable logging [A-37](#)
  - software update [A-37](#)
- Agent (Windows)
  - interaction with Windows firewall [A-33](#)
  - interaction with Windows Security Center [A-34](#)
- Agent kit
  - preconfigured sample [4-8](#)
- Agent kits
  - Linux installation [A-39](#)
  - preconfigured sample [3-4](#)
- quiet install [3-15](#)
- reboot vs. no reboot [3-24](#)
- Solaris installation [A-35](#)
- status [3-21](#)
- Agent registration [3-26](#)
- Registration control [3-25](#)
- Agent reset
  - effect on quarantined files [15-10](#)
- Agent service
  - stop and start [A-31](#)
- Agent service control [6-3](#)
- Agent UI [A-8, A-9](#)
  - AntiVirus Protection [A-17](#)
  - assigning sounds to events [A-29](#)
  - changing security level [A-12](#)
  - Contact Information [A-28](#)
  - Events [A-26](#)
  - File Protection [A-20](#)
  - installing software updates [A-11](#)
  - Personal Firewall [A-14](#)
  - poll for new configuration [A-11](#)
  - preventing network connections [A-13](#)
  - responding to queries [A-24](#)
  - Resume button [A-14](#)
  - shortcut menu [A-30](#)
  - Status [A-9](#)
  - Untrusted Applications [A-22](#)
  - User Query Responses [A-24](#)
- Agent UI control rule [6-6, A-8](#)

- Alert types
  - configuring **10-45**
  - log file, generate **10-50**
- Analysis overview **13-1**
- Analysis Reports **13-34**
- AntiVirus **15-1, 15-15**
  - @virusscan **15-8, 15-27**
  - AntiVirus Exemptions **7-5**
  - AntiVirus Summary report **11-10**
  - AntiVirus Update Detail report **11-9**
  - AV Full Scan Schedule field **15-13**
  - background scan **15-6**
  - behavior-based tagging **15-8**
  - Clam AntiVirus **15-2**
  - configuring behavior-based policy **15-27**
  - creating APCRs to scan files **15-21**
  - creating FACLS to scan files **15-18**
  - creating file sets for infected files **15-24**
  - creating rules and components **15-17**
  - delete quarantined files **15-28**
  - effect of agent reset **15-10**
  - effect of turning off agent **15-9**
  - enabling **15-3**
  - Exemptions **15-14**
  - exemptions **15-15**
  - forcing signature update **15-13**
  - host scan schedule **15-13**
  - on-demand scan **15-6**
  - overview **15-1**
  - quarantined files **15-9**
  - report ClamAV virus to Cisco **15-15**
  - reporting ClamAV false positives **15-16**
  - reports **11-9, 11-12, 11-13, 15-17**
  - restore a quarantined file **15-28**
  - Restored Infection Details report **11-11**
  - scanning for viruses **15-5**
  - scan on close **15-6**
  - scan on open **15-6**
  - scheduling background scan **15-11**
  - signature-based tagging **15-7**
  - signature updates **15-4**
  - start on demand virus scan **15-28**
  - Virus Infections Details **11-13**
  - Virus Infections report **11-12**
  - virus tags **15-5, 15-7**
  - AntiVirus Exemptions **15-14, 15-15**
    - creating with Wizard **15-14**
  - AntiVirus Summary report **11-10**
  - AntiVirus Update Detail report **11-9**
  - AntiVirus update report **11-9**
  - Apache license acknowledgement **C-5**
  - Application Behavior Investigation **10-33**
    - analysis process overview **13-26**
    - Behavior Analyses Reports **13-34**
    - Behavior Analysis **13-27**
    - Configure Behavior Analysis **13-29**
    - monitor event log **13-32**
    - Overview **13-26**

- Policy creation methodology **13-38**
- Policy enforcement **13-30**
- progress status **13-32**
- Application Behavior Reports
  - Overview **13-34**
- Application-builder rule **8-17**
- Application Classes **8-2, 8-8**
  - application-builder rule **8-17**
  - application class management **8-23**
  - built-ins **8-4**
  - creation from rule page **8-22**
  - double-click to view **8-23**
  - dynamic **8-12**
  - enable/disable for product **8-23**
- First Time Application Execute **8-5**
- Installation Applications **8-7**
- managing application classes **8-23**
- Network Applications **8-5**
- Processes created by Network Applications **8-5**
- Processes created by Servers (TCP and UDP) **8-6**
- Processes executing untrusted content **8-7**
- Processes monitoring the Keyboard **8-6**
- Processes performing a Print Screen **8-6**
- Processes requiring kernel only protection **8-7**
- Processes requiring OS stack execution protection **8-7**
- Processes with elevated privileges **8-6**
- Processes writing untrusted content **8-7**
- Recently created untrusted content **8-6**
- Remote clients **8-6**
- remove process **8-9, 8-15**
- Server (TCP based) **8-6**
- Server (UDP based) **8-6**
- shell scripts **8-3**
- static application classes **8-8**
- Suspected Virus Applications **8-7**
- System Process **8-6**
- Third Party Security Applications **8-8**
- Application class management **8-23**
- Application control **6-11**
  - creating rule to virus scan file **15-21**
- Application Deployment Investigation
  - Application Classes **13-8**
  - Data Management **13-11**
  - Enable options **13-5**
  - Group Settings **13-4**
  - investigation process overview **13-3**
  - Product Associations **13-7**
  - Unknown Applications **13-10**
- Application Deployment Reports
  - AntiVirus Installations **13-13**
  - Installed Products **13-14**
  - Network Data Flows **13-21**
  - Network Server Applications **13-23**
  - Product Usage **13-19**
  - Unprotected Hosts **13-16**
  - Unprotected Products **13-18**

