Programming Guide

NetIQ Security Manager™

October 2011

NetIQ Security Manager is protected by United States Patent No: 05829001.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, VPN-1, Provider-1, and SiteManager-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This product claims FIPS compliance by use of one or more of the Microsoft cryptographic components listed below. These components were certified by Microsoft and obtained FIPS certificates via the CMVP.

893 Windows Vista Enhanced Cryptographic Provider (RSAENH)

894 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

989 Windows XP Enhanced Cryptographic Provider (RSAENH)

990 Windows XP Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

997 Microsoft Windows XP Kernel Mode Cryptographic Module (FIPS.SYS)

1000 Microsoft Windows Vista Kernel Mode Security Support Provider Interface (ksecdd.sys)

1001 Microsoft Windows Vista Cryptographic Primitives Library (bcrypt.dll)

1002 Windows Vista Enhanced Cryptographic Provider (RSAENH)

1003 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

1006 Windows Server 2008 Code Integrity (ci.dll)

1007 Microsoft Windows Server 2008 Kernel Mode Security Support Provider Interface (ksecdd.sys)

1008 Microsoft Windows Server 2008

1009 Windows Server 2008 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

1010 Windows Server 2008 Enhanced Cryptographic Provider

1012 Windows Server 2003 Enhanced Cryptographic Provider (RSAENH)

This product may also claim FIPS compliance by use of one or more of the Open SSL cryptographic components listed below. These components were certified by the Open Source Software Institute and obtained the FIPS certificates as indicated.

918 - OpenSSL FIPS Object Module v1.1.2 - 02/29/2008 140-2 L1

1051 - OpenSSL FIPS Object Module v 1.2 - 11/17/2008 140-2 L1

1111 - OpenSSL FIPS Runtime Module v 1.2 - 4/03/2009 140-2 L1

Note: Windows FIPS algorithms used in this product may have only been tested when the FIPS mode bit was set. While the modules have valid certificates at the time of this product release, it is the user's responsibility to validate the current module status.

Contents

Chapter 2

Understanding the Development Console 23

Chapter 3

Understanding Alerts and Alert Configuration 33

Chapter 4
Understanding Computer Groups 43

Chapter 5

Understanding Processing Rule Groups 63

Chapter 6

Understanding Processing Rules 77

Appendix A
Providing Support for SNMP 157

Appendix B
Understanding WMI 167

About This Book and the Library

The programming guide provides conceptual information about the NetIQ Security Manager product (Security Manager), including rules and step-by-step guidance for rule customization tasks using the Development Console.

Intended Audience

This book provides conceptual information about Security Manager rules and step-by-step guidance for rule customization tasks using the Development Console.

Other Information in the Library

The library provides the following information resources:

Trial Guide

Provides general information about the product and guides you through the trial and evaluation process.

Installation Guide

Provides detailed planning and installation information.

User Guide

Provides conceptual information about Security Manager. This book also provides an overview of the Security Manager user interfaces and the Help.

Module Documentation

Provide information to help you configure specific products to monitor with Security Manager, such as Cisco IDS or Symantec Norton AntiVirus.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as descriptions of each field on each window.

Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	• Window and menu items • Technical terms, when introduced
Italics	• Book and CD-ROM titles • Variable names and values • Emphasized words
`Fixed Font`	• File and folder names • Commands and code examples • Text you must type • Text (output) displayed in the command-line interface
Brackets, such as [*`value`*]	• Optional parameters of a command
Braces, such as {*`value`*}	• Required parameters of a command
Logical OR, such as *`value1`*|*`value2`*	• Exclusive parameters. Choose one parameter.

About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measurable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

For questions about products, pricing, and capabilities, please contact your local partner. If you cannot contact your partner, please contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, please contact our Technical Support team.

Worldwide:	www.netiq.com/Support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, please visit http://community.netiq.com.

Chapter 1

Introduction

As IT environments become increasingly complex, it becomes more difficult and costly for IT professionals to meet important objectives such as:

- Mitigating risks from internal and external attacks
- Leveraging existing investments in security sensors
- Improving security knowledge, response, and reporting
- Complying with government regulations and audits

Security Manager allows you to meet these objectives by:

- Improving security knowledge through a comprehensive knowledge base that automatically builds, internalizing new and updated information into the product, and assuring the availability of that security knowledge. The Knowledge Base contains information supplied with Security Manager. You can also add and store your own security knowledge using the company knowledge base.
- Increasing protection levels by correlating events from your heterogeneous and best-of-breed security point solutions, systems and processes to identify true incidents.

- Boosting operational performance and improving the return on investment (ROI) by consolidating security information from across your organization into a central location, filtering out noise and false positives, and presenting the real, true incidents.
- Assuring compliance by capturing and securing event log data for auditing, daily analysis, and archival purposes.

What Is Security Manager?

Security Manager is an automated security information and event management (SIEM) solution that addresses the following security management challenges:

- Quickly identifying hidden threats while meeting audit, regulatory, and legal requirements with scalable and centralized log and event consolidation.
- Identifying real incidents with event correlation to reduce false positives and minimize event noise.
- Providing streamlined, customizable reporting to track both high-level enterprise-wide trends and possible security threats.

Security Manager uses modules to provide out-of-the-box support for a broad range of applications and platforms, including support for:

- Servers and workstations, including those using Windows, Linux, UNIX, and iSeries operating systems
- Critical services such as databases
- Security point solutions, including antivirus products, firewall products, and intrusion detection and protection systems
- Network devices, including routers and switches
- NetIQ solutions, including the NetIQ Secure Configuration Manager product (Secure Configuration Manager), the NetIQ AppManager product (AppManager), the NetIQ Change Guardian for Windows product (Change Guardian for Windows), and the NetIQ Change Guardian for Group Policy product (Change Guardian for Group Policy), among others

Modules are predefined solutions to configure Security Manager to monitor or collect log data for specific environments and applications. New and updated modules are delivered through the NetIQ AutoSync server.

Easy to install in simple environments but versatile enough to manage complex installations, Security Manager provides solutions in the following areas to help you meet your information and event management needs:

- Event management
- Log management

What Is Security Manager Event Management?

An **event** is a significant occurrence on a computer that requires user notification or a record added to a log. Every application, business service, and security product writes events to a log to record its status, but logs can be impossible to manually review and aggregate.

Security Manager's event management capability applies correlation rules and built-in security knowledge to present a clear picture of how your applications and security point products are performing. For more information about correlation, see "Event Correlation Data Flow" on page 15.

Security Manager improves your operational efficiency in the following ways:

- Identifies events important enough to command immediate attention and then generates an alert for the condition. An **alert** is a notification of a significant event.
- Reduces false positive alerts generated by poorly configured sensors.
- Minimizes event noise by consolidating repetitive messages into a single alert.

In real time, Security Manager monitors the following types of best-of-breed products and services:

- Security point solutions such as antivirus and firewall products
- Network devices such as routers and switches
- Critical services such as databases

To help manage events and alerts, Security Manager includes detailed security knowledge to help your staff understand and address issues as they arise. The Security Manager incident management workflow helps you track and audit alert status to ensure risks are quickly and successfully addressed.

These features are available in views and incident packages, which you can access in the Security Manager Control Center. A **view** is a window that displays and allows you to examine a group of items matching certain criteria. **Incident packages** are containers for information you can use to investigate and resolve an incident.

What Is Security Manager Log Management?

Many regulations require you to collect, store, and safeguard security log information. To meet audit requirements, you may have to research the archives to verify specific events and when they occurred.

Security Manager collects event information to provide a powerful solution for storing and analyzing event data from a secure, central database. Security Manager offers the following log management capabilities:

- Collects and archives log data from all your Security Manager sources.
- Stores the data for archive, backup, research, and reporting.
- Offers Forensic Analysis and Trend Analysis reports.

Security Manager funnels information from event sources throughout your enterprise to a log archive. A **log archive** is a folder used by Security Manager to securely store archived log data. Archived event and alert information is available for review in a centralized console.

With Security Manager, you can manage the entire lifecycle of events, from event collection to long-term trend analysis and archival.

Security Manager provides Forensic Analysis and Trend Analysis reports, safeguarding forensic evidence before hackers can clear logs to cover their tracks. Using interactive Trend Analysis reports from the Control Center, you can answer the following types of questions:

- How many severe security incidents occurred this quarter compared to the same quarter last year?
- Which production servers were most targeted for attack in the last six months?
- How many times were ports on my corporate Web servers scanned in the last week?

Log consolidation, archival, analysis, and reporting help you spot trends in events across the enterprise and help you meet mandated data-retention policies.

How Security Manager Works

Security Manager is a multi-tiered enterprise product that offers a comprehensive and scalable solution for a number of prominent security management problems:

- Monitoring perimeter security products in real time
- Correlating events across multiple entry points to detect complex attacks
- Understanding security trends in your enterprise
- Delivering log archival and reporting solutions

Security Manager offers real-time data collection components as well as log archival and event correlation components. This product architecture overview assumes you plan to employ the full spectrum of features Security Manager offers. If you are not using all available Security Manager products or features, such as correlation, you may not need all the components shown in the following figures.

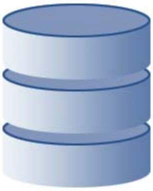
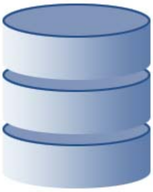
Understanding Product Components

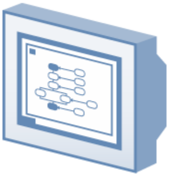
Security Manager includes a number of software components that you can distribute and install as needed to meet your security management objectives and environment.

If you are evaluating Security Manager, you can install all the components on one computer. However, this approach is not recommended for a production installation. You should plan to distribute the workload over a number of computers, installing components strategically.

The following table defines the major purposes of the product components.

Software Component	Purpose
Windows, UNIX, and iSeries Agents 	Services running on Windows, UNIX, or iSeries computers to monitor operating systems, devices, or applications, such as antivirus and firewall products, in real time.
Central Computer Components 	Software running on central computers that receive data from agents and send real-time and log data to log archives. **Central computers** also install, uninstall, and configure Windows agents, distribute rules to Windows agent computers, and control data flow between all agents and the log archive and database servers. Central computers can provide the following additional services: **Correlation server –** receives data forwarded by all central computers, applies correlation rules, and generates responses when rule matches occur. **Web Console server –** hosts the Web site for the Web Console computers.

Software Component	Purpose
Databases 	Databases located on the **database server** store real-time events and alerts, report data resulting from Forensic Analysis queries, and configuration data. Security Manager includes the OnePoint database, LogManagerConfiguration database, and SecurityManagerCommon database, depending on your configuration, in a Microsoft SQL Server repository. Each configuration group contains one database server.
Log archive server 	The **log archive server** is the computer used by Security Manager to store daily log data in log archives, including both events and alerts. Each central computer sends log data to a log archive server.
Reporting server 	The **reporting server** gathers data from the log archive to construct and store the reporting cube, using Microsoft SQL Server Analysis Services. A **cube** is a multidimensional database of interrelated, summarized data. The **reporting cube** provides data for Trend Analysis reports and can also provide data for custom Summary reports created using SQL Server Business Intelligence Development Studio. The **cube depot** is the staging database that receives exported log archive data and uploads it into the reporting cube.

Software Component	Purpose
Consoles 	The consoles present information for different purposes: **Control Center –** monitor and resolve alerts about real-time events, create reports of Trend Analysis or Forensic log data, and compile your research into incident packages across multiple configuration groups. **Development Console –** customize processing rules, computer groups, and other Security Manager components for your environment. **Web Console –** monitor and resolve alerts about real-time events using Microsoft Internet Explorer.

Understanding Configuration Groups

Security Manager operates in a domain environment running on distributed computers configured to work together as a group. A Security Manager **configuration group** typically includes the following computers:

- Agent computers. Agent computers are computers with agents installed from which Security Manager collects logs or monitors real-time events.
- One or more central computers
  - For event correlation, consider adding a central computer to act as a dedicated Correlation server.
  - For the Web Console, select a central computer to host the Web Console server.
- One database server
- One reporting server (optional). You need a reporting server only if you want to use Security Manager reporting capabilities.
- One or more computers running consoles
- One or more log archive servers (optional). You need a log archive server only if you want to use Security Manager log management capabilities.

Security Manager provides a great deal of installation flexibility. For example, to increase the number of agents you want to monitor, you can add more central computers. If you need to monitor several regional locations, you can add more configuration groups. If you want to send data from one central computer to one log archive server but want to keep data from a second central computer separate, you can add a second log archive server.

Understanding the Architecture

Because of the inherent adaptability of Security Manager, there is no "one-size-fits-all" solution for installing Security Manager. When you install Security Manager, you can decide where to install the product components based on your environment and requirements for load balancing, failover, and performance.

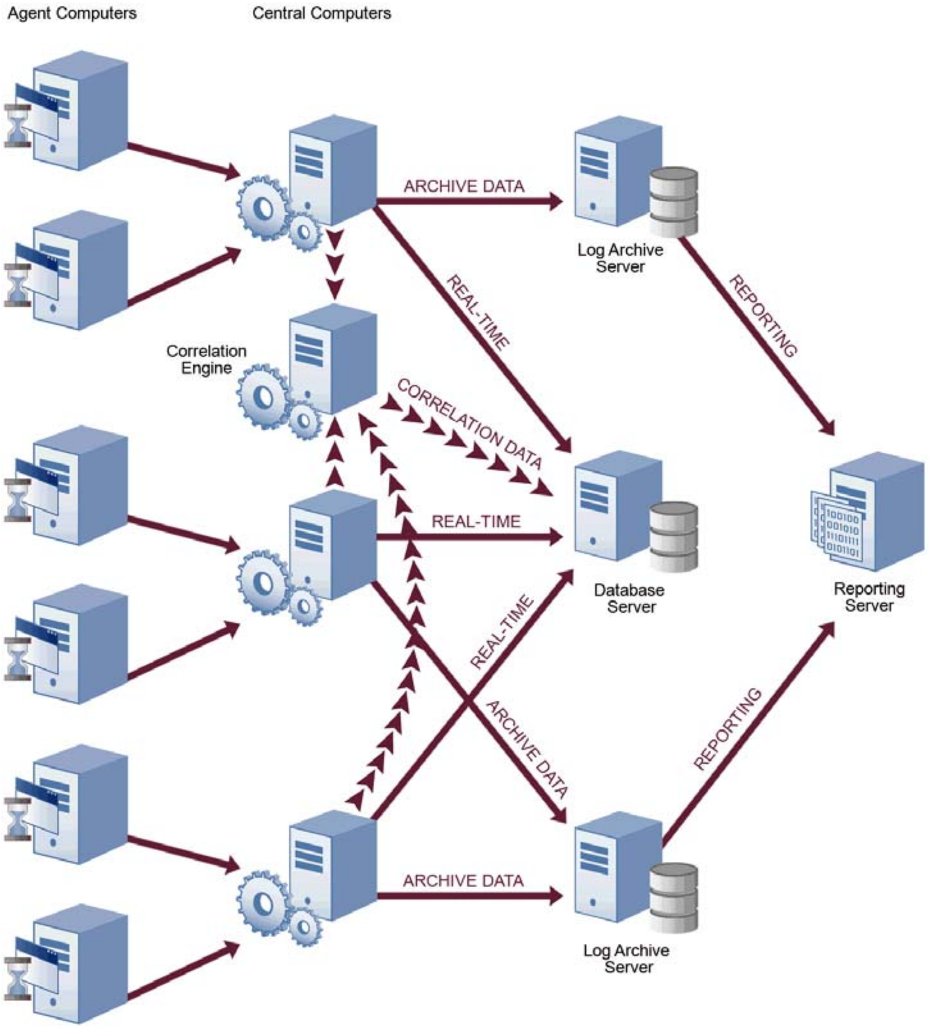
The agent computers, central computers, reporting server, log archive servers, and database server make up a configuration group. You can control where to install various components of the configuration group, including where to install the database server and how many central computers or log archive servers to install.

A choice of configuration options is especially important in large distributed enterprises or when communicating over slower network links, such as WANs. In some environments, you may want to optimize load balancing and performance by installing multiple configuration groups.

The best way to choose a deployment model is to conduct a pilot study that emulates the modules you want to install, the production hardware you plan to use, and the anticipated event volume.

Note
Although it is possible to install all Security Manager components on a single computer, NetIQ does not recommend this deployment model due to performance issues.

The following model illustrates a typical way to deploy Security Manager in a production environment.



This model uses many agents that report to distributed central computers, one database server configured to gather real-time data and store configuration information for Security Manager, one reporting server, and multiple log archive servers configured to store log data for archival and reporting purposes. You can have one or more log archive servers, depending on the number of events your environment generates.

When you use this model and plan to use Security Manager event correlation, designate a central computer as the Correlation server. For more information about the roles central computers serve in a configuration group, see “Anticipating Your Hardware Needs” on page 11.

Anticipating Your Hardware Needs

The following table outlines the major purpose of each component running on computers in the configuration group and identifies important hardware considerations.

Computer Roles	Software Components
Central computers 	**Agent Manager –** installs, configures, identifies, updates, and uninstalls agents on Windows computers. **Consolidator –** receives event data from Windows agents, stores events in the real-time database, and periodically distributes rules to Windows agents (I/O-intensive). The Consolidator also acts as an agent on its local computer. If a central computer becomes unavailable, another central computer in the configuration group continues to collect event and alert data from agents. **Core Service –** processes queued event data for storage on log archive server, digitally signs log archive data, and processes user queries and query results, using the Business Services, Log Handler, and Log Watcher subcomponents. **Data Access Server –** interacts with the database server and provides database access control. **Log Engine –** collects event data for Forensic Analysis reports. **Web Console server –** hosts the Web Console server, which is a Web site that provides alerts to the Web Console.

Computer Roles	Software Components
Central computer selected as Correlation server 	**Correlation Engine –** correlates events across multiple entry points to detect complex attacks and generates responses (memory-intensive). To optimize performance, do not use the Correlation server central computer to monitor Windows, UNIX, or iSeries agents. If the Correlation server becomes unavailable, correlation fails over to another central computer in the configuration group.
Reporting server 	**Reporting cube –** stores summarized log archive data from the log archive server for use in Trend Analysis reports and in custom Summary reports. **Cube depot –** acts as a staging database for log archive data using a scheduled SQL Server Integration Services package to update the reporting cube.
Database server 	**OnePoint database –** stores real-time alerts, events, and configuration data. **LogManagerConfiguration database –** stores configuration data about NetIQ UNIX Agent (UNIX agent) and NetIQ Security Agent for iSeries (iSeries agent) for use by Security Manager. **SecurityManagerCommon database –** stores user settings, Favorites, and Incident Packages for the configuration group and connected configuration groups. This Microsoft SQL Server database computer must have appropriate disk capacity and I/O speed. Fast disk access, multiple physical devices, and RAID arrays are recommended for most environments.

Computer Roles	Software Components
Log archive server 	**Log archives –** associated with one or more specified central computers to store daily log data (I/O-intensive). Fast disk access, multiple physical devices, and RAID arrays are recommended for most environments.

Understanding Security Manager Data Flows

The Security Manager central computer receives data from agents running on servers throughout your enterprise. Security Manager uses the data in the following ways to help you comprehend and improve your security:

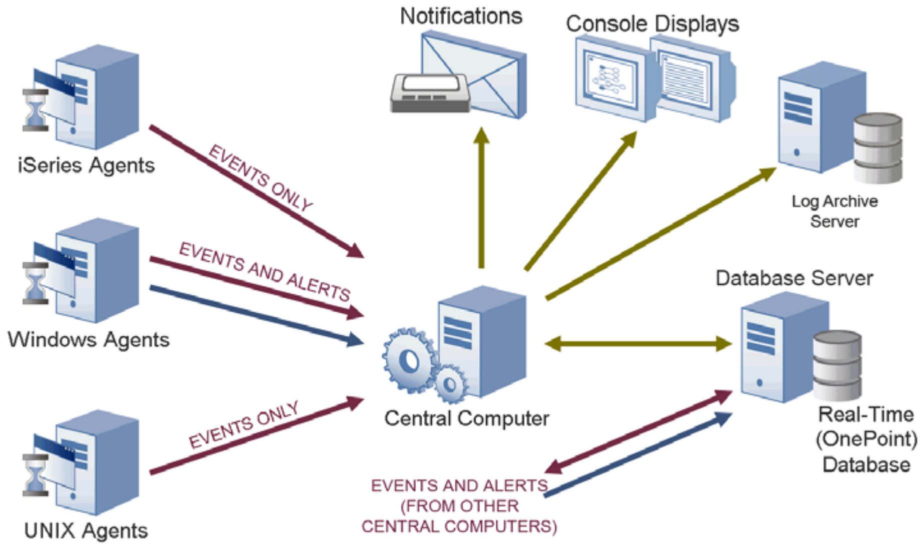
- Inform you about the current state of security (real-time alerts and events)
- Identify events indicating complex threats (correlated real-time events)
- Research significant historical security incidents (log data)
- Understand current security and trends (reporting data)

To better understand how Security Manager uses the data it collects to help you manage security, you should understand how the data flows through each path or **datastream**. To collect and store this useful information, the central computer receives or gathers data and passes it into the following datastreams:

- Real-time
- Correlation
- Log management
- Reporting and trend analysis

Real-Time Alerting Data Flow

As events occur, Windows agents evaluate Security Manager rules. When a rule match occurs, the Windows agent generates an alert and sends it to a central computer, along with the events that triggered the alert. If the rule specifies to notify a security analyst or group, the central computer delivers the page or email. UNIX and iSeries agents also apply rules as events occur and send the events to the central computer, as shown in the following figure.



All central computers forward alert and event data to the real-time database on the database server. You can manage the automatic grooming settings for the real-time database from the Development Console. **Grooming** allows Security Manager to remove data from databases based on specified settings.

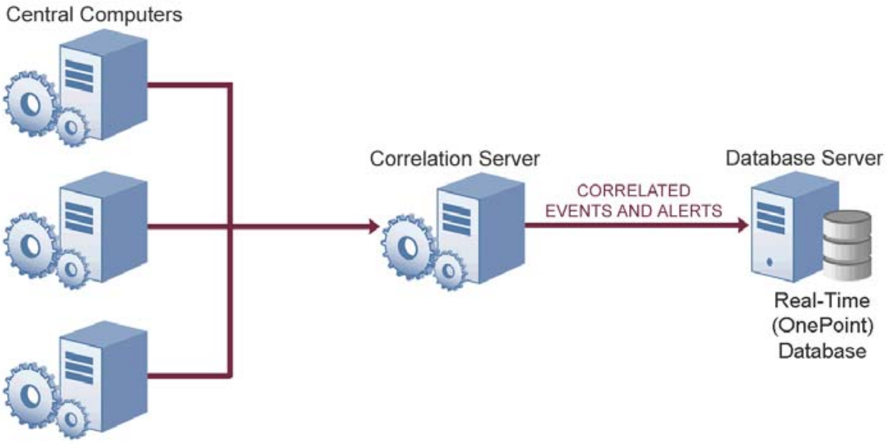
The central computers also send alert and event data to the log archive server for storage in the log archive. You can manage the automatic grooming settings for the log archive from the Log Archive Configuration utility.

The consoles poll for updated information from the central computer, which communicates with the real-time OnePoint database to acquire information from all the central computers in the configuration group.

The consoles initially display an alert resolution state of New. Security analysts can address the alert using the alert resolution workflow.

Event Correlation Data Flow

Event correlation is the analysis of a stream of real-time events to identify their meaning in context. Event correlation limits false positive alerts to provide timely and relevant alerts. All central computers collect events from agents and forward selected events to the central computer designated as the Correlation server to apply event correlation rules, as shown in the following figure.

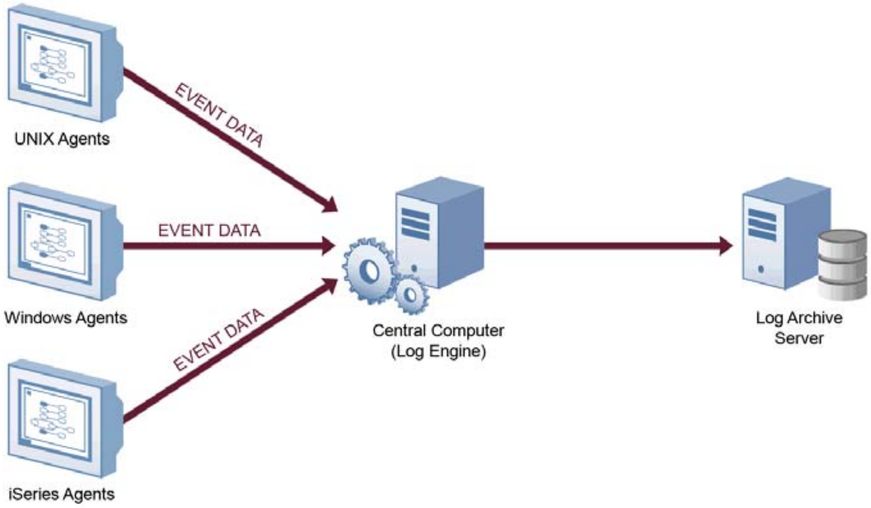


A **correlation rule** is a set of criteria that configures Security Manager to detect a pattern of real-time events and respond accordingly. The Correlation server evaluates collected alerts and events against the correlation rules as data arrives. When a rule match occurs, the Correlation server responds as defined in the rule and sends the source events and resultant alerts to the real-time (OnePoint) database on the database server and to the log archive.

You can define event correlation rules to evaluate events received from the real-time datastream from Windows, UNIX, or iSeries agents. To create event correlation rules, run the **Correlation Wizard**. The Correlation Wizard lets you select multiple alerts and then easily define a relationship and time frame. Correlation rules can amplify the importance of alerts, suppress less important alerts, and alert you to seemingly unrelated activities that may indicate a threat.

Log Management Data Flow

Central computers receive events from Windows agents and forward them to the Log Engine component. The Log Engine also periodically retrieves UNIX and iSeries event logs, as shown in the following figure.



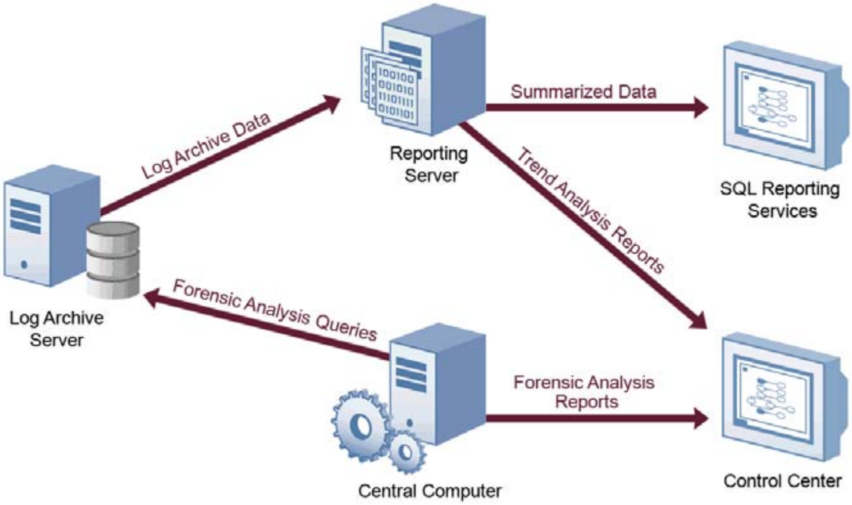
The Log Engine receives the event data and sends it to a log archive for storage. Each central computer receives only a portion of the log data, so the Log Engine on each central computer transfers its portion to a log archive on a dedicated log archive server.

Initially, Security Manager retains log data in the log archive for 90 days by default. When log data is older than the retention period, the log archive server deletes the oldest data to free space for newer data. You can configure the log archive retention period using the Log Archive Configuration utility on the log archive server.

Reporting and Trend Analysis Data Flow

After the log archives receive and store data from the central computers, Security Manager sends log data from the log archives to the reporting server. Security Manager does not send whole events to the reporting server, but sends a predefined list of most frequently used fields from each event to save space and processing time.

The reporting server summarizes the data, stores the summarized reporting data in the reporting cube, and assembles dimension information for Trend Analysis reports, as shown in the following figure.



Trend Analysis reports are charts of interrelated, summarized log data contained in a multi-dimensional database called a cube. Trend Analysis reports allow you to examine enterprise-wide security trends.

The reporting server updates the reporting cube with collected log archival data from different log archive servers. Scheduled reporting cube processing occurs every 3 hours, by default. You can view processed reporting data in the Trend Analysis reports in the Control Center. You can also access reporting cube data directly using Microsoft SQL Server Reporting Services.

Raw event data is available for Forensic Analysis queries as soon as it is stored and indexed on the log archive server. You can use the Control Center to query all the log archive servers to retrieve raw event data. **Forensic Analysis reports** are the results of the queries and provide event-level detail that spans all dates available in the log archives. The log archive data retention period is initially set to 90 days, but you can change the retention period to suit your needs.

Understanding Windows Component Communication

Security Manager components installed on Windows computers communicate at specified intervals using agents to transfer data and receive processing rules. **Processing rules** define how Security Manager collect, process, and respond to information.

Your enterprise can adjust the following default communication intervals to meet your needs:

- Windows agents initiate a heartbeat every 5 minutes to report status and request updates from the central computer. A **heartbeat** is a periodic communication from agents that contain information related to their viability.
- Central computers check for processing rule changes every 5 minutes.
- Central computers scan managed agent computers daily at 2:05 AM to install, uninstall, and configure managed agents.

Allow the appropriate time for any configuration or rule changes you make to take effect. For example, when you change an event processing rule, the product can take up to 15 minutes to automatically begin enforcing the rule on monitored Windows computers.

An **event processing rule** is a rule that configures Security Manager to monitor and process event data and then specifies any actions Security Manager takes in response to detecting a certain event. To implement changes immediately, you can initiate a rule update or scan for new computers.

A **monitored computer** is a computer from which Security Manager collects and processes information. Collected information can indicate critical security events occurring on the monitored computer. In most cases, an agent resides on a monitored computer.

Understanding Windows Agent Communication Security

Security Manager uses the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocols included in the Microsoft Secure Channel (SChannel) security package to encrypt data.

Security Manager supports all SChannel cipher suites, including the Advanced Encryption Standard (AES), adopted as a standard by the U.S. government. Central computers and agents authenticate one another by validating client and/or server certificates, an industry-standard technique for establishing trust.

Out of the box, Security Manager uses a default self-signed certificate, installed on the central computer, for communication between the central computer and monitored Windows agents. If you want to enable authenticated communication, you can implement your own Public Key Infrastructure (PKI) and deploy custom certificates on central computers and agents, replacing the default central computer certificate.

The following Security Manager core components comply with the requirements of the FIPS 140-2 Inside logo program:

- central computer
- log archive server
- database server
- reporting server
- Security Manager 6.5.4 Windows agents

Understanding Self-Scaling Windows Operations

Security Manager automatically adds agents to Windows computers throughout your network. As you add Windows computers to your network, Security Manager automatically detects those computers, checks them for the role they serve in the network, such as an IIS server, and installs agents as necessary.

As your Windows network changes, Security Manager automatically changes with it. Security Manager ensures that the right knowledge is applied to the right computers at the right time.

The low-overhead components in Security Manager allow you to monitor tens or hundreds of servers in your enterprise with little system degradation. Security Manager also regularly updates Windows agents with new or modified processing rules. Central computers automatically apply updated processing rules to the appropriate monitored Windows computers.

Understanding Supported Windows Platforms

Security Manager can monitor Windows computers running the following versions of Windows:

- Windows 7 (32- and 64-bit)
- Windows Server 2008 R2
- Windows Server 2008 R2 Server Core
- Windows Server 2008 (32- and 64-bit)
- Windows Server 2008 Server Core (32- and 64-bit)
- Windows Server 2003 R2 (32- and 64-bit)
- Windows Vista (32- and 64-bit)
- Windows Server 2003 (32- and 64-bit)
- Windows XP (32- and 64-bit)
- Windows 2000

Understanding Supported Data Formats

Security Manager can receive and process data in both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) formats. In addition, you can install Security Manager components on dual-stack computers, which are computers that have both IPv4 and IPv6 running at the same time.

However, you cannot install Security Manager components on computers running only IPv6. Security Manager requires that IPv4 be installed, either by itself or along with IPv6.

Note

If you want to use your Security Manager agent to receive data that contains IPv6 format IP addresses, you must install IPv6 on the agent computer. For more information about installing IPv6, see the Microsoft Windows Server Help.

Managing UNIX and iSeries Agents

Security Manager provides communication with UNIX and iSeries agents but does not directly install agents or deploy updated rules to them.

Security Manager offers support for UNIX, Linux, and iSeries operating systems. For more information about specific operating system support and for more information about using agents on these platforms, see the NetIQ UNIX Agent or NetIQ Security Solutions for iSeries documentation.

Chapter 2

Understanding the Development Console

The Development Console interface includes the Development Console snap-in and the Configuration snap-in. Use the Development Console to customize the way Security Manager monitors computers and collects data.

Security Manager can monitor your enterprise right out of the box using built-in knowledge in the form of computer groups and processing rules. To extend and control Security Manager, use the Development Console to perform the following types of customization:

- Define your own computer grouping rules and processing rules.
- Extend Security Manager capabilities with scripting.
- Add custom computer attributes for defining computer groups.
- Control who is notified in response to an alert.
- Update the Security Manager configuration to include your changes.
- Identify additional sources of data in your enterprise that Security Manager can use.

Development Console Permissions Requirements

The Security Manager setup program installs the Development Console if your license includes this feature. Security Manager uses a combination of licensing and Windows group membership to permit access to features within the Development Console. To use the Development Console, log on with a user account that is a member of the OnePointOp Operators or OnePointOp ConfgAdms group. For more information about assigning permissions based on the OnePointOp group memberships, see the *Installation Guide for NetIQ Security Manager.*

To use all the features provided by the Development Console and Configuration snap-ins, ensure you are a member of the OnePointOp ConfgAdms group. For more information about the permissions each OnePointOp group provides, see the *Installation Guide for NetIQ Security Manager.*

Licensing

Your license controls the Security Manager functions you can use. You can review your license components in the Development Console.

To review your license components:

1. Log on to the Development Console computer with a user account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console > Configuration.**
4. In the left pane, click **Global Settings.**
5. In the right pane, click **License**.
6. On the Action menu, click **Properties.**

7. On the License tab, review your license components.
8. ***If the list does not include a license for the components you have licensed,*** contact your NetIQ sales representative.
9. Click **OK**.

For more information about licensing UNIX agents, see the NetIQ UNIX Agent documentation. For more information about licensing iSeries agents, see the NetIQ Security Solutions for iSeries documentation.

Working with Multiple Configuration Groups

When you install Security Manager, you can install components on different computers, depending on your environment and needs. If your enterprise requires more than one configuration group, install Security Manager using more than one database server.