- Application Trust Levels  
 setting by Event Management Wizard **7-3**  
 setting by hand **7-2**
- Application trust levels **7-2**
- Are you there?, VPN client **17-2**
- Attack Details pop-up window **14-14**
- Attributes matching, file sets UNIX **9-14**
- Audit Mode **5-44**  
 details **5-44**  
 group **3-6**  
 rule module **5-5**
- Audit trail **2-32**
- Auto-enrollment **3-3, 4-7**
- Automatic signature generation **14-1, 14-3**  
 @highrisk\_signatures **14-7**  
 @signatures **14-7**  
 compared to signature-based antivirus protection **14-8, 15-10**  
 confidence level **14-6**  
 correlating LPC signatures **7-14, 14-11**  
 correlating MSRPC signatures **7-13, 14-10**  
 created signatures report **11-21**  
 denial of service attack report **11-19**  
 denial of service detail **11-19**  
 deploying **14-18**  
 expiring signatures **14-7**  
 filtering detail **11-20**  
 for offline agents **14-8**  
 generation detail **11-21**  
 global signature detail **14-13**
- managing global signatures **14-11, 14-15**  
 managing local signatures **14-17**  
 permanent signatures **14-7**  
 refining signatures **14-7**  
 reports **11-19, 14-18**  
 signature enforcement report **11-20**  
 signature tags **14-7**  
 stack recovery **14-5**  
 using the Wizard to remove **14-23**  
 using wizard to create exceptions **14-20**
- Available button  
 agent **A-11**
- Available software updates **3-54**
- AV full scan schedule **3-31**
- 
- B**
- background DLP scan  
 scheduling **16-16**
- background virus scan **15-6**  
 scheduling **15-11**
- Backing up configurations **12-3**  
 differential backup **12-4**  
 full backup **12-4**
- Behavior Analysis  
 import policy **13-33**  
 start analysis **13-33**
- Behavior Investigation  
 Behavior analysis process **13-26**

- BIOS supported boot detection [3-32](#)
- Black List [7-2, 7-4](#)
- @blacklist [7-4](#)
  - identifying members of [7-4](#)
- BootExecute [9-39](#)
- broadcast messages [6-32](#)
- Browser requirements [2-3](#)
- Buffer Overflow rule [6-78](#)
- Windows [6-75](#)
- Built-in Application Classes [8-4](#)
- Bulk transferring hosts [3-45, 3-46](#)
- C**
- Caching query responses [5-43](#)
- CD ROM drives [2-46](#)
- CGIC License acknowledgement [C-14](#)
- Cisco Intrusion Prevention System integration [17-2](#)
- Cisco IPS integration [17-2](#)
- Cisco Security Agent [A-1](#)
- agent diagnostics [A-29](#)
  - common error codes [A-34](#)
  - downloading and installing [A-2](#)
  - resetting agent [A-30](#)
  - shortcut menu [A-30](#)
  - uninstalling from Windows [A-33](#)
  - user interface [A-8](#)
- Cisco Trust Agent (CTA) [3-31, 9-41](#)
- host posture status [3-31](#)
- plugin [12-22](#)
- software update [3-58](#)
- Cisco VPN client support [17-2](#)
- Clam AntiVirus [15-2](#)
- reports [11-9](#)
  - signature updates [15-4](#)
- Classifying applications [7-3](#)
- Clear Pending Alerts [10-46](#)
- Clipboard access control [6-42](#)
- CMU-SNMP Libraries license acknowledgement [C-12](#)
- COM Component Access Control rule [6-45](#)
- COM Component Sets [9-4](#)
- extract utility [12-11](#)
- Compare configurations [2-35, 5-10](#)
- Compare policies [5-10](#)
- Confidence Ratings [7-10](#)
- configuration manager [B-2](#)
- Configuration shortcuts [2-37](#)
- Configuration view [2-33](#)
- Connection Rate Limit [6-15](#)
- Consistency check [5-14](#)
- Contact information
- agent [3-30](#)
- Copy rules [5-9](#)
- creating AV exemption [15-15](#)
- CSAAPI [18-2](#)
- csactl Utility (UNIX agents) [A-37](#)
- CSA MC
- logging in [2-4](#)