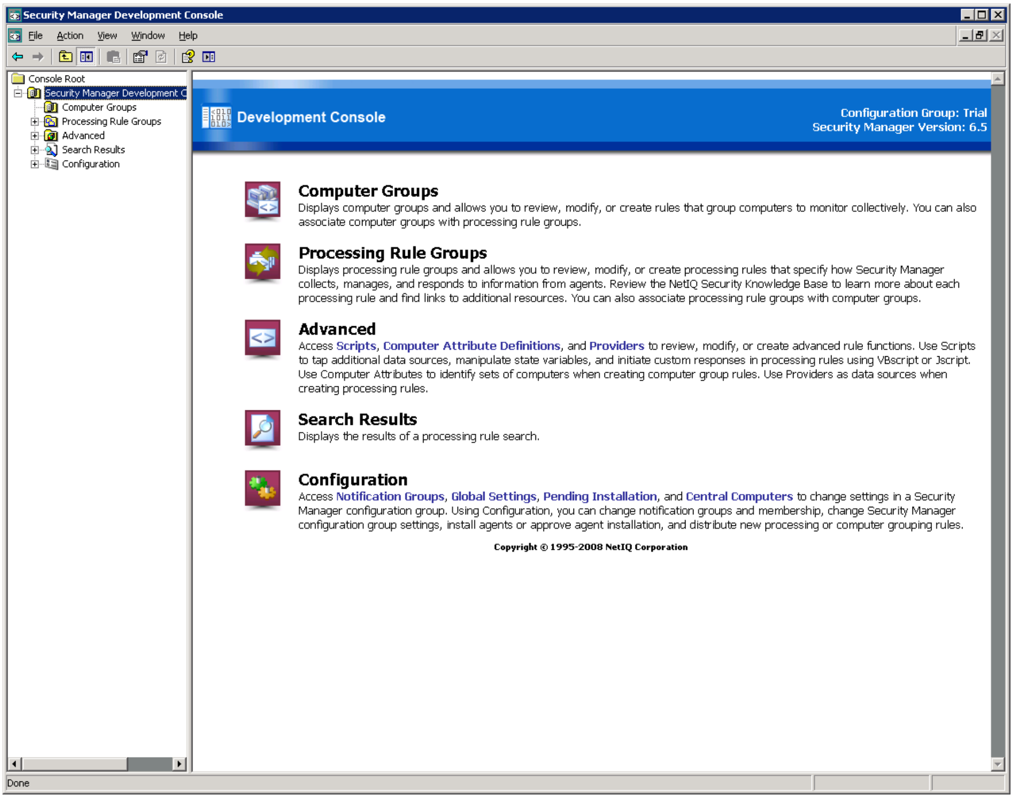
The Development Console allows you to monitor rules for only one configuration group at a time. If you need to define rules for more than one configuration group, you have the following options:

- Add another instance of the Development Console snap-in for each configuration group in your environment.
- Export information from the Development Console from one configuration group and import it into a Development Console in another configuration group.

For more information about the considerations and benefits of different installation configurations, see the *Installation Guide for NetIQ Security Manager.*

Development Console Snap-in

The following figure illustrates the Development Console:



Development Console

Configuration Group: Trial
Security Manager Version: 6.5

Computer Groups
Displays computer groups and allows you to review, modify, or create rules that group computers to monitor collectively. You can also associate computer groups with processing rule groups.

Processing Rule Groups
Displays processing rule groups and allows you to review, modify, or create processing rules that specify how Security Manager collects, manages, and responds to information from agents. Review the NetIQ Security Knowledge Base to learn more about each processing rule and find links to additional resources. You can also associate processing rule groups with computer groups.

Advanced
Access Scripts, Computer Attribute Definitions, and Providers to review, modify, or create advanced rule functions. Use Scripts to tap additional data sources, manipulate state variables, and initiate custom responses in processing rules using VBscript or Jscript. Use Computer Attributes to identify sets of computers when creating computer group rules. Use Providers as data sources when creating processing rules.

Search Results
Displays the results of a processing rule search.

Configuration
Access Notification Groups, Global Settings, Pending Installation, and Central Computers to change settings in a Security Manager configuration group. Using Configuration, you can change notification groups and membership, change Security Manager configuration group settings, install agents or approve agent installation, and distribute new processing or computer grouping rules.

Copyright © 1995-2008 NetIQ Corporation

The Development Console provides the following panes:

- The left pane allows you to navigate through the Development Console snap-in and the Configuration snap-in.
- The right pane displays details or results. When you select an item in the left pane, the right pane displays details for the item you selected.

Note
Many items in the Development Console include a right-click menu that lets you choose context-sensitive actions. The items on right-click menus are also available on the Action menu.

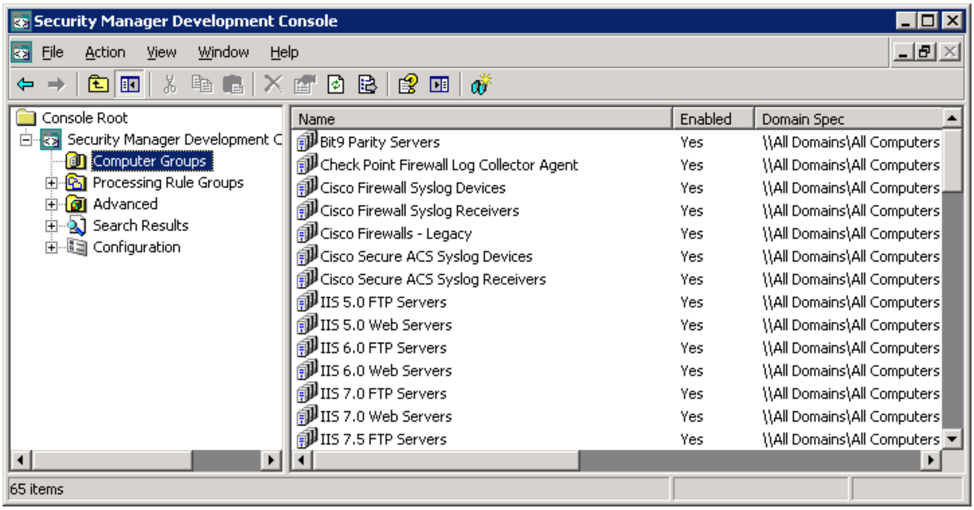
Expand **Security Manager Development Console** in the left pane to display the following windows:

- Computer Groups
- Processing Rule Groups
- Advanced
- Search Results
- Configuration

The Development Console does not automatically refresh its panes and windows. Refresh the display by clicking the Refresh icon on the console tool bar or by restarting the Development Console. The following sections provide an overview of the Development Console windows and how to use them to customize Security Manager.

Computer Groups Window

A **computer group** defines a set of computers. All computers in a computer group are monitored in the same way. Click **Computer Groups** in the left pane to display a list of Windows computer groups in the right pane. The following figure displays defined computer groups.



Name	Enabled	Domain Spec
Bit9 Parity Servers	Yes	\\All Domains\All Computers
Check Point Firewall Log Collector Agent	Yes	\\All Domains\All Computers
Cisco Firewall Syslog Devices	Yes	\\All Domains\All Computers
Cisco Firewall Syslog Receivers	Yes	\\All Domains\All Computers
Cisco Firewalls - Legacy	Yes	\\All Domains\All Computers
Cisco Secure ACS Syslog Devices	Yes	\\All Domains\All Computers
Cisco Secure ACS Syslog Receivers	Yes	\\All Domains\All Computers
IIS 5.0 FTP Servers	Yes	\\All Domains\All Computers
IIS 5.0 Web Servers	Yes	\\All Domains\All Computers
IIS 6.0 FTP Servers	Yes	\\All Domains\All Computers
IIS 6.0 Web Servers	Yes	\\All Domains\All Computers
IIS 7.0 FTP Servers	Yes	\\All Domains\All Computers
IIS 7.0 Web Servers	Yes	\\All Domains\All Computers
IIS 7.5 FTP Servers	Yes	\\All Domains\All Computers

65 items

You cannot create or view non-Windows computer groups using the Development Console. Security Manager automatically creates computer groups for non-Windows computers during installation and configuration. Security Manager uses non-Windows computer groups to allow you to run reports against specific platforms using the Control Center. You can create computer groups for Windows agents to monitor non-Windows devices.

Security Manager is a rules-based system that requires you to create a **computer grouping rule** to define a Windows computer group. Typically, you define a computer group by identifying an attribute shared by the Windows computers in the group. For example, you can group computers running Microsoft Internet Information Services (IIS) 4.0. For more information about creating computer grouping rules, see “Understanding Computer Groups” on page 43.

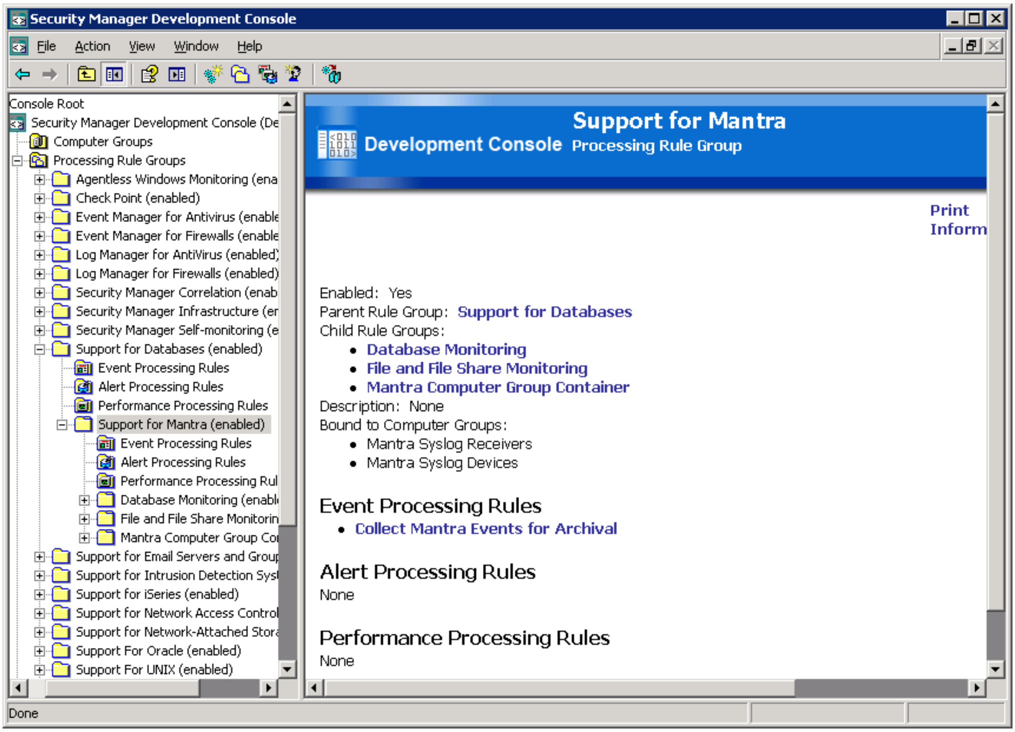
You can group Windows computers based on domain or computer name, a computer attribute (registry key or value), or by including or excluding a computer. If the built-in list of computer attributes does not include an attribute you want to use to group computers, you can define additional computer attributes. For more information about defining new computer attributes, see “Understanding Windows Computer Attributes” on page 53.

Processing Rule Group Window

Processing rule groups contain related processing rules. Processing rule groups organize related processing rules, such as all the rules to monitor a specific application. Each processing rule group may include **parent** rule groups and **child** rule groups. Expand **Processing Rule Groups** in the left pane to display the parent rule groups. Expand a parent processing rule group to view its child rule groups.

Processing rules define how Security Manager monitors your enterprise. For more information about processing rules, see “Understanding Processing Rules” on page 77.

The following figure shows the Security Manager for Mantra processing rule group and its child processing rule groups. The right pane displays information about the Security Manager for Mantra rules.


Security Manager Development Console
File
Action
View
Window
Help
Console Root
Security Manager Development Console (De
Computer Groups
Processing Rule Groups
Agentless Windows Monitoring (ena
Check Point (enabled)
Event Manager for Antivirus (enable
Event Manager for Firewalls (enable
Log Manager for AntiVirus (enabled)
Log Manager for Firewalls (enabled)
Security Manager Correlation (enab
Security Manager Infrastructure (er
Security Manager Self-monitoring (e
Support for Databases (enabled)
Event Processing Rules
Alert Processing Rules
Performance Processing Rules
Support for Mantra (enabled)
Event Processing Rules
Alert Processing Rules
Performance Processing Rul
Database Monitoring (enabl
File and File Share Monitorin
Mantra Computer Group Co
Support for Email Servers and Group
Support for Intrusion Detection Syst
Support for iSeries (enabled)
Support for Network Access Control
Support for Network-Attached Stora
Support For Oracle (enabled)
Support For UNIX (enabled)
Development Console
Print
Inform
Done

Support for Mantra
Processing Rule Group

Enabled: Yes
Parent Rule Group: Support for Databases
Child Rule Groups:

- Database Monitoring
- File and File Share Monitoring
- Mantra Computer Group Container

Description: None
Bound to Computer Groups:

- Mantra Syslog Receivers
- Mantra Syslog Devices

Event Processing Rules

- Collect Mantra Events for Archival

Alert Processing Rules
None

Performance Processing Rules
None

When you create a processing rule group, Security Manager automatically creates three subgroups: Event Processing Rules, Alert Processing Rules, and Performance Processing Rules.

You can search processing rule groups for a specific processing rule or for rules that match specified search criteria. When you perform a search, the right pane displays the rules that match the search criteria. For more information about processing rules, see “Working with Processing Rules” on page 101.

You can also print reports about processing rule groups or rules. For more information about printing reports, see “Processing Rule Group Example” on page 65.

Advanced Window

When you expand **Advanced** in the left pane, the right pane displays descriptions of advanced capabilities Security Manager provides. Security Manager provides the following advanced capabilities:

Scripts Window

Create new scripts or modify existing scripts to use in creating custom responses in your processing rules. You can write your own scripts using VBScript or JScript. For more information about scripting, see “Understanding Scripts” on page 139.

Computer Attribute Definitions Window

Expand **Computer Attribute Definitions** to view available computer attributes or create new ones. For more information about computer attributes, see “Understanding Computer Grouping Criteria” on page 46.

Providers Window

When you create a processing rule, you define an information source, or data provider, of the information you want to monitor. Processing rules use data provided from several predefined sources, such as Windows event logs or scripts. Expand **Provider** to see all the predefined data providers. You can also create providers in this window. For more information about providers, “Understanding Data Providers” on page 89.

Search Results Window

You can search processing rule groups based on keywords or wildcard characters. The Search Results window displays any processing rules that match your search criteria. You may want to search for processing rules to find all rules related to one topic or to locate processing rules you want to customize. For more information about using the search feature, see “Finding a Processing Rule” on page 116.

Configuration Snap-in

The Development Console also provides the Configuration snap-in.

To provide access to the Configuration snap-in, add users or groups to the OnePointOp ConfgAdms group.

The Configuration snap-in allows you to manage the following Security Manager features:

Notification Groups

Lets you create or modify notification groups. Notification groups are groups of operators to be notified in response to alerts. You can also create or modify operators.

Global Settings

Lets you configure component settings that apply throughout the configuration group, such as alert resolution, license, and correlation settings.

Pending Agents

Lets you review, approve, or cancel pending changes to Windows agents. The Pending Agents folder contains lists of Windows computers with pending installations and updates and pending uninstallations.

Central Computers

Lists all central computers in the configuration group and lets you view details of each central computer, including the agents they manage. You can also specify the service account used by the agents that a central computer installs on Windows computers.

For more information about using the Configuration snap-in, see the *User Guide for NetIQ Security Manager* or the Help.

Chapter 3
Understanding Alerts and Alert Configuration

Alerts indicate potential problems or informational events. Each alert identifies the severity of its associated event or performance threshold. Alert severity helps you prioritize conditions.

You create alerts within processing rules using the Development Console. Processing rules indicate when to generate alerts and how to respond if the alert occurs.

Security Manager rules can issue alerts as part of their response to events or performance data. The following types of processing rules can generate alerts:

- Event rules
- Missing event rules
- Threshold rules
- Correlation rules

Users monitor alerts using the Control Center or the Web Console. You can create **alert views** that display the alerts you want to monitor, including alerts from specific computers, alerts of a particular severity, or alerts with a specific resolution state. For more information, see the *User Guide for NetIQ Security Manager.*

You can assign more than one alert to an event. For example, Security Manager provides a performance threshold rule that checks CPU utilization. If the average of the samples taken over a 30-minute period indicate greater than 95 percent use, the computer could be experiencing a Denial of Service (DoS) attack. The rule response is to generate a Security Breach alert. An additional processing rule could also respond by generating an Error alert that sends a Simple Network Management Protocol (SNMP) trap to an administrator monitoring HP OpenView.

Alert processing rules let you manage multiple alerts so you can issue the same response to many alerts issued by many processing rules. For example, one alert processing rule can specify to page the Network Administrators notification group when any Security Breach alert occurs from rules in a specified processing rule group. For more information about alert rules, see “Understanding Alert Processing Rules” on page 87.

Defining Alerts

Security Manager provides predefined alerts for monitored environments or applications within processing rule groups. You can also create alerts that are specific to your enterprise using the Development Console.

You can define alerts when you create processing rules. Processing rules identify the information to collect, the alert to generate, and additional responses to the condition.

The following types of processing rules allow you to define alerts:

Event rules
Can generate an alert when specified events occur.

Missing event rules
Can generate an alert when a specified event does not occur during a specified time.

Threshold rules
Can generate an alert when a Windows performance counter or Windows Management Instrumentation (WMI) numeric value crosses a defined threshold.

Correlation rules

Can generate an alert when real-time event patterns indicate a security breach.

You can use alert processing rules to define additional responses to alerts issued by processing rules. For more information about defining responses to alerts, see "Understanding Alert Processing Rules" on page 87.

Alert Severity

When an event or threshold occurs that matches a processing rule, Security Manager associates the specified alert and alert severity to that event and displays the alert in the Control Center and Web Console. Alert severity allows security personnel monitoring alerts to quickly determine the importance of the indicated condition. Set the alert severity when you create the processing rule. Possible alert severities are defined as follows:

Service Unavailable

Identifies alerts generated for missed agent heartbeats and other events indicating that an application or service is unavailable to its users.

Security Breach

Identifies an alert that indicates a security compromise has occurred. Systems on the network are at risk.

Critical Error

Identifies an alert that indicates a serious problem needing attention immediately.

Error

Identifies an alert that is important and needs attention soon.

Warning

Identifies an alert that might indicate future problems or lower priority issues requiring research.

Information

Identifies an alert that simply provides information.

Success

Identifies an alert that indicates a successful event or operation.

Duplicate Alert Suppression

Event storms can occur when an application or system rapidly produces a large number of identical events. If you have an alert associated with an event in an event storm, you may receive multiple alerts for the same event within a short time.