- csanode **5-33**
- CTA
- software update **3-58**
- current application Virus Classification attribute **5-26**
- 
- D**
- Data access control **6-19**
- Database Maintenance **12-8**
  - Event full-text search **12-8**
  - shrink database **12-8**
- Database restoring log **12-7**
- Data Discovery report **11-15**
- Data filter installation, required for data access control rule **12-11**
- Data Justification Details report **11-16**
- Data Loss Prevention **16-3**
  - applying scanning data tags **16-19**
  - applying static data tags **16-22**
  - built-in scanning data tags **16-11**
  - cloning scanning data tags **16-13**
  - creating Data Discovery reports **11-15**
- Data Discovery report **11-14**
  - deleting scanning data tags **16-14**
  - editing scanning data tags **16-12**
  - enabling **16-3**
  - group DLP scan schedule **16-18**
  - host DLP scan schedule **16-18**
  - managing data tags **16-9**
- on-demand scan **15-12, 16-17**
- Protected Data Movement report **11-17**
- reports **11-14, 16-19**
- scanning data tags **16-4**
- scanning data tag search patterns **16-5**
- scanning methods **16-16**
- scheduling background scan **16-16**
- static data tags **16-4, 16-14**
- Data Payload attribute **5-28**
- Data Sets **9-7**
- Denial of service, protection against **14-2, 14-4**
- Deployment Overview **1-4**
- Detailed descriptions **4-3**
- Detailed status and diagnostics **3-32**
- Details link **10-3**
- detected boot **5-31**
- detected rootkit **5-32**
- Diagnostics **3-32**
- Directory protection **2-48, 6-25, 15-20, 16-21, 16-25**
- Disable
- application class **8-23**
  - policy rule enforcement **10-33, 13-30**
  - rule **5-7**
- Discovery of other CSA nodes Enabled, Disabled **5-33**
- Disk space
- shrink your database files **12-8**
- Display only in Show All mode **9-8**
  - checkbox **9-3**

Distributed configuration software  
updates **3-60**

DL full scan schedule **3-32**

**E**

Enable rule **5-7**

Ephemeral ports

using **2-53**

ephemeral ports **9-26**

Error codes

common Windows agent error codes **A-34**

Ethereal software **10-3, 10-14**

Event Analysis **10-15**

Event code **6-58**

Event ID **6-58**

Event log **10-2**

packet details **10-14**

Event logging exception wizard **10-28**

Event Management Wizard **10-23**

about **10-23**

Advanced Mode use **10-24**

Analyze Application **10-33**

application analysis **10-23**

behavior analysis **10-33**

behavior analysis investigation **10-23**

Classify an application **10-23**

Classifying applications **7-3**

copying exceptions **10-32**

creating "allow" exception **10-25**

creating AV exemption **15-14**

Creating exceptions **10-23**

creating logging exception **10-28**

deleting exceptions **10-32**

disabling exceptions **10-32**

editing exceptions **10-31**

enabling exceptions **10-32**

event suppression filter **10-36**

moving exceptions **10-32**

purging similar events **10-23, 10-38**

rule module for exceptions **10-24**

setting trust levels **7-3**

Simple Mode use **10-24**

suppressing events **10-23**

suppressing similar events **10-36**

Event Monitor **10-14**

Events **10-2, 10-13, 10-14**

aggregation and suppression **10-9**

auto-pruning **10-18**

details **10-13**

event insertion tasks **10-18**

event log **10-2**

event log change filter **10-7**

event log start and end dates **10-7**

event managing tasks **10-17**

Event Monitor **10-14**

Event Sets **10-39**

event suppression filter **10-36**

filter out similar events **10-8**

- find similar **10-3**
  - log filter out similar events **10-5**
  - log filter text **10-5**
  - managing **10-17**
  - minimum and maximum severity **10-7**
  - minimum severity **10-7**
  - packet details **10-3, 10-14**
  - reading details **10-13**
  - reading logs **10-13**
  - reading packet details **10-14**
  - rule number link **10-3**
  - searching details with Google **10-13**
  - Status Summary **2-27**
  - System State link **10-4**
  - third party access **10-43**
  - Events by Group reports **11-5**
  - Events by Severity reports **11-3**
  - Event Sets **10-39**
    - Purge events **10-41**
    - View button **10-41**
  - Event suppression filter **10-36**
  - Exception rule wizard **10-24**
  - Exceptions **10-30**
    - configuring **10-30**
    - copying **10-32**
    - deleting **10-32**
    - disabling **10-32**
    - editing **10-31**
    - enabling **10-32**
  - Exception page **10-30**
  - moving **10-32**
  - Expanded views **2-16**
  - expiring signatures **14-7**
  - Explain rules link **5-13**
  - Export configurations **12-17**
  - extract\_com **12-11**
- 
- F**
  - File access control **6-23**
    - creating rules to virus scan files **15-18**
  - file interceptor **B-5**
  - File Sets **9-12**
    - to indicate infected files **15-24**
    - using @virusscan **15-27**
  - file trusted, untrusted **5-35**
  - File version control **6-49**
  - Filter user info from events **3-7**
  - Find database items **2-39**
  - Find Similar **10-3**
  - Firefox
    - version support **2-3**
  - First Time Application Execute **8-5**
  - floppy drives **2-43, 2-46**
  - Force reboot after install **3-14, 3-57**
  - forcing virus signature update **15-13**
  - full text search **12-8**
  - database **12-8**