Security Manager can provide **duplicate alert suppression**. If duplicate alerts are received while the original alert remains unresolved, Security Manager combines the duplicate alerts into a single alert. The Control Center and Web Console display only a single alert. The alert properties indicate the number of combined alerts.

You can enable duplicate alert suppression when you create or modify a processing rule that generates an alert.

Custom Alert Fields

You can create your own custom alert property fields and view these fields when you view the properties of any alert. You might use custom alert fields in the following situations:

- Trouble-ticket number from a related help desk system
- Customer name whose service level agreement is affected
- Building containing the affected computer

Alert Responses

Processing rules also let you define a response to an alert. Responses to alerts can help resolve the issue that caused the event or alert. You can define the following responses to alerts:

- Send a notification to a notification group
- Execute a command or batch file
- Send an SNMP trap
- Change state variables
- Launch a script

Processing rules let you define more than one alert response. For example, if a Security Breach alert indicates that a security violation has occurred, Security Manager can respond by running a batch file that locks out an offending user account and also responds by paging security personnel. For more information about responses, see “Working with Processing Rule Responses” on page 122.

Monitoring Alerts

Security personnel monitor alerts using the Control Center or Web Console. Monitoring alerts depends on several conditions being met, whether from your own processing rules or from default Security Manager processing rules. The following conditions apply:

- An alert is defined within a processing rule.
- The processing rule group that contains the processing rule is associated with a computer group.
- The event or performance criteria specified in the processing rule has occurred.
- Security Manager has generated an alert.

Alerts provide detailed information about computer conditions. Security personnel can read in-depth information about each alert in its knowledge base. They can view the alert resolution history to verify which resolution actions have been taken and determine any further actions to resolve the situation that caused the alert.

The Control Center supports custom views so you can track just the alerts you choose. Security Manager also supplies predefined views to help you get started. For example, the Control Center supplies views called All Open Alerts and All Service Level Exceptions. Custom views you could create include Open alerts from a specified source and Alerts that are not Resolved, or other criteria you specify. For more information about using the Control Center, see the *User Guide for NetIQ Security Manager.*

Alert Resolution

When an event or threshold occurs that matches an alert-generating processing rule, Security Manager generates an alert. When security personnel monitor alerts, they can read important information about each alert that helps determine the next action. The Control Center display information about alerts, such as the following properties:

- Alert icon indicating the severity
- Computer generating the event associated with the alert
- Resolution state
- Resolution history
- Knowledge Base
- Custom alert fields

You can define these alert fields in rules using the Development Console. For more information about defining alert fields in rules, see “Working with Processing Rules” on page 101.

Resolution State

Resolution state indicates alert resolution progress. Using the Control Center or Web Console, security personnel can change the resolution state of an alert to track resolution progress. The default resolution states are defined as follows:

New
Indicates this alert has not yet been addressed. Alerts are New by default.

Acknowledged
Indicates that this alert has been read and acknowledged, but not assigned.

Level 1: Assigned to helpdesk or local support
Indicates that the help desk or local support is responsible for this alert.

Level 2: Assigned to subject matter expert
Indicates that a subject matter expert is responsible for this alert.

Level 3: Requires scheduled maintenance
Indicates that the alert identifies a condition requiring maintenance, which is scheduled.

Level 4: Assigned to external group or vendor
Indicates that an external group or vendor is responsible for this alert.

Resolved
Indicates that the condition that generated this alert is solved.

You can modify or delete most of the default resolution states in the Alert Resolution Global Setting in the Configuration snap-in. You cannot modify or delete the New and Resolved states. You can also create your own states to meet the needs of your enterprise. For example, you can create In Progress or Deferred resolution states.

You can set a service level agreement time for each resolution state. Service level agreement time is the maximum time that an alert can remain in a particular resolution state. For example, company policy might require that no alert can remain in the New resolution state for longer than 10 minutes. If an alert remains in the New state for longer than 10 minutes, it is considered a service level exception. Use the Control Center to view all service level exceptions.

The All Service Level Exceptions view in the Control Center and Web Console shows alerts that spent more time than expected at a particular service level. For more information about resolving alerts, see “Alert Resolution” on page 38.

Note

Scripts can also change alert resolution states. For example, if you run a script to resolve an alert condition, the script can change the resolution state to Resolved.

Resolution History

Security Manager automatically tracks and records all changes to alert properties, including changes made by a processing rule, changes made by scripts, and any automatic responses. You cannot edit the automatic alert resolution history. It provides a record of alert resolution.

Using the Control Center, security personnel can add information to the resolution history. When you change the resolution state of a specific alert or when you have gathered more information about the issue, you can provide your own comments to keep an up-to-date record of the alert resolution process. Providing specific comments allows you to accumulate knowledge about this particular instance of the alert. By adding resolution comments to individual alerts, you can track how a particular condition was addressed. The resolution history is important in tracking the alert, particularly if the process of resolving the alert spans several operator shifts.

Creating Alert Knowledge

Using the Control Center, security personnel monitoring alerts can add information to the company knowledge base when an alert is resolved. Using the Development Console, security personnel can add information to the company knowledge base when they create a rule and when an alert is resolved.

This information can include details on the resolution of this particular alert, which can help others resolve similar alerts in the future. The information you add to the company knowledge base is appended to the Knowledge Base of the processing rule that generated the alert, and becomes available in later alerts. You can, over time, collect a valuable knowledge base of alert resolution information specific to your company and enterprise.

Chapter 4
Understanding Computer Groups

Computer groups are groups of computers that have some attribute in common, such as all computers with McAfee VirusScan installed. You can create Windows computer groups. You can also add Windows computers to built-in computer groups.

Computer groups use **computer grouping rules** to define the types of computers to include. Organizing Windows computers into computer groups allows Security Manager to apply certain processing rules to the same computers in a configuration group. For more information about processing rules, see “Understanding Processing Rules” on page 77. Organizing non-Windows computers into computer groups allows Security Manager to provide all computer groups for reports in the Control Center.

Security Manager groups UNIX computers, iSeries servers, and other devices differently than Windows computers. During product installation and configuration, Security Manager groups non-Windows computers and devices into computer groups that you cannot customize. For more information about installing and configuring support for UNIX computers, iSeries servers, and other devices, see the *Installation Guide for NetIQ Security Manager.*

You do not need to create or modify computer groups for correlation. Security Manager stores all correlation rules in the Correlation processing rule group folder, which is associated with the NetIQ Security Manager Central Computer computer group. For more information about event correlation, see “Correlate Events (Correlation Rule)” on page 82.

The following sections provide information about working with computer groups for Windows computers.

Built-in Windows Computer Groups

Security Manager provides built-in computer groups for Windows network configurations and commonly used applications that Security Manager monitors out-of-the-box.

If you are creating custom processing rules, the built-in Windows computer groups might not contain the computers to which you want to deploy the custom processing rules. You can create a Windows computer group to contain the computers. You can identify the computers to place in the computer group using computer grouping criteria, such as explicit inclusion or computer attributes. For more information about computer grouping criteria, see “Understanding Computer Grouping Criteria” on page 46. For more information about creating computer groups, see “Creating a Windows Computer Group” on page 48.

Windows Computer Group Membership

As you change the role of specific Windows computers in your environment, Security Manager automatically identifies and places computers in the appropriate computer groups. You do not need to build lists of computer names and maintain those lists to keep computer groups up to date.

For example, a computer group that includes all computers with Trend Micro ScanMail for Exchange installed today will continue to include these computers and other computers on which you install the application at a later date. Likewise, if you uninstall ScanMail for Exchange from a computer, Security Manager no longer includes it in the computer group.

The central computer places Windows computers in the appropriate computer groups if the following two conditions are met:

- An agent is installed or to be installed on the Windows computer. For more information about installing agents on Windows computers or other platforms, see the Help and the *Installation Guide for NetIQ Security Manager*.
- The computer matches the criteria defined in the computer group properties. For more information about computer group properties, see “Understanding Computer Grouping Criteria” on page 46.

The central computer also places Windows **agentless monitored computers** in the same computer groups associated with the Windows **proxy agent** computer. An agentless monitored computer is a Windows computer with no agent that is monitored by an agent on another Windows computer, which is called a proxy agent.

Central computers place Windows computers in or remove computers from the appropriate computer groups at the following times:

- Upon receiving computer attributes from a Windows agent during a heartbeat
- After computer attribute definitions change
- During a managed computer scan, which occurs at 2:05 AM, by default

If you modify computer attribute definitions, the central computer sends the computer attribute definitions to the Windows agents at the next heartbeat. The Windows agents send their computer attributes to the central computer at the following heartbeat. Then the central computer places computers in or removes computers from the appropriate computer groups. This process typically occurs within 10 minutes.

If you create a custom computer attribute, the central computer sends the custom computer attribute definitions at the next heartbeat, and it receives the computer attributes as usual. However, if you created the computer attribute definition before using it in a computer group, you may need to wait until the next managed computer scan or when Windows agents resend their attributes, whichever occurs first, before the central computer places computers in the computer group.

You can accelerate the process. For more information about computer group membership, see “Updating Windows Computer Group Membership” on page 60.

Note
If the computer group is associated with a processing rule group, the central computer also periodically updates the Windows agent with processing rules contained in the processing rule group. For more information about associating computer groups with rule groups, see “Associating a Windows Computer Group with a Processing Rule Group” on page 52.

Understanding Computer Grouping Criteria

Security Manager allows you to group Windows computers based on specified criteria, such as domain, computer name, or registry keys or values that identify computer attributes, such as the operating system or installed applications. You can also specify exceptions to explicitly include or exclude particular computers in a group, even if the computer otherwise matches the rule. A computer group can also specify to include another computer group. This control and flexibility lets you match any set of Windows computers in your environment so Security Manager can appropriately monitor each computer.

The following computer group properties let you specify computer grouping criteria and processing rules to apply to the computers:

General
Specify a computer group name and description and choose to enable or disable the rule.

Computer Types
Specify to match Windows computers based on their roles as primary domain controller (PDC), backup domain controller (BDC), member servers, or workstations.

Computers (Computer Name and Domain)

Specify to match all Windows computers based on domain or computer naming conventions using wildcard characters, regular expressions, or Boolean regular expressions. For more information about how Security Manager recognizes text strings that include wildcard characters, see the Help.

Formulas (Computer Attributes)

Specify to match Windows computers based on a registry key or value (computer attribute), membership in an existing computer group, or combined criterion using Boolean operators or wildcard matching. When you create a computer grouping rule based on a computer attribute, you can choose from a list of predefined or custom computer attributes. You can also create a custom computer attribute on the Formulas tab. For more information about computer attributes, see "Understanding Windows Computer Attributes" on page 53.

Excluded or Included Computers

Specify to explicitly exclude or include specific computers by domain or computer name. Choose from a variety of text pattern matching methods to identify computers. For more information about excluding or including computers, see "Understanding Exclusion and Inclusion" on page 57.

Processing Rules

Specifies which processing rule groups to associate with this computer group. For more information about associating computer groups with rule groups, see "Associating a Windows Computer Group with a Processing Rule Group" on page 52.

Working with Computer Groups

Security Manager provides tremendous flexibility with Windows computer groups. You can create new computer grouping rules to define new sets of Windows computers for Security Manager to manage and monitor. The following topics provide step-by-step guidance for working with Windows computer groups.

Creating a Windows Computer Group

Computer groups define sets of Windows computers with something in common, such as a group of all computers with Norton AntiVirus installed. You can associate computer groups with processing rule groups so that the rules apply to all computers in the computer group.

You can also create computer groups based on other computer groups. For example, you could create a computer grouping rule that includes all the computers in the Windows 2003 computer group, and evaluates for an attribute that indicates they are also running Microsoft Exchange 2000.

For new or modified computer groups, Security Manager places computers in computer groups at the next managed computer scan or when the central computer receives computer attributes from Windows agents. For more information about this process, see "Windows Computer Group Membership" on page 44.

To create a Windows computer group:

1. Log onto the Development Console computer with a user account that is a member of the OnePointOp ConfgAdms group. Creating a computer group requires OnePointOp Operators group membership. However, applying your changes immediately requires OnePointOp ConfgAdms group membership. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*

2. Start the **Development Console** in the NetIQ Security Manager program group folder.

3. In the left pane, expand **Security Manager Development Console**.

4. Click **Computer Groups**.

5. On the Action menu, click **Create Computer Group**.

6. Follow the instructions until you have finished creating a new computer group and associating it with processing rule groups. For more information about the fields on a window, see the Help.

7. ***If you want the computer group and associated processing rules to take effect immediately,*** complete the following steps.

    a. In the left pane, expand **Security Manager Development Console > Configuration**.

    b. Click **Central Computers**.

    c. On the Action menu, click **Scan All Managed Computers**.

    d. Click **OK**.

8. ***If you want to verify that the computer group is created,*** examine the Computer Groups window and locate the computer group you created.

9. ***If you want to verify that computers are placed in the computer group,*** examine the **All Computer Groups** view in the Development Console or the Control Center. Locate the computer group in this view, and then ensure the appropriate computers are identified as members. For more information about fields on a window, see the Help.

Copying a Windows Computer Group

You can copy a Windows computer group, paste it, and modify its properties to create a new computer group. You can copy and paste a computer group within the current Development Console or into a Development Console for another configuration group.

To copy a Windows computer group:

1. Log on to the Development Console computer with a user account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*

2. Start the **Development Console** in the NetIQ Security Manager program group folder.

3. In the left pane, expand **Security Manager Development Console**.

4. Click **Computer Groups**.

5. In the right pane, click the computer group you want to copy.

6. On the Action menu, click **Copy**.

7. In the left pane, click **Computer Groups**. You can paste a computer group only into a Computer Groups folder in a Development Console.

8. On the Action menu, click **Paste**.

Deleting a Windows Computer Group

If a Windows computer group is no longer required, you can delete it. When you delete a computer group, the processing rule groups associated with the computer group are no longer applied to computers in the deleted computer group.

Warning
Do not delete built-in computer groups. The built-in processing rule groups that use the built-in computer groups no longer work properly if you delete the built-in computer groups.

To delete a Windows computer group:

1. Log on to the Development Console computer with a user account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.

2. Start the **Development Console** in the NetIQ Security Manager program group folder.

3. In the left pane, expand **Security Manager Development Console**.

4. Click **Computer Groups**.

5. In the right pane, click the computer group that you want to delete.

6. On the Action menu, click **Delete**.

7. Click **Yes**.

Modifying Windows Computer Group Properties

When you modify computer grouping rules, Security Manager places or removes computers as necessary. Security Manager places computers in or removes computers from computer groups at the next managed computer scan or when the central computer receives computer attributes from Windows agents. For more information about computer group properties, see “Windows Computer Group Membership” on page 44.

Warning
Modify built-in computer groups with extreme caution. The built-in processing rule groups that use the built-in computer groups you modify may no longer work properly.

You can also modify computer group properties using the Control Center. For more information about using the Control Center to modify computer group properties, see the *User Guide for NetIQ Security Manager.*

To modify Windows computer group properties:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**.
4. Click **Computer Groups**.
5. In the right pane, click the computer group you want to modify.
6. On the Action menu, click **Properties**.
7. Specify the appropriate settings.
8. Click **OK**.

Associating a Windows Computer Group with a Processing Rule Group

If you create a Windows computer group, associate it with the processing rule group containing the processing rules you want applied to the computers in the computer group. You can associate computer groups and processing rule groups in the Development Console. Built-in processing rule groups are already associated with built-in computer groups.

Processing rules are updated periodically on agents. You can expedite this process. For more information about updating processing rules, see “Forcing Processing Rule Changes” on page 121.

You can also associate computer groups with processing rule groups using the Control Center. For more information about using the Control Center to modify computer group properties, see the *User Guide for NetIQ Security Manager*.

To associate a Windows computer group with a processing rule group:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**.
4. Click **Computer Groups**.
5. In the right pane, click the computer group you want to associate with a processing rule group.
6. On the Action menu, click **Properties**.
7. Click the Processing Rules tab.
8. Follow the instructions on the Processing Rules tab. For more information about the fields on a window, see the Help.
9. Click **OK**.

Understanding Windows Computer Attributes

You can group Windows computers using characteristics the computers have in common. These characteristics are called **computer attributes** and are based on the presence of registry keys or registry key values.

When you create a Windows computer group, you can choose from a list of predefined or custom computer attributes. You can also create a custom computer attribute during the computer group creation process. Security Manager places computers with the specified attribute in the computer group.

The central computer sends computer attribute definitions to Windows agents whenever it installs a Windows agent or the definitions change. The Windows agents send their computer attributes to the central computer when it first installs the Windows agents, every 24 hours since the Windows agents last sent their computer attributes, or during a managed computer scan if the computer attributes are older than 24 hours. For more information about computer group attributes, see "Windows Computer Group Membership" on page 44.

Predefined Windows Computer Attributes

Security Manager provides predefined computer attributes that define built-in Windows computer groups. Predefined computer attributes are located in the Advanced window in the Development Console.

You can use predefined computer attributes to create a Windows computer group. For more information about working with computer attributes, see "Creating a Windows Computer Group" on page 48.

Custom Windows Computer Attributes

You can create custom computer attributes that you can use and reuse to create Windows computer groups. For more information about creating Windows computer groups, see "Creating a Windows Computer Group" on page 48.

When you create or modify a computer attribute, the central computer sends the computer attribute definition to the Windows agents at the next heartbeat. Then the Windows agents collect their computer attributes and send them to the central computer at the following heartbeat. After the central computer receives computer attributes, it places computers in the appropriate computer groups. For more information about Windows computer groups, see "Windows Computer Group Membership" on page 44.

Working with Windows Computer Attributes

The topics in the following sections provide step-by-step guidance for completing computer attribute tasks.

Creating a Custom Windows Computer Attribute

You can use custom computer attributes to create Windows computer groups. For example, you can create a custom computer attribute that identifies computers running Netegrity SiteMinder. You can then use the custom computer attribute to create a Windows computer group.

You can define a computer attribute based on a Windows registry key or registry value. Security Manager supports defining computer attributes based on the following registry types: `REG_SZ, REG_EXPAND_SZ, REG_MULTI_SZ, REG_DWORD`.