---

## G

Generating Rules **5-16**

  Details link **5-16**

  fails due to polling interval **5-16**

  pending changes **2-34**

Global Event Correlation **7-7**

global event manager **B-2**

Global Settings

  AntiVirus Exemptions **7-5, 15-14**

  Global Event Correlation **7-7**

  Scanning data tags **7-15**

  scanning data tags **16-5**

  static data tags **7-15**

Global Signature Management page **14-11**

global signatures

  managing **14-9, 14-11**

  viewing details **14-13**

GNU General Public License **C-46**

Google **10-13, 14-14**

Google searches of details **10-13**

Grey List **7-2, 7-4**

  @greylist **7-4**

  identifying members of **7-4**

Groups

  about **3-2**

  adding or removing hosts from **3-45**

  attaching policies to **4-12**

Audit mode **3-6**

bulk transferring hosts between **3-45**

configure **3-4**

DLP scan schedule **16-18**

Filter user info from events **3-7**

Learn mode **3-7**

Log overrides **3-7**

mandatory enrollment in **3-3**

membership **3-36**

modifying group membership **3-30**

modifying host memberships in **3-44, 3-48**

Polling interval **3-6**

preconfigured sample **3-4**

reset agents **3-10**

Rule overrides **3-6**

search for hosts and change group membership **3-48**

Send polling hint **3-6**

Verbose logging mode **3-7**

GUID (Globally Unique Identifier) **14-14**

---

## H

Hard link protection

  file access control **6-26**

Help

  online **2-12**

Host address untrusted **5-35**

Host details **3-28**

  Application Deployment **3-35**

  audit mode **3-35**



- contact information **3-30**
- diagnostics **3-32**
- events in past 24 hours **3-31**
- filter user info from events **3-35**
- group membership **3-36**
- host description **3-30**
- host identification **3-30**
- host name **3-30**
- host settings **3-34**
- host status **3-31**
- last Application Deployment data upload **3-32**
- last known IP address **3-30**
- log deny actions **3-35**
- policies **3-36**
- policy inheritance **3-36**
- policy version **3-31**
- polling interval **3-34**
- product information **3-30**
- rules **3-36**
- send polling hint **3-35**
- software version **3-31**
- time since last poll **3-31**
- UID **3-31**
- verbose logging mode **3-35**
- view related events **3-30**
- Host groups **3-2**
- Host history collection **2-28**
- Host identification
  - registration time **3-31**
- Host Managing Tasks **3-51**
- Hosts **3-38, 3-42**
  - about **3-4**
  - active hosts **3-42**
  - add or remove from group **3-44**
  - bulk transferring between groups **3-45**
  - changing groups **3-43**
  - copy from one group to another **3-46**
  - deleting **3-38**
  - diagnose **3-32**
  - DLP scan schedule **16-18**
  - group membership **3-36**
  - history **2-28, 3-34**
  - inactive hosts **3-42**
  - managing tasks **3-51**
  - migrated hosts in recycling bin **3-39**
  - modify group membership **3-43, 3-48**
  - modifying group membership **3-45**
  - moved hosts in recycle bin **3-38**
  - move from one group to another **3-46**
  - moving to recycle bin **3-41**
  - moving to recycling bin **3-40**
  - policy inheritance **3-36**
  - posture status **3-31**
  - purging hosts from CSA MC **3-42**
  - recycle bin **3-38**
  - reset **3-34**
  - search for and add to group **3-48**
  - search for and change group membership **3-48**

- search for and delete [3-48](#)
- searching for [3-36](#)
- unprotected [3-37](#)
- unsupported platforms [3-37](#)
- upload diagnostics [3-32](#)
- viewing details [3-28](#)
- viewing hosts managed by CSA MC [3-27](#)
- viewing host statuses [3-27](#)
- view relevant event log [3-30](#)
- view status [3-26](#)
- host scanning tasks [15-11, 16-16](#)
  - background DLP scanning [16-16](#)
  - data loss prevention [16-16](#)
  - on-demand DLP task [15-12, 16-17](#)
- Host settings [3-34](#)
- Host Status [3-31](#)
  - Active [3-27](#)
  - Audit Mode [3-28](#)
  - Last Poll [3-28](#)
  - Latest Software [3-28](#)
  - Protected [3-28](#)
- HTTPS [A-6](#)
- ICMP information message [6-38](#)
- ICMP ping message [6-38](#)
- ID
  - rule [5-8](#)
- IIS installation
- Windows Vista [12-12](#)
- Import configurations [12-17](#)
  - delete [12-21](#)
- Import history [12-21](#)
- Insecure boot detected [3-32](#)
- Insecure boot detection [6-55, 6-87](#)
- Install
  - agent [A-2](#)
- Installation Applications [8-7](#)
- Insufficient disk space event [12-8](#)
- interceptors [B-5](#)
  - file [B-5](#)
  - network application [B-5](#)
  - network traffic [B-5](#)
  - registry [B-5](#)
- Interface characteristics [9-21](#)
  - Bluetooth [9-23](#)
  - IEEE1394 [9-23](#)
  - Loopback [9-23](#)
  - PPP [9-22](#)
  - Virtual [9-22](#)
  - WiFi [9-22](#)
  - Wired [9-22](#)
- Internet Explorer
  - version requirements [2-3](#)
- Intrinsic security [1-1](#)
- Invalid TCP/UDP/ICMP header [6-36](#)
- IPS