Notes

- Before you create a custom Windows computer attribute, check for the presence of a registry key or value to use to identify the product you want to monitor. In some cases you can use a registry key to identify whether the product is installed. In other cases, you may need to identify the version of the installed application, and so may need to know the value of a specific registry key.
- If you need to specify a registry value, be sure to note whether the value is a string, integer, float, or IP address.

The following task describes the process of creating a custom computer attribute. You can also create a custom computer attribute while creating a computer group.

To create a custom Windows computer attribute:

1. Identify and make a note of the registry key or value that conclusively identifies the computers you want to monitor.
2. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
3. Start the **Development Console** in the NetIQ Security Manager program group.
4. In the left pane, expand **Security Manager Development Console** > **Advanced**.
5. Click **Computer Attribute Definitions**.
6. On the Action menu, click **New > Computer Attribute Definition**.
7. Follow the instructions until you finish creating a computer attribute. For more information about the fields on a window, see the Help.

Copying a Windows Computer Attribute

You can copy a Windows computer attribute, paste it, and modify its properties to create a custom computer attribute. You can copy and paste a computer attribute within the current Development Console or into a Development Console for another configuration group.

To copy a Windows computer attribute:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console** > **Advanced**.
4. Click **Computer Attribute Definitions**.

5. In the right pane, click the computer attribute you want to copy.

6. On the Action menu, click **Copy**.

7. In the left pane, click **Computer Attribute Definitions**. You can paste a computer attribute only into a Computer Attributes folder in a Development Console.

8. On the Action menu, click **Paste**.

Modifying Windows Computer Attribute Properties

You can modify the properties of Windows computer attributes as your network changes.

Warning
Use extreme caution when modifying predefined computer attributes. Changing predefined computer attributes may cause problems with computer grouping rules that rely on them. Also, a later Security Manager upgrade resets predefined computer attributes. If you create a computer group, consider creating a custom computer attribute to use in the computer grouping rule.

For more information about creating custom Windows computer attributes, see “Creating a Custom Windows Computer Attribute” on page 54.

To modify a Windows computer attribute:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*

2. Start the **Development Console** in the NetIQ Security Manager program group.

3. In the left pane, expand **Security Manager Development Console > Advanced**.

4. Click **Computer Attribute Definitions**.

5. In the right pane, click the computer attribute you want to modify.

6. On the Action menu, click **Properties**.

7. Specify the appropriate settings.

8. Click **OK**.

Understanding Exclusion and Inclusion

When a Windows computer matches a computer grouping rule, Security Manager automatically places it in the computer group. However, you can override the rule match by explicitly excluding or including computers.

Explicit Exclusion

You may want to group all similar Windows computers into a computer group to be monitored collectively, except for one special case. For example, if you monitor four Microsoft Exchange servers, but one server is routinely taken offline for backup purposes, you may not want to monitor it in the same way as you monitor the other Exchange servers. You can specify a Windows computer grouping rule that includes all computers running Exchange, but specifically excludes the special case computer.

The central computer does not place computers you exclude in the computer group even if they match other computer grouping criteria or were explicitly included. Exclusions override inclusions.

Explicit Inclusion

Sometimes the computer you want to monitor does not have a registry value you can use to create a computer attribute. If you do not have a computer attribute to use in the computer grouping criteria, then Security Manager cannot automatically identify the computer to place it in the computer group. You may need to explicitly include the computer in the computer group.

Unless explicitly excluded, computers you explicitly include are placed in the computer group even if they do not match other computer grouping criteria. However, exclusions override inclusions. If you use regular expressions or wildcard characters to both explicitly include and exclude groups of computers, computers matching only the inclusion criteria, not both, are placed in the computer group.

Working with Computer Exclusion and Inclusion

Using the Development Console, you can specify, by domain and computer name, which computers to always exclude or include in the computer group. The computers are excluded from or included in the Windows computer group regardless of their other properties. However, exclusions override inclusions. The following topics provide step-by-step guidance for working with exclusion and inclusion.

You can also modify computer group properties using the Control Center. For more information about using the Control Center to modify computer group properties, see the *User Guide for NetIQ Security Manager*.

Excluding a Computer from a Computer Group

You can exclude computers from a computer group. Computer exclusion changes take effect at the next managed computer scan or the next time agents send their computer attributes to the central computer. For more information about this process, see "Windows Computer Group Membership" on page 44. You can expedite this process. For more information about updating group membership, see "Updating Windows Computer Group Membership" on page 60.

To exclude a computer from a computer group:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**.

4. Click **Computer Groups**.
5. In the right pane, click the computer group from which you want to exclude a computer.
6. On the Action menu, click **Properties**.
7. Click the Excluded Computers tab.
8. Click **Add**.
9. Identify the computer you want to exclude. You can also browse to identify the computer to be excluded.
10. Click **OK**.

Including a Computer in a Computer Group

You can include computers in a computer group. Computer inclusion changes take effect at the next managed computer scan or the next time agents send their computer attributes to the central computer. For more information about this process, see "Windows Computer Group Membership" on page 44. You can expedite this process. For more information about updating group membership, see "Updating Windows Computer Group Membership" on page 60.

To include a computer in a computer group:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**.
4. Click **Computer Groups**.
5. In the right pane, click the computer group in which you want to include computers.
6. On the Action menu, click **Properties**.

7. Click the Included Computers tab.

8. Click **Add**.

9. Identify the computer you want to include. You can also browse to identify the computer to be included.

10. Click **OK**.

Updating Windows Computer Group Membership

Depending on the change, Security Manager updates computer group membership at different times. Updating computer group membership allows the central computer to place computers in or remove computers from the appropriate computer groups. For more information about this process, see "Windows Computer Group Membership" on page 44.

You can cause the central computer to immediately update computer group membership by initiating a managed computer scan.

Note

If the computer group is associated with a processing rule group, the central computer also periodically updates the Windows agent with processing rules contained in the processing rule group. For more information about this process, see "Forcing Processing Rule Changes" on page 121.

To immediately add Windows agents to computer groups:

1. ***If the computer on which you wish to update an agent is running the Windows Event Viewer or any MMC console,*** close the Windows Event Viewer and the MMC console before proceeding.

2. Log on to the Development Console computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*

3. Start the **Development Console** in the NetIQ Security Manager program folder.

4. In the left pane, expand **Security Manager Development Console > Configuration**.

5. Click **Central Computers**.

6. On the **Action** menu, click **Scan All Managed Computers**.

7. Click **OK**.

8. On the Action menu, click **Refresh** until the status of each central computer returns to idle. If the Windows computer does not have an agent installed and you configured the central computer to manage it, the central computer either installs the Windows agent or places it in the Pending Agents Installation list for approval. For more information about installing agents, see the Help.

9. Review the computers included by your computer grouping rule changes. For more information about viewing computers, see "Modifying Windows Computer Group Properties" on page 51.

Chapter 5
Understanding Processing Rule Groups

Processing rule groups are containers that let you categorize and organize your processing rules by application or topic. Each processing rule group automatically contains three folders that group rules by type: event, alert, or performance.

When you want specific processing rules to apply to a computer group, you associate a processing rule group with a computer group. You can associate parent or child processing rule groups with computer groups. However, you cannot associate a single processing rule with a computer group.

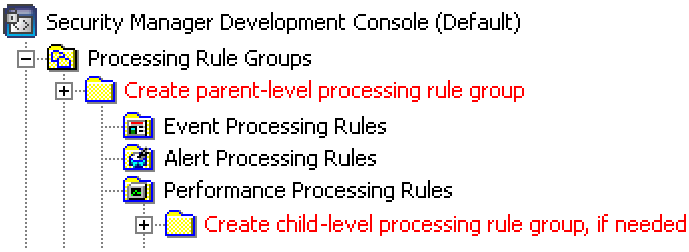
Note
You do not need to create processing rule groups for correlation. Security Manager stores all correlation rules in the Correlation processing rule group folder. For more information about event correlation, see “Correlate Events (Correlation Rule)” on page 82.

Processing Rule Group Hierarchy

Processing rule groups are hierarchical folders for your processing rules. Parent-level processing rule group folders typically contain no processing rules, but do contain other processing rule groups. The child-level processing rule groups contain the processing rules. When you create a processing rule group, consider if it should be a parent-level processing rule group or if your rules would more logically nest as a rule group under an existing parent-level processing rule group.

Note
Alert processing rules in the root processing rule group respond to alert rules in any processing rule group. Alert processing rules within a sub processing rule group respond only to alerts within that processing rule group, unless the rule specifically targets another processing rule group.

Consider the following example structure for processing rule group folders:



Security Manager Development Console (Default)
Processing Rule Groups
Create parent-level processing rule group
Event Processing Rules
Alert Processing Rules
Performance Processing Rules
Create child-level processing rule group, if needed

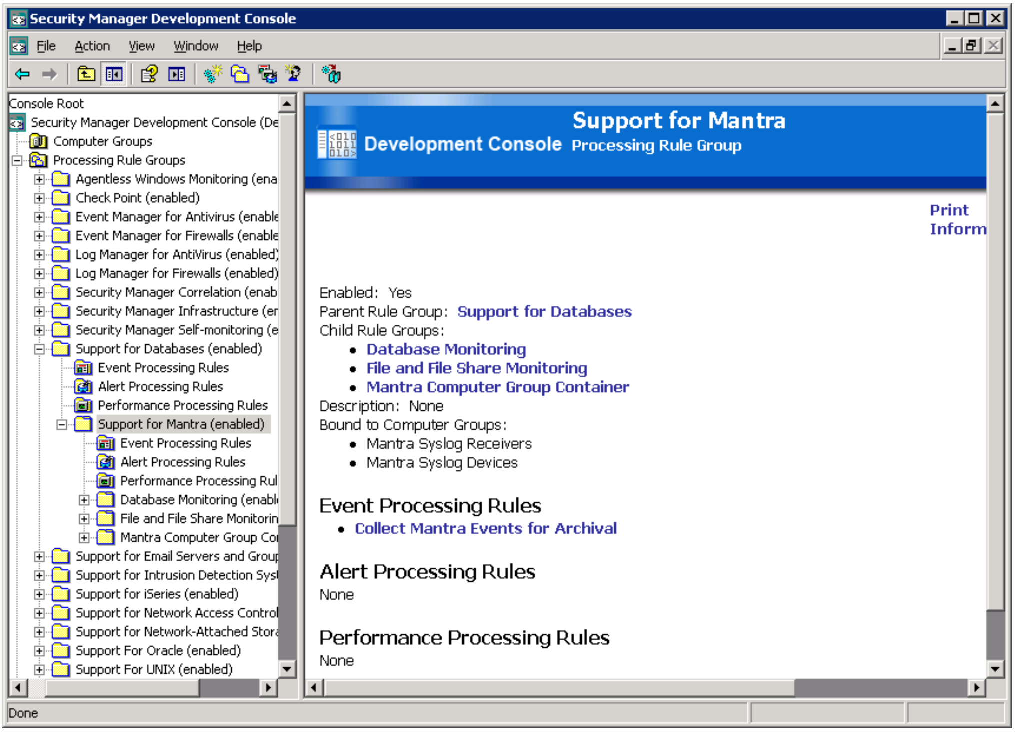
You can associate multiple Windows computer groups with a processing rule group. Rules are matched to computer groups using logical `OR` matching and are then distributed to the appropriate computer groups. Therefore, if a Windows computer matches any one of multiple computer groups associated with the processing rule group, Security Manager applies the rules in the processing rule group.

When you associate a computer group with a parent-level processing rule group, the computer group is automatically associated with all child-level processing rule groups nested under that processing rule group. To deliver rules only to specific computer groups to which they apply, you may want to associate child-level processing rule groups with computer groups.

Processing Rule Group Example

Since you associate processing rule groups with specific Windows computer groups, you can think of processing rule groups as groups of processing rules that pertain to specific types of computers. For example, you could group all processing rules you want to apply to computers running a specific application, such as Netegrity SiteMinder, into a processing rule group.

When you select a processing rule group in the left pane, the Development Console displays details describing the contents of the processing rule group in the right pane. The following figure shows the Development Console with the Security Manager for Mantra processing rule group selected.



Console Root
- Security Manager Development Console (De
  - Computer Groups
  - Processing Rule Groups
    - Agentless Windows Monitoring (ena
    - Check Point (enabled)
    - Event Manager for Antivirus (enable
    - Event Manager for Firewalls (enable
    - Log Manager for AntiVirus (enabled)
    - Log Manager for Firewalls (enabled)
    - Security Manager Correlation (enab
    - Security Manager Infrastructure (er
    - Security Manager Self-monitoring (e
    - Support for Databases (enabled)
      - Event Processing Rules
      - Alert Processing Rules
      - Performance Processing Rules
      - Support for Mantra (enabled)
        - Event Processing Rules
        - Alert Processing Rules
        - Performance Processing Rul
        - Database Monitoring (enabl
        - File and File Share Monitorin
        - Mantra Computer Group Co
    - Support for Email Servers and Group
    - Support for Intrusion Detection Syst
    - Support for iSeries (enabled)
    - Support for Network Access Control
    - Support for Network-Attached Stor
    - Support For Oracle (enabled)
    - Support For UNIX (enabled)

Enabled: Yes
Parent Rule Group: Support for Databases
Child Rule Groups:
- Database Monitoring
- File and File Share Monitoring
- Mantra Computer Group Container

Description: None
Bound to Computer Groups:
- Mantra Syslog Receivers
- Mantra Syslog Devices

Event Processing Rules
- Collect Mantra Events for Archival

Alert Processing Rules
None

Performance Processing Rules
None

Click links in the right pane to perform the following actions:

- To display a description of the child rule group, including a list of processing rules in the child rule group, click a child rule group link.
- To print the processing rule group report pane, click **Print** in the upper right corner. For more information about printing the report pane, see “Printing a Processing Rule Group Report” on page 73.
- To export information about the current processing rule group and all displayed rules to an HTML file, click **Export Group/Rule Information**. For more information about exporting the report pane, see “Exporting a Processing Rule Group Report” on page 74.

Processing Rule Group Security Knowledge

When you select a processing rule group in the left pane, the Development Console displays the NetIQ Knowledge Base in the right pane. The NetIQ Knowledge Base provides information about the processing rule group, including a summary of features and configuration information.

The NetIQ Knowledge Base is also available through the Control Center. For example, you can view the properties of an alert to learn more about the alert condition and what actions to take to address the cause of the alert.

You cannot modify the NetIQ Knowledge Base but you can add your own security knowledge in the **company knowledge base** when you create processing rules and when you resolve alerts. Over time, your company knowledge base adds value to your organization. Adding information to your company knowledge base reflects your security knowledge and helps others become more familiar with the security issues your organization faces.

Information you add to the company knowledge base when you resolve an alert can include details on the resolution of the alert, which can help others resolve similar alerts in the future. The information you add to the company knowledge base is appended to the Knowledge Base of the processing rule that generated the alert, and becomes available in later alerts.

Understanding the User Actions Processing Rule Group

Advanced users create most processing rules by using the Development Console. However, Control Center users who are members of the OnePointOp Operators group can create some event and alert processing rules. When Control Center users click an event in the Results window of an event view, Security Manager allows them to create an Event rule to generate an alert based on the event or a Filtering rule to filter the event. When Control Center users click an alert in the Results window of an alert view, they can create an Alert rule that notifies a particular notification group or sends an SNMP trap.

When Control Center users create Event, Filtering, or Alert rules, Security Manager creates the User Actions processing rule group to store the rules. The User Actions processing rule group is available the next time you open the Development Console. You can use the Control Center to reverse or modify these rules. Open the Control Center and click **Global Tasks > Undo User Actions** on the Tasks menu. For more information, see the *User Guide for NetIQ Security Manager.*

Control Center users can also create Correlation rules. Security Manager stores Correlation rules in the Correlation processing rule group folder.

Working with Processing Rule Groups

The following topics provide step-by-step instructions for working with processing rule groups.

Creating a Processing Rule Group

Processing rule groups contain processing rules. Creating different processing rule groups allows you to categorize processing rules. You can also create child groups, which are processing rule groups within a processing rule group. When you create a processing rule group, Security Manager automatically creates the following folders within the processing rule group:

- Event Processing Rules
- Alert Processing Rules
- Performance Processing Rules

To create a processing rule group:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager program group folder.
3. In the left pane, expand **Security Manager Development Console**.
4. Click **Processing Rule Groups**.
5. ***If you want to create a child processing rule group***, select the processing rule group to which you want to add the child, and on the Action menu, click **New > New Processing Rule Group**.
6. ***If you want to create a new parent processing rule group***, on the Action menu, click **Create Processing Rule Group**.
7. Follow the instructions to create the processing rule group. For more information about the fields on a window, see the Help.

Viewing Processing Rule Group Properties

You can view, modify, print, and export the properties of a processing rule group, including Knowledge Base and computer group information. You can view the properties of a processing rule group in two ways:

- The Processing Rule Group Properties window allows you to view and modify the properties.
- The right pane HTML report allows you to view, print, and export properties. You cannot modify processing rule group properties in the HTML report.

Note
You can configure the Development Console to display only custom rules created or modified by a user in the HTML report.

Viewing Properties in the Processing Rule Group Properties Window

The Processing Rule Group Properties window allows you to view and modify the properties.

To view processing rule group properties in the Processing Rule Group Properties window:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager program group folder.
3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.
4. Click the processing rule group with properties you want to view.
5. On the Action menu, click **Properties**.

Viewing Properties in an HTML Report

The right pane HTML report allows you to view, print, and export properties. You cannot modify processing rule group properties in the HTML report.

To view processing rule group properties in an HTML report in the right pane:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager program group folder.
3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.
4. Click the processing rule group with properties you want to view. The processing rule group properties are displayed in the right pane.
5. ***If you want to view all child processing rule group properties,*** click the **Expand/ Collapse all subprocessing rule groups** button on the toolbar.
6. ***If you want to view properties for all rules in all child processing rule groups,*** click the **Expand/Collapse all rules under subprocessing rule groups** button on the toolbar.
7. ***If you want to view only custom rules created or modified by a user,*** click the **Show custom rules only/all rules** button on the toolbar.

Modifying Processing Rule Group Properties

You can modify processing rule group properties, including the company knowledge base and associated computer groups.

To modify processing rule group properties:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager program group folder.
3. In the left pane, expand **Security Manager Development Console** > **Processing Rule Groups**
4. Click the processing rule group with properties you want to modify.
5. On the Action menu, click **Properties**.
6. Specify the appropriate values. For more information about fields on a window, see the Help.
7. Click **OK**.

Disabling a Processing Rule Group

You can disable a processing rule group to temporarily stop its processing rules from being evaluated on Windows agent computers in the associated computer group. When you disable a parent processing rule group, Security Manager also disables all child processing rule groups.

To disable a processing rule group:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager program group folder.
3. In the left pane, expand **Security Manager Development Console** > **Processing Rule Groups**.
4. Click the processing rule group that you want to disable.

5. On the Action menu, click **Properties**.
6. Clear the **Enabled** check box.
7. Click **OK**.

Deleting a Processing Rule Group

If a processing rule group is no longer required, you can delete it. All rules within the group are also deleted.

To delete a processing rule group:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager program group folder.
3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.
4. Click the processing rule group you want to delete.
5. On the Action menu, click **Delete**.
6. ***If you are deleting a parent rule group,*** click **Yes**. Child groups are not deleted. Child groups are moved to the top level of the rule group hierarchy.
7. ***If you are deleting a child rule group,*** click one of the following options:

   Delete the relationship with the parent rule group. The rule group is not deleted.

   The selected processing rule group is moved up to the top level in the rule group hierarchy. It is not deleted. If the child rule group is the child of a second rule group, the child group is displayed only in the hierarchy of the second rule group.

Delete the rule group. Do not delete child rule groups.

The selected rule group is deleted. Child rule groups are not deleted but are now displayed at the top level, unless the child rule group is the child of a second rule group. If the child rule group is the child of a second rule group, the child group is displayed only in the hierarchy of the second rule group.

8. Click **Processing Rule Groups** in the left pane.
9. On the Action menu, click **Refresh**.

Printing a Processing Rule Group Report

A parent-level processing rule group contains a knowledge base that provides summary information about the module. You can also expand the subfolders and rules with the toolbar to display more detailed information about the processing rule group in an HTML report. You can print this report.

To print the report of a processing rule group:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager program group folder.
3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.
4. Select a processing rule group.

5. On the toolbar, expand the processing rule group as follows:

    - To include a list of subprocessing rule groups and rules, on the toolbar, click **Expand/Collapse all subprocessing rule groups**.
    - To include details about each rule in the report, on the toolbar, click **Expand/ Collapse all rules under subprocessing rule groups**. Expanding all rules can make the report long and take time to display.
    - To include only rules created or modified by a user, click the **Show custom rules only/all rules**.

6. In the right pane, click **Print**.

7. ***If you want to collapse the subfolders and rules after you have printed the report***, click the same buttons that you clicked in Step **5**.

Note

Security Manager prints only rule group and rule information displayed in the HTML report in the right pane. If you do not expand groups or rules and click **Print**, Security Manager only prints the top-level list of rule groups or rules, as displayed in the report.

Exporting a Processing Rule Group Report

In addition to printing the HTML report displayed in the right pane of the Development Console, you can export all displayed information about the current processing rule group or groups and rules to an HTML file on your local computer. You can use this HTML report to view information about your processing rule groups and rules offline.

To export the report of a processing rule group to an HTML file:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*

2. Start the **Development Console** in the NetIQ Security Manager program group folder.

3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.

4. Select a processing rule group.

5. On the toolbar, expand the processing rule group as follows:

    - To include a list of subprocessing rule groups and rules, on the toolbar, click **Expand/Collapse all subprocessing rule groups**.
    - To include details about each rule in the report, on the toolbar, click **Expand/ Collapse all rules under subprocessing rule groups**. Expanding all rules can make the report long and take time to display.
    - To include only rules created or modified by a user, click the **Show custom rules only/all rules**.

6. In the right pane, click **Export Group/Rule Information**.

7. ***If you want to collapse the subfolders and rules after you have printed the report***, click the same buttons that you clicked in Step **5**.

Note
Security Manager only exports rule group and rule information displayed in the HTML report in the right pane. If you do not expand groups or rules and click **Export Group/Rule Information**, Security Manager only exports the top-level list of rule groups or rules, as displayed in the report.

Associating Processing Rule Groups and Computer Groups

Security Manager applies processing rules in processing rule groups to computers in the associated computer group. Rules in processing rule groups are not applied to any computers unless the processing rule group is associated with a computer group.

If you associate a computer group with a parent-level processing rule group, rules in the parent-level processing rule group and child-level processing rule groups are evaluated on the computers in the computer group. If you want all child group rules to be evaluated on the computers in a computer group, associate the parent group with the computer group.

If you associate one computer group with the parent-level processing rule group, and a different computer group with a child-level processing rule group, the child-level rules are evaluated on computers in both the parent- and child-level associated computer groups.

For more information about how the processing rule group hierarchy affects on which computers Security Manager applies the processing rules, see "Processing Rule Group Hierarchy" on page 64.

To associate a processing rule group with a computer group:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager program group folder.
3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.
4. Select the parent- or child-level processing rule group you want to associate with a computer group.
5. On the Action menu, click **Associate with computer group**.
6. Click **Add**.
7. Select the computer group to associate with this processing rule group.
8. ***If you want to associate this processing rule group with another computer group,*** click **Apply**. Repeat **Steps 4** through **6** to continue adding computer groups.
9. To complete the association, click **OK**.

Chapter 6

Understanding Processing Rules

Processing rules specify how Security Manager detects, collects, and responds to events collected by agents installed locally on Windows computers or remotely to monitor non-Windows computers and devices.

Security Manager stores processing rules in processing rule groups. Security Manager applies processing rules to Windows computers in the computer groups associated with the processing rule groups. For more information about computer groups, see “Understanding Computer Groups” on page 43.

Security Manager can apply processing rules only to Windows agent computers or to central computers, which also contain agent functionality. For example, Security Manager can apply processing rules to agents on central computers to configure receiving and monitoring syslog data sent by UNIX agents. The processing rules reside on the central computer.

The UNIX agent also provides a rule set to configure sending syslog data to Security Manager. The UNIX rule set is different than Security Manager processing rules and resides on the UNIX agent. For more information about the UNIX rule set, see the NetIQ UNIX Agent documentation and the Security Manager for UNIX module documentation.

Security Manager supplies many built-in processing rules, but you can also create or modify processing rules. Security Manager supports the following processing rule types:

- Event processing rules
- Performance processing rules
- Alert processing rules

Note
It is not recommended that you modify the processing rules in the Security Manager Self-monitoring Module. Unlike other Security Manager modules, upgrading the Self-monitoring Module deletes all changes to its processing rules.

Understanding Event Processing Rules

Event processing rules configure Security Manager to collect, monitor, or respond to events.

Security Manager can use some event processing rules to collect, monitor, correlate, or respond to **real-time events**. Real-time events are events that Security Manager is configured to detect and respond to in real-time for rapid resolution of critical issues. Security Manager stores real-time events in the OnePoint database on the database server. Some modules monitor only real-time events.

Security Manager can also use log collection rules to collect events from logs across the network for centralized analysis and reporting. These events are called **archival events**. Archival events are events that Security Manager collects, consolidates, and then stores in the log archive partitions on the log archive server. Security Manager uses log collection rules to process archival events separately from real-time events. Archival events are not further evaluated by other real-time event processing rules.

Security Manager supports the following types of real-time event processing rules:

Event rules
Alert on or respond to real-time events.

Filtering rules
Filter real-time events.

Missing event rules
Detect missing real-time events.

Consolidation rules
Consolidate similar real-time events.

Collection rules
Collect real-time events.

Correlation rules
Analyze real-time events and identify patterns.

Correlation collection rules
Collect real-time events for correlation.

Security Manager supports the following types of archival event processing rules:

Log collection rules
Collect archival events for storage in the log archive partitions.

Log filter rules
Filter archival events to prevent their storage in the log archive partitions.

Alert on or Respond to Event (Event Rule)

Choose **Alert or Respond to Event** if you want Security Manager to monitor for a certain real-time event, and then generate an alert a response, such as running a script or paging a response team. Security Manager stores the alert and the event in the OnePoint database. For more information about alerts and automated responses, see “Understanding Alerts and Alert Configuration” on page 33 and “Working with Processing Rule Responses” on page 122.

After you create an event processing rule that generates an alert, you can create an alert processing rule that initiates responses to the alerts the event rule generates. For more information about creating alert processing rules, see “Understanding Alert Processing Rules” on page 87.

Filter Event (Filtering Rules)

Filtering rules help you more effectively manage the large number of real-time events that Security Manager collects. Filtering rules can specify whether Security Manager processes events or stores them on the database server. This allows you to store only the events that are important for your security objectives.

Note

Filtering rules affect only real-time events, not archival events. For more information about filtering archival events, see “Filter Archival Event (Log Filter Rule)” on page 83.

For example, in Windows 2003 environments, you can filter events related to computer authentication and system-to-system communication from domain controllers. By filtering less important events, you can preserve resources for event processing and reduce storage space on the database server.

In another example, Security Manager provides a rule named `Pre-Filter Security Event 528 when User Name ends in '$'`. This rule filters security event 528, Successful Network Logon, when the user name ends in a dollar sign, indicating a computer logon. If this event is important in your enterprise, you may want to disable this predefined filtering rule.

Security Manager provides you with the following filtering rule types:

Pre-filter

For real-time events matching a pre-filter, Security Manager stops evaluating further processing rules, and does not save these events to the OnePoint database.

Database filter

For real-time events matching a database filter, Security Manager continues evaluating processing rules, but does not save matching events to the OnePoint database. Using these rules, you can define responses to these events, but not store the event in the OnePoint database.

Conditional filter

For real-time events matching a conditional filter, Security Manager continues evaluating processing rules, but saves events to the OnePoint database only if another processing rule match occurs. You can define responses for conditional filter rules.

Detect Missing Event (Missing Event Rule)

A **missing event** is a real-time event that you expect to occur within a specified time interval, but does not. For example, if you perform or automate routine tasks such as system backups, Security Manager can generate alerts and responses if these tasks do not occur as planned. You can create a missing event processing rule to respond to events that you expect to occur within a specific time interval. If the event does not occur, the rule takes the defined responses.

Consolidate Similar Events (Consolidation Rule)

Consolidation rules group similar real-time events from an agent into one summary event. **Event consolidation** provides a combined event to replace many similar events generated in a short time to reduce event noise.

For example, Security Manager provides a consolidation rule that consolidates all IIS 401.1 errors that occur within two minutes. IIS 401 errors are typically the result of permission problems accessing the appropriate page. If 10 or more of these events occur in two minutes, an IIS intrusion may be occurring. When 10 or more of these events occur, Security Manager denies the offending computer access to the IIS server and generates a consolidated event.

The consolidated event shows the number of duplicate events and the time of the first and last event that the consolidated event represents.

Security Manager can consolidate events from a single computer. If multiple similar events occur on two computers during the specified time, the individual agents consolidate the events on each computer, resulting in two separate summary events.

Consolidation rules do not generate alerts or define responses. You can create other event rules to generate alerts or provide responses for the consolidated event.

Collect Specific Events (Collection Rule)

Security Manager collects real-time events that match processing rules. Collection rules allow you to identify events to collect from specified sources that you want to monitor in real-time. Events that match a collection rule are further evaluated for other processing rule matches and stored in the OnePoint database.

Collection rules do not generate alerts or provide other responses. You can use collection rules if you want to collect real-time events only for inclusion in an event view. Otherwise, consider creating a log collection rule.

Correlate Events (Correlation Rule)

Correlation rules allow you to monitor and analyze a stream of real-time events to look for patterns that indicate a security breach. Rather than detecting a single event, a correlation rule detects multiple events and identifies patterns using the elapsed time, the number of events, the event identification, matching event parameters, or the order in which the event occurred.

Correlation rules can generate alerts. You can also use a correlation rule in the criteria of another correlation rule. You can create correlation rules using the Correlation Wizard. After you create correlation rules, you can view or modify the properties for each rule in the Development Console. For more information about modifying rule properties, see “Correlating Specific Events” on page 105.

When you create a correlation rule, the Correlation Wizard creates an associated correlation collection rule. Correlation collection rules are advanced rules used by Security Manager to collect the events and pass them to the Correlation Engine for evaluation by the correlation rules. You should not modify correlation collection rules. You can specify to make changes to the correlation rule using the Correlation Wizard, and then the wizard modifies the correlation collection rule, if necessary.

Collect Logs for Archival (Log Collection Rule)

Log collection rules allow you to collect logs for archival and reporting. Security Manager can collect, normalize, consolidate, and store archival events so you can analyze, run reports, and maintain an archive of events from numerous logs on various platforms.

Log collection rules are similar to collection rules because they also do not generate alerts or respond to events. However, events that match a log collection rule are not further evaluated for other real-time processing rule matches. You cannot specify which parameters to store. Instead, events that match a log collection rule are normalized to a standard format, evaluated for log filter rule matches, and then stored in the log archive.

Filter Archival Event (Log Filter Rule)

Log filter rules allow you to filter collected log data and prevent Security Manager from storing it in the log archive. You can create log filter rules to filter archival events that you have determined are too noisy or unimportant. Security Manager neither collects these events nor includes them in reports.

You can also use log filter rules with log collection rules to collect specific archival events from a log that Security Manager does not collect by default. For example, you can customize Security Manager to collect the Application log, and then use log filter rules to reject archival events you do not want to store.

Note

You cannot create log archival filter rules to filter syslog data sent by a syslog provider. You can create log archival collection rules for syslog data, but the syslog provider ignores any criteria specified. If you want to filter syslog data or collect only specific events, you must configure the parse map for your syslog provider to process syslog data.

For more information about syslog providers, see “Creating a Data Provider for Syslog” on page 97.

Event Processing Rule Properties

When you review a defined rule, Security Manager displays the rule Properties window. For more information about displaying the Properties for a rule, see “Working with Processing Rules” on page 101. The Properties tabs typically display the rule criteria that you supply when creating event processing rules. For more information about any entry on a tab, see the Help.

Depending on the event processing rule, the following tabs may be available:

General

Specifies a name and whether the processing rule is enabled. This tab also provides information about the processing rule description, path, GUID, and last modified date.

Data Provider

Specifies the event or performance data provider name and type. For more information about data providers, see “Understanding Data Providers” on page 89.

Criteria

Specifies the properties to match, such as event source, event number, event type, description, user generating the event, source computer, source domain, computer on which the event is logged, or domain in which the event is logged.

You can define some criteria using wildcard characters, regular expressions, or Boolean regular expressions. For more information about text string pattern matching, see the Help.

Schedule

Specifies the schedule that defines when to apply the processing rule: always process data, process data only during the specified time, or always process data except during the specified time. The default schedule is to always apply the rule and process the data.

Alert

Specifies whether to generate an alert for a real-time event if a rule match occurs.

Alert Suppression

Specifies whether to suppress duplicate alerts and allows you to select the criteria for the alert to be considered duplicate.

Responses

Specifies response actions to take when a rule match occurs for a real-time event. For more information about processing rule responses, see “Working with Processing Rule Responses” on page 122.

Knowledge Base

Specifies information about the processing rule, such as what caused an alert, how to resolve an issue, or how to configure the processing rule or parameters in a script response.

Understanding Performance Processing Rules

Performance processing rules provide real-time monitoring of Windows computers for system resource usage and performance thresholds based on the following types of information:

- Windows performance counters
- Windows Management Instrumentation (WMI) numeric data
- Script-generated performance data

If the monitored computers exceed specified performance thresholds, Security Manager can issue a real-time response, such as an alert. For example, a performance rule can monitor CPU usage on an FTP server. If the CPU usage exceeds a threshold you establish, Security Manager can issue an alert.

Sample Performance Data (Measuring Rule)

Measuring rules specify to collect Windows-based performance data for graphs in views, or initiating responses, such as running a script or batch file, or updating a state variable. Sampled performance data is stored in the OnePoint database. **Performance data** are sampled numeric data collected from Windows performance counters.

Measuring rules monitor Windows performance counters and WMI numeric data. You can identify trends by sampling average values. You can view graphs of sampled performance data in the Web Console.

Measuring rules cannot generate alerts. For more information about processing rule responses, see “Working with Processing Rule Responses” on page 122.

Compare Performance Data (Threshold Rule)

Threshold rules compare sampled values, average values, or changes in values to a threshold you supply. Security Manager can use comparative performance data to initiate standard responses, such as running a script or batch file, issuing an SNMP trap, notifying a specified notification group, or updating state variables.

Creating threshold rules allows you to monitor computers for performance thresholds that you define. **Performance thresholds** are limits at which the threshold rule is triggered. Security Manager generates an alert if the threshold is crossed in either direction. You can define responses for threshold rules.

For example, Security Manager provides a performance threshold rule in the Security Manager Self-monitoring module that checks the free disk space on your database server. If the free disk space available falls below 40 percent, Security Manager generates an Error alert to notify you that your database server is becoming full.

Performance Processing Rule Properties

When you review a defined rule, Security Manager displays the rule Properties window. For more information about displaying the properties for a rule, see “Working with Processing Rules” on page 101. The Properties tabs display the rule criteria that you supply when creating processing rules. For more information about entries on each tab, see the Help.

Depending on the performance processing rule, the following tabs may be available:

General

Specifies a name and whether the processing rule is enabled. This tab also provides information about the processing rule description, path, GUID, and last modified date.

Data Provider

Specifies the event or performance data providers name and type. For more information about data providers, see “Understanding Data Providers” on page 89.

Criteria

Specifies the properties to match, such as counter, object, instance, domain, or computer.

You can define some criteria using wildcard characters, regular expressions, or Boolean regular expressions. For more information about wildcard use and Boolean and regular expressions, see the Help.