integration with CSA MC **17-2**  
 IP security checks **6-35**  
 IPv6 addresses **2-53, 9-19**  
 IPv6 packets on platforms without IPv6 support **6-36**  
 iText version 1.3.1 license acknowledgement **C-32**

---

**J**

Jasper Reports version 1.2.0 license acknowledgement **C-21**  
 Java Runtime Environment JRE 1.5.0.06 license acknowledgement **C-42**  
 JFreeChart, version 1.0.5 license acknowledgement **C-21**

---

**K**

Kernel Protection **6-53**  
 Keystroke trapping  
     kernel level **6-56**  
     preventing **6-73**

---

**L**

Last update time **3-31**  
 LDAP authentication for administrators **2-21**  
 Learn Mode **5-48**  
     automatic 72 hour learning **5-6**  
     details **5-48**

first time execute **5-49**  
 group **3-7**  
 rule module **5-6**  
 unusual system calls **5-49**  
 Learn mode **3-28**  
 libpcap license acknowledgement **C-11**  
 Lifecycle of an attack **1-2**  
 Listener option in NACL **6-32**  
 local event manager **B-5**  
 Localized directory paths **2-47**  
 local signatures  
     managing **14-9, 14-17**  
 Location based states  
     Remote VPN clients **9-44**  
 Log deny actions **3-7**  
 Logging **10-21**

    suppression of log messages **10-21**  
     verbose logging mode **3-35**  
 Logging agent **13-27**  
 Logging modes  
     verbose **5-45**  
 Log overrides **3-7**  
 Log set actions **3-7**  
 LPC (Local Procedure Call) interfaces, protection of **14-5**

LPC interface  
     defending against denial of service attacks **7-14, 14-11**  
     protection of **14-1**

---

## M

Maintenance

    Available Software Updates **3-54**

    Event Managing Tasks **10-17**

Make kit button **3-15**

Manage

    application classes **8-23**

    dynamically quarantined files **7-10**

    dynamically quarantined IP addresses **7-10**

Mandatory group enrollment **3-3**

Manual data filter installation **12-11**

    Linux **12-14**

    Solaris **12-16**

    Window **12-13**

MARS appliance

    integration **17-3**

MarshallSoft Computing SMTP/POP3 Email Engine license acknowledgement **C-20**

Media device monitoring **6-74**

Media type syntax **2-46**

Menu bar **2-10**

Merge

    analysis products **13-9**

    configurations **2-35, 5-12**

    rule modules **5-12**

MICROSOFT SOFTWARE LICENSE TERMS **C-15**

minimum severity **10-7**

Modify agent configuration

self-protection **6-5**

Modifying group membership **3-43**

Modifying host membership **3-44, 3-45**

Monitor Action **5-24**

Move hosts to Recycle Bin **3-42**

MSRPC (Microsoft Remote Procedure Call) interfaces, protection of **14-5**

MSRPC interface

    defending against denial of service attacks **7-13, 14-10**

    protection of **14-1**

multicast packet signals **6-32, 10-21**

Multiple MC software update **3-60**

---

## N

Navigation shortcuts

    insert link **2-37**

    new application class link **2-37**

    variables **2-14**

    View references **2-36**

netForensics

    integration **17-3**

net start command **12-2, A-32**

net stop command **12-2, 12-10, A-32**

Network access control **6-29**

Network Address Sets **9-18**

Network Admission Control **9-41**

network application interceptor **B-5**

Network Applications **8-5**

Network interface control **6-81**  
 Network Interface Sets **9-21**  
 Network interface state **9-41**  
 Network service ephemeral ports **2-53**  
 Network Services **9-24**  
 Network service syntax **2-53**  
 Network shield **6-34**  
   detect port scans **6-37**  
   ICMP covert channels **6-38**  
   ICMP information/configuration **6-38**  
   invalid IP addresses **6-35**  
   invalid IP headers **6-35**  
   malicious packets **6-39**  
   prevent SYN floods **6-36**  
   randomize TCP sequence numbers **6-37**  
   source routed packet **6-36**  
   TCP blind session spoofing **6-37**  
   trace route **6-36**  
   unrestricted network connectivity during boot **6-39**  
 network traffic interceptor **B-5**  
 Notification settings **9-27**  
   syntax **9-32**  
   use of tokens **9-32**  
 Notify User action **5-24**  
 NT Event log **6-57**