Schedule

Specifies a schedule to run the processing rule. If no schedule is specified, the processing rule is always active.

Threshold

Specifies the threshold value and matching criteria.

Alert

Specifies whether to generate a real-time alert if a rule match occurs.

Alert Suppression

Specifies whether to suppress duplicate real-time alerts and allows you to select the criteria for the alert to be considered duplicate.

Responses

Specifies response actions to take when a rule match occurs. For more information about processing rule responses, see "Working with Processing Rule Responses" on page 122.

Knowledge Base

Specifies information about the processing rule, such as what caused an alert, how to resolve an issue, or how to configure the processing rule or parameters in a script response.

Understanding Alert Processing Rules

Alert processing rules differ in purpose from event and performance processing rules. Event and performance processing rules act on events or threshold data. Alert rules process the alerts that event and performance processing rules generate.

Alert processing rules define the real-time response Security Manager takes when another rule issues a specified level of alert. For example, an alert rule can specify that when Security Manager issues a Critical level alert from any rule in a specific processing rule group, Security Manager responds by notifying the Network Administrators notification group.

Respond to Alert (Alert Rule) Sources

Alert rules let you define the actions Security Manager should take if an event or performance processing rule generates an alert. You can specify the following properties of the alert on the Alert Criteria tab:

- Alert source, such as a log containing the event
- Specific alert severity
- Alerts from specific processing rule groups
- Other alert matching criteria

Security Manager can use alert rules to initiate real-time responses, such as running a script or batch file, notifying a notification group, issuing SNMP traps, or updating a state variable. For more information about alerts and responses, see "Understanding Alerts and Alert Configuration" on page 33 and "Working with Processing Rule Responses" on page 122.

Alert Rule Properties

When you review a defined rule, Security Manager displays the rule properties window that specifies criteria and the real-time response to initiate when a rule match occurs. For more information about displaying the properties for a rule, see "Viewing Processing Rule Properties" on page 115. The properties tabs display the rule criteria that you supply when creating processing rules. For more information about fields on each tab, see the Help.

The following tabs are available for alert processing rules:

General

Specifies a name and whether the processing rule is enabled. This tab also provides information about the processing rule description, path, GUID, and last modified date.

Alert Criteria

Specifies the source, severity, owner, resolution state, or computer and the processing rule group to which the alert applies.

Schedule

Specifies a schedule to run the processing rule. If no schedule is specified, the processing rule is always active.

Responses

Specifies immediate actions to take when a rule match occurs. For more information about processing rule responses, see “Working with Processing Rule Responses” on page 122.

Knowledge Base

Specifies information you know about the processing rule, such as what caused an alert, how to resolve an issue, or how to configure the processing rule or parameters in a script response.

Understanding Data Providers

An **event** is a significant occurrence in a system or in an application. Security Manager monitors events written to logs or sent by devices, and responds to timed events, missing events, and events generated by scripts.

Security Manager collects event information from a variety of sources called **data providers**. Data providers are sources of collected information. Choose a data provider based on the information you want to Security Manager to collect and the type of rule you want to create.

Event Data Providers

Security Manager collects information from a variety of sources called data providers. Processing rules specify which provider includes the information you want to collect.

Windows Event Logs

Windows computers log events in specific event logs, and Security Manager can collect events from these logs. By default, Security Manager collects events from the Security event log. Security Manager can collect events from the following Windows event logs:

Application
Records events from applications on the computer.

System
Records events from Windows system components.

Security
Records events based on specified Windows security options.

DNS Server
Records events from the Domain Name Service (DNS) server on Windows DNS servers.

File Replication
Records events from the File Replication service on Windows.

Directory Service
Records events from the Active Directory service on Windows.

Application Log Events

Some software applications create their own log files referred to as application log files. Using Security Manager, you can monitor the following application log files or messages:

- Microsoft Internet Information Services, such as World Wide Web or FTP services
- Internet Locator Service
- Any generic single-line log

Note
Security Manager can monitor log files if the applications append entries to the log. If the application you want to monitor periodically overwrites the log file, you can create a script or batch file that monitors the application log and appends the new information to a separate file for Security Manager to monitor.

Timed Events

Security Manager can create **timed events,** events automatically created on a timed basis. For example, you want to test your third-party paging notification software once a day. You can create a processing rule that creates a daily event at 3:00 PM. You can then assign a notification response to page a network administrator, sending a test message. Timed events are not stored in the OnePoint database. Security Manager does not create timed events for agentless monitored computers. For more information about agentless monitored computers, see the *Installation Guide for NetIQ Security Manager.*

WMI Events

Windows Management Instrumentation (WMI) displays Windows management information, such as computer configuration information and events, as a database structure. Security Manager can monitor WMI extrinsic or intrinsic events. Security Manager does not monitor WMI events from agentless monitored computers. For more information about agentless monitored computers, see the *Installation Guide for NetIQ Security Manager.*

Extrinsic events are provided to WMI by other applications. For example, Security Manager can monitor SNMP traps through WMI extrinsic events. An SNMP trap is a packet of information sent by a network device, such as a router or computer, running the Simple Network Management Protocol (SNMP). Devices can send SNMP traps in response to an event, such as a service stopping, or to indicate normal system operation.

Intrinsic events are generated by changes to WMI data, such as configuration changes on a computer. Security Manager can monitor configuration changes, such as the status of services running on a computer using intrinsic WMI events. A WMI event is generated when the state of a service changes such as a change from stopped to started, or running to pausing.

For example, an event processing rule can use a WMI intrinsic event to monitor the Remote Access Service (RAS) on a managed computer. The rule monitors WMI for an event indicating that a RAS session has started. When the event occurs, the event processing rule can generate an alert and a response to this WMI event. For more information about WMI, see “Understanding WMI” on page 167.

Syslog Provider

Systems using syslog can forward syslog messages to another computer, and Security Manager can collect these messages as events. For example, depending on your license, you can collect specific syslog messages from UNIX computers. For more information about creating syslog providers, see “Creating a Data Provider for Syslog” on page 97. For more information, see the module documentation for products you want to monitor.

Performance Data Providers

Security Manager can monitor and graph numeric data from Windows performance counters, WMI, or data generated by scripts. Security Manager collects information from a variety of sources called data providers that allow you to monitor Windows performance objects, such as counters or instances.

Security Manager allows you to monitor Windows performance objects. In Windows, an **object** represents a system resource, such as an application, shared memory, or a type of device. Object types can have **instances**. For example, the Processor object has one instance for each processor on the monitored computer. Some objects do not have instances. Each object type has a unique set of counters that produce statistical information.

You can also monitor WMI numeric properties. In WMI, the **namespace** is a unit for grouping classes and instances. A **class** is the basic unit of management. An **object** is a hardware or software system component represented as an instance of a WMI class, and an instance is the representation of a managed object. The **property** of the object instance contains the numeric value you want to monitor.

When you create performance processing rules, Security Manager can collect information from the following data providers:

Windows performance counter providers

Can provide sampled data from supported Windows environment performance counters.

WMI numeric data providers

Can provide sampled WMI numeric values.

The data provider for alert rules is other Security Manager event or performance processing rules. For more information about alert processing rules, see “Understanding Alert Processing Rules” on page 87.

Security Manager also includes scripting objects you can use to collect performance data. For more information about scripts, see “Understanding Scripts” on page 139.

Performance Measurement

Security Manager can sample and store performance information by sampling numeric data from Windows performance counters or from WMI sources. Collecting and graphing performance data periodically can help identify trends in processor usage or memory usage. This information can help you detect overstressed CPU or memory situations to help you plan for new or upgraded hardware. You can also use another rule to run a script that analyzes the information. The script can then generate events or issue alerts depending on its results.

For more examples, review the built-in performance measuring rules. Search for performance rules and select a measuring rule to review. For more information about how to search for processing rules, see “Working with Processing Rules” on page 101.

Performance Thresholds

Security Manager can sample performance information by sampling numeric data from Windows performance counters or from WMI sources. Performance processing rules that collect this data can monitor computers and applications for performance thresholds or tolerances. When the data is outside the threshold tolerance, the rule can generate a response.

For example, you can create a rule that checks the amount of memory currently in use by a process. If you detect a growing amount of memory use, it may indicate that an application has a memory leak. Using a timed performance rule, you can observe the memory usage data periodically. If the memory use exceeds the threshold you specify, indicating an extreme load on the server, the rule could issue an alert to operators who can then investigate, or run a script to bounce the service.

For more examples, review the built-in performance threshold rules. Search for performance rules and select a threshold rule to review. Double-click the rule to display the Properties window. For more information about how to search for processing rules, see “Working with Processing Rules” on page 101.

Working with Data Providers

The following topics provide step-by-step guidance for data provider tasks.

Creating a Data Provider

If Security Manager does not provide a data provider you need, you can create one. After you create the data provider, you can specify the new data provider in processing rules to collect information.

To create a data provider:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console > Advanced**.
4. In the left pane, click **Providers**.
5. On the Action menu, click **New > Provider**.
6. Select the type of provider you want to create and click **Next**.
7. Follow the instructions until you have finished creating a new data provider. For more information about the fields on a window, see the Help.

Creating a Data Provider for a Generic Single-line Text Log

You can create a data provider for a generic single-line text log based on the application log data provider. The application log data provider provides a mechanism to parse logs using the following methods:

- Delimiter-based parsing
- Regular expression-based parsing

When you create an application log data provider, you can identify field delimiters, such as the comma (,), used to separate parameters in the log file. Specifying field delimiters allows Security Manager to retrieve individual parameters from a single-line application log file.

Note
The application log data provider can collect data only from text logs encoded using the ASCII character encoding standard. The application log data provider cannot collect data encoded using the Unicode character-encoding standard.

To create a data provider for a generic single-line log file:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console > Advanced**.
4. In the left pane, click **Providers**.
5. On the Action menu, click **New > Provider**.
6. On the Select Data Provider Type window, click **Application Log** and then click **Next**.
7. On the Log Type window, select **Generic single-line log file,** and then click **Next**.
8. On the Directories window, click **Add**.
9. On the Directory Edit window, specify the command location, format, and file name, and then click **Next**. The file name provides Security Manager with the file name convention for each generated log file. For example, an application may include a sequential number in its log file names, such as `error*.log.` For more information about window options, see the Help.
10. ***If you want to specify parsing instructions***, complete the following steps:
    a. On the Parsing window, select **Enable Parsing**.

    b. ***If you want to specify delimiter-based parsing instructions,*** select Use basic parsing instructions, and then complete the appropriate delimiter and log file parameter information. For more information about window options, see the Help.

    c. ***If you want to specify regular expression-based parsing,*** select Use XML parsing instructions, and then click Configure XML. For more information, contact NetIQ Professional Services.
11. Click **Next**.
12. On the Name window, specify a provider name and then click **Finish**.

Creating a Data Provider for Syslog

When you create a data provider for syslog, you can secure the syslog event data by limiting the IP addresses from which a proxy agent accepts syslog events.

You can also provide parsing instructions using regular expressions in XML format. For more information about configuring an XML file to provide regular expression-based parsing, see the *Syslog Provider Parse Map Structure and Usage Technical Reference*, located on the NetIQ Support site for Security Manager at www.netiq.com/support/sm, or contact NetIQ Professional Services.

Notes

- If you are creating a data provider for syslog, ensure each application or device sends syslog events to a unique agent.
- You cannot create log archival filter rules to filter syslog data sent by a syslog provider. You can create log archival collection rules for syslog data, but the syslog provider ignores any criteria specified. If you want to filter syslog data or collect only specific events, you must configure the parse map for your syslog provider to process syslog data.
- The syslog provider currently only supports transmission of syslog messages over UDP, not TCP.

To create a data provider for syslog:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console > Advanced**.
4. In the left pane, click **Providers**.
5. On the Action menu, click **New > Provider**.
6. On the Select Data Provider Type window, click **Syslog** and then click **Next**.

7. On the Syslog Provider Properties - Configuration window, specify a name for the new provider.

8. Specify the port number. Syslog uses port 514, by default.

9. ***If you want to specify parsing instructions,*** complete the following steps:

    a. Select **Enable Parsing**, and then click **Configure XML**.

    Note
    The **Enable Catch All** feature, which is selected by default, does not apply to real-time events. If you attempt to use this feature for real-time events, the syslog provider does not capture any results.

    b. Enter the XML parsing instructions, and then click **OK**. For more information, contact NetIQ Professional Services.

10. ***If you do not want to specify parsing instructions,*** click **Next**.

11. ***If you want to specify authorized syslog source IP addresses,*** complete the following steps:

    a. Select the **Only accept syslog data from specified computers** check box, and then click **Add**.

    b. Type the IP address, and then specify a computer name or alias.

    Note
    You cannot add a computer from which Security Manager already receives syslog data. Computer names or aliases cannot contain spaces or the following characters: ` ~!@#$^&*()=+[]{}\\|;:\'\",.<>/?.

    c. Click **OK**.

12. ***If you want to import authorized syslog source IP addresses from a file,*** complete the following steps:

    a. Use a text editor to create a file containing the IP addresses and their respective computer names or alisases. Use the following format:

    ```
    0.0.0.1;computer1
    ```

```
0.0.0.2;computer2
0.0.0.3;computer3
```

b. Save the file.

c. Select the **Only accept syslog data from specified computers** check box, and then click **Import**.

d. Browse to the text file containing the IP addresses and their respective computer names or alisases.

e. Click **Open**.

13. Click **Finish**.

Modifying Data Provider Properties

You can modify properties for most data providers. You cannot modify some predefined providers.

To modify data provider properties:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console > Advanced**.
4. Click **Providers**.
5. In the right pane, click the data provider with properties you want to modify.
6. On the Action menu, click **Properties**.
7. Specify the appropriate values. For more information about a field on a window, see the Help.
8. Click **OK**.

Copying a Data Provider

You can copy a provider, paste it, and modify its properties to create a new provider. You can copy and paste a provider within the current Development Console or into a Development Console for another configuration group.

You cannot copy Windows event providers or generic providers.

To copy a provider:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console > Advanced**.
4. Click **Providers**.
5. In the right pane, click the provider you want to copy.
6. On the Action menu, click **Copy**.
7. In the left pane, click **Providers**. You can paste a provider only into a Providers folder in a Development Console.
8. On the Action menu, click **Paste**.

Understanding Processing Rule Matches

When you create most processing rules, you define how Security Manager collects, handles, and responds to specified information. When Security Manager then receives information that matches a processing rule, a **processing rule match** occurs.

When a processing rule match occurs, Security Manager performs the action specified by the processing rule, and any **response** that might be defined defined in that rule, as well. For example, an event rule can save the event to the OnePoint database, generate an alert, and send an email to a response team member.

Security Manager saves most real-time event information matching a processing rule in the OnePoint database unless you specify otherwise. For example, if you create an event rule that generates an alert for a specified event, Security Manager stores the event and the alert in the OnePoint database. However, you can create filtering rules that specify real-time events that you do not want Security Manager to process or store. For more information about filtering events, see "Filter Event (Filtering Rules)" on page 80.

Security Manager saves all archival event information matching a log collection rule and stores it in the log archive unless you specify otherwise. You can filter archival event data using log filter rules. For more information about log collection rules, see "Collect Logs for Archival (Log Collection Rule)" on page 82.

You can monitor the collected real-time events and alerts using the Control Center and the Web Console. You can also create Forensic Analysis reports from the collected archival events using the Control Center. For more information about using the Control Center and Web Console, see the *User Guide for NetIQ Security Manager*.

Depending on which type of processing rule you create, the rule provides an implicit action, such as collecting an event, generating an alert, or storing the data. For more information about responses that Security Manager can carry out when a processing rule match occurs, see "Working with Processing Rule Responses" on page 122.

Working with Processing Rules

When you create a processing rule, you specify a variety of information including the data source (data provider) and the response to take when a rule match occurs. The following topics provide step-by-step guidance for processing rule tasks.

Note
You can also use the Security Manager Control Center to create basic event processing and filtering rules based on specific real-time events. For more information about creating rules using the Control Center, see the *User Guide for NetIQ Security Manager*.

Alerting on or Responding to an Event

Security Manager can generate an alert or run a response in real-time for specified events. You can create event rules when certain events are not covered in other processing rules. For more information about event responses and alerts, see “Alert on or Respond to Event (Event Rule)” on page 79.

To alert on or respond to an event:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.
4. Expand the processing rule group to which you want to add an event processing rule.
5. Click **Event Processing Rules**.
6. On the Action menu, click **Create Real-Time Rules > Alert on or Respond to Event**.
7. Follow the instructions until you have finished creating the processing rule. For more information about the fields on a window, see the Help.

Filtering a Real-Time Event

Security Manager can ignore specified real-time events. Filtering rules typically identify events that you do not consider significant. For more information about event filtering, see “Filter Event (Filtering Rules)” on page 80.

To filter a real-time event:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console** > **Processing Rule Groups**.
4. Expand the processing rule group to which you want to add an event processing rule.
5. Click **Event Processing Rules**.
6. On the Action menu, click **Create Real-Time Rules > Filter Event**.
7. Follow the instructions until you have finished creating the processing rule. For more information about the fields on a window, see the Help.

Detecting a Missing Event

Security Manager can generate an alert or a response when particular real-time events do not occur during a specified time. For more information about detecting missing events, see “Detect Missing Event (Missing Event Rule)” on page 81.

To detect a missing event:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console** > **Processing Rule Groups**.
4. Expand the processing rule group to which you want to add an event processing rule.
5. Click **Event Processing Rules**.

6. On the Action menu, click **Create Real-Time Rules > Detect Missing Event**.
7. Follow the instructions until you have finished creating the processing rule. For more information about the fields on a window, see the Help.

Consolidating Similar Events

Security Manager can group multiple similar real-time events on a Windows agent computer into a single summary event. For more information about event consolidation, see “Consolidate Similar Events (Consolidation Rule)” on page 81.