---

**O**

on-demand virus scan **15-6**

Open Market FastCGI license acknowledgement **C-13**  
 OpenSSL - Open SSL Project **C-2**  
 Operating system changes, agent **A-4**

---

**P**

Packet details **10-14**  
 packet sniffers **6-69, 6-81**  
 Peers  
   groups **13-22**  
   hosts **13-22**  
   network address sets **13-22**  
 Peripherals **2-43, 2-46**  
 Perl license acknowledgement **C-10**  
 permanent signatures **14-7**  
 Policies  
   agent UI control **6-6**  
   application control **6-11**  
   applying **4-11, 4-12, 5-14**  
   attaching rule modules to **4-11, 5-14**  
   buffer overflow **6-78**  
   buffer overflow protection **6-78**  
   building **4-8**  
   clipboard access control **6-42**  
   combining **4-6**  
   com component access control **6-45**  
   compare, copy, merge **5-10**  
   file access control **6-15, 6-19, 6-23, 6-45, 6-61**  
   file version control **6-49**

- generate rules **5-16**
  - network access control **6-29**
  - network interface control **6-81**
  - network shield **6-34**
  - NT event log **6-57**
  - port scan detection **6-37**
  - preparing a security policy **4-2**
  - printer access control **6-59**
  - registry access control **6-61**
  - resource access control **6-84**
  - rootkit /kernel protection **6-86**
  - service restart **6-67**
  - sniffer and protocol detection **6-69**
  - SYN flood protection **6-36**
  - Syslog control **6-90**
  - system API control **6-71**
  - Policy enforcement **10-33, 13-30**
  - Policy inheritance **3-36**
  - polling **1-9**
    - for software updates **A-11**
    - interval **3-6**
    - polling hint message **3-6**
  - Port scan detection **6-37**
  - Printer access control **6-59**
  - Processes created by Network Applications **8-5**
  - Processes created by Servers (TCP and UDP) **8-6**
  - Processes executing untrusted content **8-7**
  - Processes performing a Print Screen **6-44, 8-6**
  - Processes requiring kernel only protection **8-7**
  - Processes requiring OS stack execution protection **8-7**
  - Processes with elevated privileges **8-6**
  - Processes writing untrusted content **8-7**
  - Product data collection **13-5**
  - Products
    - configure associations **13-7**
  - promiscuous mode **6-83**
  - Protected Data Movement Report **11-17**
  - Purge events **10-41**
- 
- Q**
  - QoS **5-32**
    - marking **5-32**
  - Quarantined files **7-8, 15-7, 15-9**
  - Quarantined files and IP addresses **7-10**
  - Quarantined IP addresses **7-9**
  - Query responses
    - caching **5-43**
    - challenge user **5-42**
    - clear **5-43**
    - configure prompt text **9-28, 9-30**
    - Don't ask again **5-42, 5-43**
    - user justification **5-43**
  - Query settings **9-29**
    - syntax **9-32**
    - use of tokens **9-32**
  - Query User **5-39**
  - Quiet install **3-15, 3-57**

---

**R**

- Read-only items **2-16**  
     modify **2-16**
- Reboot operations **9-39**
- Reboot optional  
     agent **A-6**
- Reboot vs. no reboot for agents **3-24**
- Recently created untrusted content **8-6**
- Recycle bin **3-38**
- refining signatures **14-7**
- Registration control **3-25**
- Registry access control **6-61**
- registry interceptor **B-5**
- Registry sets  
     BootExecute **9-39**  
     Reboot operations **9-39**  
     Run keys **9-38**  
     Shell commands **9-39**
- Remote access **2-4**
- Remote clients **8-6**
- Removable media **2-46**
- Remove process from application class **8-9, 8-15**
- Replace items, search **2-39**
- report generator **B-3**
- Reporting ClamAV false positives **15-16**
- Reports  
     AntiVirus reports **11-9**  
     AntiVirus Summary Report **11-10**
- AntiVirus Update **11-9**
- automatic signature generation **11-19**
- Clam AntiVirus **11-9**
- creating Data Discovery report **11-15**
- Data Discovery **11-14**
- Data Justification Details Report **11-16**
- Data Loss Prevention **11-14, 16-19**
- Events by Group **11-5**
- Events by Severity **11-3**
- Exporting **13-25**
- generating **11-3**
- Group Detail **11-8**
- Host Detail **11-6**
- Policy Detail **11-7**
- Protected Data Movement report **11-17**
- Restored Infection Details report **11-11**
- signatures **14-18**
- Unprotected Products **13-18**
- Virus Infections **11-12**
- virus infections **11-12**
- Virus Infections Details **11-13**
- Reports Data Discovery Details **11-14**
- Requirements  
     agent **A-3**
- Reset Cisco Security Agent **3-10, 14-17, 14-20**
- Reset to factory **A-8**
- Resource access control **6-84**
- responding to queries **A-24**
- Restored Infection Details report **11-11**

- Restoring configurations [12-6](#)
- Right-click menu shortcuts [2-33](#)
- Role-based administration [2-14](#)
- Rootkit / kernel protection [6-86](#)
- Rule ID [5-8](#)
- Rule Modules
- Add/Remove process [5-21](#)
  - adding rules [5-6](#)
  - configuring [5-4](#)
  - Monitor action [5-24](#)
  - Notify user [5-44](#)
  - Notify User action [5-24](#)
  - Query user [5-39](#)
  - Set action [5-25](#)
  - System state sets [9-40](#)
  - User state sets [9-46](#)
- Rule overrides [3-6, 5-5, 5-6](#)
- Rules
- about [5-3](#)
  - action definitions [5-19](#)
  - action options [5-18](#)
  - agent service control [6-3](#)
  - agent UI control [6-6](#)
  - application control [6-11](#)
  - buffer overflow [6-78](#)
  - clipboard access control [6-42](#)
  - com component access control [6-45](#)
  - compare, copy, merge [5-10](#)
  - connection rate limit [6-15](#)
  - consistency check [5-14](#)
  - copying rules between modules [5-9](#)
  - data access control [6-19](#)
  - enable/disable [5-7](#)
  - Events column [5-8](#)
  - explain link [5-13](#)
  - explain rules running on a host [3-30](#)
  - file access control [6-23](#)
  - file version control [6-49](#)
  - ID column [5-8](#)
  - kernel protection [6-53](#)
  - Logging options [5-22](#)
  - manipulating precedence [5-22](#)
  - network access control [6-29](#)
  - network interface control [6-81](#)
  - network shield [6-34](#)
  - NT event log [6-57](#)
  - port scan detection [6-37](#)
  - precedence, ordering [5-18](#)
  - printer access control [6-59](#)
  - registry access control [6-61](#)
  - resource access control [6-84](#)
  - rootkit / kernel protection [6-86](#)
  - service restart [6-67](#)
  - show enabled rules only checkbox [5-9](#)
  - sniffer and protocol detection [6-69](#)
  - SYN flood protection [6-36](#)
  - syslog control [6-90](#)
  - System API Control [6-71](#)

**S**

- View All rules **5-9**
- view change history **5-12**
- Run keys **9-38**

---

- S**
- Sample policies **10-39**
- Save configurations **2-35**
- scanning data tag
  - editing **16-12**
  - scanning data tags **7-15, 16-9, 16-11**
  - built-in scanning patterns **16-8**
  - built-in tags **16-11**
  - cloning **16-13**
  - creating **16-11**
  - creating FACLs that apply tags **16-19**
  - deleting **16-14**
  - descriptions **16-9**
  - pattern syntax **16-5**
  - search patterns **16-5**
  - text-matching patterns **16-6**
- Scheduled database backups **12-4**
- Scheduled software updates **3-56**
- Scripted agent installs and uninstalls **3-26**
- Scripting interface **18-2**
  - API summary **18-3**
  - change host groups **18-27**
  - encryption, authentication **18-8**
  - escape character **18-17**
- get even information **18-33**
- get host information **18-30**
- get overall system information **18-32**
- get reports **18-33**
- getting status **18-21**
- LIMIT construct **18-19**
- modifying system **18-24**
- object expressions **18-9**
- object type names **18-10**
- object types **18-10**
- README files **18-7**
- sample scripts **18-7**
- scripting language **18-6**
- testing **18-23**
- userid, password **18-8**
- wildcarding **18-17**
- WSDL, SOAP **18-5**
- Scripts, writing rules for **8-4**
- Search
  - host search **3-36**
  - how to use it **2-39**
  - open item in a new window **2-39**
  - replace **2-39**
- Security level **3-32, 5-36**
- Security policy **4-3**
  - preparing **1-8**
- Self-protection **5-18**
- Send polling hint **3-6, 3-35**
- Sensitive data scan **5-37**

- Server (TCP based) **8-6**
- Server (UDP based) **8-6**
- service, agent start/stop **12-3, A-32**
- Service restart **6-67**
- Set **5-25**
  - data payload Trusted, Untrusted **5-28**
  - detected access Protected, Unprotected **5-30**
  - detected boot **5-31**
  - detected rootkit **5-32**
  - Differentiated Service **5-32**
  - Discovery of other CSA nodes Disabled, Enabled **5-33**
  - file trusted, untrusted **5-35**
  - Host address untrusted **5-35**
  - Security level **5-36**
  - Sensitive Data Scan **5-37**
  - stack Recovery **5-36**
  - virus scan **5-37**
  - virus scan on close **5-38**
  - virus scan on open **5-39**
- Set action **5-25**
- set attribute
  - assigning behavior-based AV tags **5-26**
- Shell commands **9-39**
- Shell scripts, writing rules for **8-3**
- Show All mode **2-16, 9-8**
- show enabled rules only checkbox **5-9**
- SID **9-47**
- Signature-based antivirus protection
- compared to Automatic Signature Generation **14-8**
- compared to Automatic Signature Generation **15-10**
- Signatures **14-1**
  - confidence level **14-6**
  - deleting **14-15**
  - disabling **14-15**
  - enabling **14-15**
  - exporting **14-16**
  - importing **14-15**
  - make expiring **14-16**
  - make permanent **14-16**
  - removing **14-15**
  - reports **14-18**
  - setting confidence **14-16**
  - upgrading **14-17**
  - using the Wizard to remove **14-23**
  - using wizard to create exceptions **14-20**
- Signature settings page **14-9**
- Signature tag **14-7, 14-14**
- Silent agent install **3-26**
- similar events **10-36**
- Sniffer and protocol detection rule **6-69**
- SOAP **18-5**
- Socket6 license acknowledgement **C-10**
- Software updates **3-54**
  - Distributed configuration software updates **3-60**

- Force reboot **3-14, 3-57**
  - Quiet install **3-57**
  - Scheduled software updates **3-56**
  - Solaris agent install directory **A-36**
  - Solaris requirements
    - agent **A-5**
  - SQL Server database **B-3**
  - SSL **1-8**
  - Stack recovery **14-2, 14-5**
    - appropriate uses **14-5**
  - Stack recovery attribute **5-36**
  - Start agent service **12-3, A-32**
  - State conditions **9-40**
  - Static data tag **16-22**
  - Static data tags **7-15**
  - static data tags **16-14**
    - adding descriptions **16-15**
    - viewing references **16-15**
  - Status **A-9**
    - Event Log **10-2**
  - Status, agent kits **3-21**
  - Status Summary
    - colored chart **2-30**
    - Database Maintenance **2-30**
    - Event counts per day **2-30**
    - Host history collection **2-28**
    - Most active **2-30**
    - Network Status **2-28**
  - Stop agent service **12-3, A-32**
  - Stop and start agent security **A-31**
  - Stop logging button **13-30**
  - Suppressed events, always show **2-15**
  - Suspected Virus Applications **8-7**
  - Symbolic link protection
    - file access control **2-50, 6-26, 6-85**
    - general **6-85**
  - Syntax **2-41**
  - Syslog control **6-90**
  - System API Control **6-71**
  - System calls, unusual **6-76, 6-80**
  - System components **B-1**
  - System Process **8-6**
  - System Startup Security checks **6-39**
  - System state
    - insecure boot detected **9-43**
    - installation process detected **9-43**
    - management center reachable **9-42**
    - network interface **9-41**
    - security level **9-41**
    - system booting **9-43**
    - unprotected access detected **9-43**
    - untrusted rootkit detected **9-43**
    - virus detected **9-43**
  - System State sets **9-40**
  - Take precedence over other rules **5-22, 5-23**
- 

**T**

TCL license acknowledgement **C-9**

TCP Chimney Offload **6-39**

Terminal services **A-3**

Third party

    access to events **10-43**

Third Party Security Applications **8-8**

Timed audit mode **3-51**

Timed learn mode **3-51**

Time since last AV signature update **3-31**

Time since last AV signature update field **15-13**

Trace route, prevent **6-36**

Transport security checks **6-36**

Trusted payloads **14-6**

Turn agent off **A-31**

---

## U

UNICODE **16-7**

UNIX agent install directory **A-36**

Untrusted payloads **14-6**

Untrusted rootkit detected **3-32**

User State sets **9-46**

Utilities

    csactl (Solaris agent) **A-37**

    extract\_com **12-11**

    net stop/start **12-2**

---

## V

Variables

    COM Component Sets **9-4**

    Data Sets **9-7**

    Event Sets **10-39**

    File Sets **9-12**

    Network Address Sets **9-18**

    Network Interface Sets **9-21**

    Network Services **9-24**

    Notification Settings **9-27**

    Notification settings **9-32**

    Query Settings **9-29**

    Query settings **9-32**

    Registry Sets **9-35**

    using **9-2**

Verbose logging mode **3-35, 10-22**

View All rules

    filter rule display **5-9**

View change history **15-27**

View change history, rules **5-12**

View references **2-36**

Virus Infection Details report

    Reports

        virus Infection details **11-13**

Virus Infections report **11-12**

Vulnerable applications **4-20**

---

**W**

Webmgr Utility [12-10](#)

White List [7-2, 7-4](#)

    @whitelist [7-4](#)

    identifying membership [7-4](#)

Wikipedia [14-5](#)

Windows Firewall [A-33](#)

Windows requirements

    agent [A-3](#)

Windows Security Center [A-34](#)

WinPcap software [10-14](#)

Wireless, interface support [9-21, 9-41](#)

Wizard

    behavior analysis [10-28](#)

    events [10-23](#)

    exception rule [10-24](#)

    using to remove unwanted signatures [14-23](#)

WSDL [18-5](#)