To consolidate similar events:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console** > **Processing Rule Groups**.
4. Expand the processing rule group to which you want to add an event processing rule.
5. Click **Event Processing Rules**.
6. On the Action menu, click **Create Real-Time Rules > Consolidate Similar Events**.
7. Follow the instructions until you have finished creating the processing rule. For more information about the fields on a window, see the Help.

Collecting Specific Events

Security Manager can identify real-time events with specific criteria to collect from specific sources. Collection rules do not provide responses or generate alerts. For more information about event collection, see “Collect Specific Events (Collection Rule)” on page 82.

Security Manager stores real-time events matching this processing rule in the OnePoint database.

To collect specific events:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.
4. Expand the processing rule group to which you want to add an event processing rule.
5. Click **Event Processing Rules**.
6. On the Action menu, click **Create Real-Time Rules > Collect Specific Events**.
7. Follow the instructions until you have finished creating an event processing rule. For more information about the fields on a window, see the Help.

Correlating Specific Events

You can use the Correlation Wizard to specify criteria with which to analyze real-time events and identify patterns. The Correlation Wizard allows you to create a correlation rule that contains the criteria and specifies the alert response. For more information about event correlation, see “Correlate Events (Correlation Rule)” on page 82.

You can specify events to correlate in different ways:

- You can select the events or alerts to correlate in a view, and then launch the Correlation Wizard with the event criteria in the correlation rule criteria. For more information about correlating events in a view, see the Help.
- You can define the event criteria using the Correlation Wizard. Consider using this option only if Security Manager is not already configured to detect the event you want to correlate. Otherwise, you should select the event based on views or rules that contain matching event criteria.

To correlate specific events or alerts:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Users group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders** and navigate to the appropriate view.
4. In the Results window, click the event or alert to correlate. You can use the `Ctrl` or `Shift` keys to select multiple events or alerts.
5. ***If correlating a specific event,*** click **Event Tasks > Correlate Events** on the Tasks menu.
6. ***If correlating events generating a specific alert,*** click **Alert Tasks > Correlate Alerts** on the Tasks menu.
7. In the left pane of the Correlation Wizard, click **Events**.
8. ***If you want to add an event to correlate from an existing view or correlation rule:***
    a. Click **Add Events**.
    b. Click the underlined text next to the Look in field, then select or browse to the view or correlation rule containing the event or alert to correlate.
    c. In the top pane, select the events, alerts, or processing rules containing the event criteria you want to add to the correlation rule criteria.
    d. Click **Add Selected**.
9. ***If you want to add an event to correlate that is not in a view or a processing rule,***
    a. Click **Add Events**.
    b. Click **Add New**.

c. Specify the event criteria Security Manager can use to detect the event and a name to identify the event.

Note
By default, correlation rules do not consider case when evaluating data against "contains," wildcard, or regular expression rule criteria. If you want a "contains," wildcard, or regular expression correlation rule criterion to match the case of a specified value, select **Match Case**.

d. Click **Add**.

10. Click **OK**.

11. Complete the wizard to correlate events.

12. Click **Finish** to save the correlation rule.

Note
After you create a correlation rule, you can view or modify the properties for the new rule in the Development Console.

Correlating a Set of Events

Using the Correlation Wizard, you can create a correlation rule based on a **set** of events. A set is a stream of real-time events occurring in any order. However, the event criteria, common fields, or the time frame in which the events occur determine the importance of the correlated condition.

To correlate a set of events, add the events or event criteria to the correlation rule criteria. You do not need to specify order or a repeat count. For more information about event correlation, see "Correlating Specific Events" on page 105.

Correlating a Sequence of Events

Using the Correlation Wizard, you can create a correlation rule based on a **sequence** of events. A sequence is a set of real-time events occurring in a particular order. For example, a remote logon is attempted, and then someone initiates a mass file transfer of sensitive files. If the remote logon did not occur first, the file transfer may have seemed unimportant.

To correlate a sequence of events:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Specify the events to correlate. For more information about event correlation, see "Correlating Specific Events" on page 105.
4. In the left pane of the Correlation Wizard, click **Order**.
5. In the right pane, click **Order Events**.
6. Specify the order in which the events must occur, and then click **OK**.
7. ***If you want two or more of the events to occur in any order to cause a rule match***, click the underlined text between the events, and then click **and**.

   This connector allows you to apply ordering criteria to a set of events, rather than to the individual events.

8. ***If you want either one event or another event to occur to cause a rule match***, click the underlined text between the events, and then click **or**.

   This connector allows you to apply ordering criteria to a sequence of events where one of the positions may be filled by either one or another specific event.

9. Complete the wizard to correlate a sequence of events.
10. Click **Finish** to save the correlation rule.

Correlating Repeating Events

When the number of times an event occurs is important, use the Correlation Wizard to correlate a repeating event. A repeating event can indicate attempts to obtain access. For example, multiple attempts to logon to the financial database using the same user account could signify a threat.

To correlate repeating events:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Specify the events to correlate. For more information about event correlation, see "Correlating Specific Events" on page 105.
4. On the Events window in the Correlation Wizard, click the event you want to repeat.
5. Click **Must Repeat**, and then select the number of times the event must repeat. You can select **Custom** to specify a value not in the list.
6. Complete the wizard to correlate repeating events.
7. Click **Finish** to save the correlation rule.

Mapping Common Fields for Correlation

A field is a location of an event property, such as the computer name where an event originated. You can specify a **common field** whose property must match for all events in the correlation rule criteria. Events that Security Manager is configured to detect typically contain properties that are mapped to a named field. Otherwise, Security Manager identifies event properties by parameter location, such as parameter 7.

If the property you want to match is stored in a different field for a certain event, you can map the property to that field. For example, if you want to correlate events that have matching IP addresses, but for some events the IP address is stored in the source address field and for another event this property is stored in the target address field, you can map the property for that event to the target address field.

You can also map fields if the property is not already mapped to a named field. You can identify the property you want to match by mapping it to a parameter. For example, Security Manager does not map all parameters for some third party applications that write events to the Windows Application log. You can map the event property to the parameter number that identifies the location of the property.

You can view event properties in the Control Center. For more information about viewing event properties, see the Help. However, Security Manager is not always configured to store all event parameters, and you may not be able to see this information. To see raw log data for an event, you can run a Forensic Analysis query. For more information about Forensic Analysis queries, see the *User Guide for NetIQ Security Manager* and the Help.

To map event properties to fields:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Specify the events to correlate. For more information about event correlation, see "Correlating Specific Events" on page 105.
4. On the Common Fields window in the Correlation Wizard, click **Map Fields**.
5. Map each field that stores the value you want to match in a different location by completing the following steps:
   a. In the top pane, click the event.
   b. In the bottom pane, click the field.
   c. Repeat Steps **a** through **b** until you have finished mapping each event.

6. Complete the wizard to correlate repeating events.

7. Click **Finish** to save the correlation rule.

Collecting Logs for Archival

Security Manager can use log collection rules to identify and collect events for archival and reporting. Log collection rules do not provide responses or generate alerts. For more information about collecting logs, see "Collect Logs for Archival (Log Collection Rule)" on page 82.

Security Manager stores events matching this processing rule in a log archive partition.

To collect events for archival:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*

2. Start the **Development Console** in the NetIQ Security Manager Program group.

3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.

4. Expand the processing rule group to which you want to add an event processing rule.

5. Click **Event Processing Rules**.

6. On the Action menu, click **Create Archival Rules > Collect Logs for Archival**.

7. Follow the instructions until you have finished creating an event processing rule. For more information about the fields on a window, see the Help.

Filtering Archival Events

Security Manager can use log filter rules to reduce the amount of data collected and stored in the log archive. Log filter rules allow you to filter events that you have determined are too noisy or unimportant. Security Manager neither collects these events nor includes them in reports. For more information about filtering events, see “Filter Archival Event (Log Filter Rule)” on page 83.

To filter archival events:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.
4. Expand the processing rule group to which you want to add an event processing rule.
5. Click **Event Processing Rules**.
6. On the Action menu, click **Create Archival Rules > Filter Archival Event**.
7. Follow the instructions until you have finished creating an event processing rule. For more information about the fields on a window, see the Help.

Sampling Performance Data

Security Manager can collect a numeric value from Windows or WMI performance counters. For more information about measuring rules, see “Sample Performance Data (Measuring Rule)” on page 85.

To sample performance data:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console** > **Processing Rule Groups**.
4. Expand the processing rule group to which you want to add a performance processing rule.
5. Click **Performance Processing Rules**.
6. On the Action menu, click **Sample Performance Data.**
7. Follow the instructions until you have finished creating a performance processing rule. For more information about the fields on a window, see the Help.

Comparing Performance Data

Security Manager can generate a real-time alert when a Windows performance counter value crosses a defined threshold in either direction. Threshold rules can also define a response. For more information about threshold rules, see “Compare Performance Data (Threshold Rule)” on page 86.

To compare performance data:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console** > **Processing Rule Groups**.
4. Expand the processing rule group to which you want to add a performance processing rule.

5. Click **Performance Processing Rules**.
6. On the Action menu, click **Compare Performance Data.**
7. Follow the instructions until you have finished creating a performance processing rule. For more information about the fields on a window, see the Help.

Creating an Alert Processing Rule

An alert processing rule allows you to specify a real-time response for an alert or for a number of previously defined alerts.

To create an alert processing rule:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.
4. Expand the processing rule group to which you want to add an alert processing rule.
5. Click the **Alert Processing Rules** folder.
6. On the Action menu, click **Respond to Alert**.
7. Follow the instructions until you have finished creating an alert processing rule. For more information about the fields on a window, see the Help.

Viewing Processing Rule Properties

You can review processing rule properties to examine property pages for the rule and make modifications.

Note
You view limited properties for correlation rules. If you want to modify correlation rule properties, use the **Edit** menu option. For more information about modifying rule properties, see “Modifying Processing Rule Properties” on page 115.

To view processing rule properties:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console** > **Processing Rule Groups**.
4. Expand the processing rule group that contains the processing rule you want to view.
5. Click the Event, Alert, or Performance Processing Rules folder that contains the processing rule you want to view.
6. In the right pane, click the processing rule you want to view.
7. On the Action menu, click **Properties**.

Modifying Processing Rule Properties

Several tabs on the Properties window provide rule components. Depending on the type of rule you examine, the Properties window provides different tabs.

To modify a processing rule:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups.**
4. Expand the parent-level processing rule group you want to modify.
5. Expand the child-level processing rule group you want to modify.
6. Select the Event, Alert, or Performance Processing Rules folder.
7. In the right pane, select the rule you want to modify.
8. On the Action menu, click **Edit**.
9. Select the tab containing the rule properties you want to modify. For more information about entries on the tab, see the Help.
10. When you are finished modifying the rule, click **OK**.

Finding a Processing Rule

Finding the processing rule you want to modify or review can be a challenge if you do not know where it is stored in the processing rule group hierarchy. You can search processing rule groups to locate the processing rule you want.

Security Manager allows you to specify detailed search criteria for each processing rule type. The following examples demonstrate criteria you can specify for event, alert, and performance processing rules:

- Find an event processing rule based on a specified event ID number.
- Find an alert processing rule based on the Windows security log that generates a warning.
- Find a performance processing rule that samples data from a specified counter.

The available criteria change based on the processing rule type you specify for your search. For best results, carefully examine search criteria and specify only the criteria that apply to your search.

To find a specific rule or set of processing rules:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.
4. Select any processing rule folder.
5. On the Action menu, click **Find processing rules**.
6. Specify the search criteria to locate the processing rule you want. You can broaden or narrow the criteria to help you find the rules you want.
7. Click **Next** until you have finished specifying the search criteria.
8. Click **Finish**. Security Manager displays the results of the rule search in a new window.

Reviewing Previous Rule Search Results

Security Manager saves rule search results. Access previous search results using the Development Console.

To review results of a previous rule search:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager Program group.

3. In the left pane, expand **Security Manager Development Console > Search Results > Processing Rule Search Results.**
4. Select a **Rule Search** results folder. Security Manager displays the search results in the right pane.

Copying a Processing Rule

You can copy a processing rule in one processing rule group and paste it within another. You can copy a processing rule and modify its properties to create a new processing rule. You can copy and paste a processing rule within a single Development Console or into a Development Console for another configuration group.

Notes

- You can paste a processing rule only within a folder containing its type of rule: Event, Alert, or Performance Processing Rules.
- In some instances, you might need to refresh the view to see the rule pasted in the new location.
- If you copy and paste a processing rule that includes a criterion with the **Match case** option selected, the new copy of the rule retains the case-sensitive value you specified for the criterion.

To copy a processing rule:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console** > **Processing Rule Groups**.
4. Expand the processing rule group containing the processing rule you want to copy.
5. Click the Event, Alert, or Performance Processing Rules node containing the rule you want to copy.

6. In the right pane, click the rule that you want to copy.
7. On the Action menu, click **Copy**.
8. In the left pane, click the Event, Alert, or Performance Processing Rules node where you want to paste the rule.
9. On the Action menu, click **Paste**.

Disabling a Processing Rule

You can disable a processing rule to temporarily stop it from being evaluated on the Windows agent computers in the computer group associated with the processing rule group.

Note
If you disable a correlation rule, Security Manager also disables any correlation collection rules associated with that correlation rule.

To disable a processing rule:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console** > **Processing Rule Groups**.
4. Expand the processing rule group that contains the processing rule you want to disable.
5. Click the Event, Alert, or Performance Processing Rules folder that contains the processing rule you want to disable.
6. In the right pane, click the processing rule you want to disable.
7. On the Action menu, click **Properties**.

8. Clear the **Enabled** check box.
9. Click **OK**.

Deleting a Processing Rule

If a processing rule is no longer required, you can delete it.

Note
Deleting a correlation rule also deletes the associated correlation collection rule.

To delete a processing rule:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.
4. Expand the processing rule group containing the processing rule you want to delete.
5. Click the Event, Alert, or Performance Processing Rules node containing the rule you want to delete.
6. In the right pane, click the rule that you want to delete.
7. On the Action menu, click **Delete**.
8. Click **Yes**.

Forcing Processing Rule Changes

You can force Security Manager to update Windows agents with new or modified processing rules, or you can wait for Security Manager to automatically update the Windows agents. By default, the central computer checks for new processing rules every 5 minutes. Windows agents contact the central computer every 5 minutes (300 seconds), by default, which is called the agent **heartbeat**. After the central computer discovers new processing rules and the Windows agent heartbeat occurs, the central computer sends the new processing rules to the Windows agent computer. This process can take up to 10 minutes.

While you are developing processing rules, you may want to frequently update the Windows agents with the new rules. You can modify how often the central computer checks for new processing rules and how often the Windows agent sends a heartbeat using Global Settings in the Configuration snap-in. For more information about configuring Global Settings, see the *User Guide for NetIQ Security Manager*.

You can also force the central computer to update the Windows agents with rule changes. The central computer sends the new or modified processing rules at the next heartbeat, shortening the overall length of time this process occurs to no more than 5 minutes.

To force processing rule changes:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, select **Security Manager Development Console**.
4. On the Action menu, click **Force Configuration Changes Now**.

5. Select the central computer with agents you want to update, and then click **OK**.
6. ***If Security Manager displays a confirmation window***, click **Close**.

Note
Forcing configuration changes distributes processing rules changes only to Windows computers with agents already installed. For more information about installing agents, see the Help.

Working with Processing Rule Responses

You typically specify a response when creating a processing rule. The response criteria is included in the processing rule properties. You can specify the response defaults, which automatically include information about the alert or event, or you can customize the alert or event response. The following topics provide step-by-step guidance for configuring processing rule responses.

Creating Notification Groups

If a processing rule contains an email or page as a response, identify a notification group to receive the notification. Notification groups are containers that include operators who are recipients of the email, paging, or command notifications that Security Manager processing rules generate.

To create a notification group:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console > Configuration**.
4. Click **Notification Groups**.

5. On the Action menu, click **Create Notification Group**.
6. Type an appropriate name for the notification group.
7. Click **Finish** on the Notification Group Properties window.

It is a good practice to identify the notification groups that a processing rule group or processing rule notifies when you create the processing rule. You can add this information in the Knowledge Base associated with the processing rule group. You may also want to instruct users to add operators to this group if they want to be notified about the event. For more information about adding operators to notification groups, see the Help.

Adding a Notification Response

You can add a notification response to any processing rule that generates an alert. Notification responses define who is notified in response to an alert.

For more information about notification responses, see the *User Guide for NetIQ Security Manager.*

To add a notification response to a rule:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console**.
4. Browse to the processing rule group that contains the processing rule you want to modify.
5. In the right pane, click the processing rule to which you want to add a response.
6. On the Action menu, click **Properties**.
7. On the Responses tab, click **Add** and then select **Send a notification to a notification group**.

8. On the notification tab, specify the notification group.

Notes

- You can also customize the response format for an email, page, or command response. For more information about modifying responses, see “Customizing Notification Responses” on page 130.
- You can define the type and schedule of the notification in the properties for each operator.

9. Click **OK**.

Adding a Script Response

You can add a script response to any of the following rule types:

- Event rules
- Missing event rules
- Filtering rules (except pre-filters)
- Alert rules
- Measuring rules
- Threshold rules

For more information about scripts, see “Understanding Scripts” on page 139.

To add a script response to a rule:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console**.
4. Expand the processing rule group that contains the processing rule you want to modify.

5. In the right pane, click the processing rule to which you want to add a response.
6. On the Action menu, click **Properties**.
7. On the Responses tab, click **Add** and then select **Launch a script**.
8. On the Launch a Script window, specify the script name, where to run it, and the script parameters.
9. Click **OK**.

Adding a State Variable Response

You can update a state variable for any of the following rule types:

- Event rules
- Missing event rules
- Filtering rules (except pre-filters)
- Alert rules
- Measuring rules
- Threshold rules

For more information about state variables, see the *User Guide for NetIQ Security Manager*.

To add a state variable response to a rule:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console**.
4. Expand the processing rule group that contains the processing rule you want to modify.
5. In the right pane, click the processing rule to which you want to add a response.

6. On the Action menu, click **Properties**.
7. On the Responses tab, click **Add** and then select **Update state variable**.
8. On the State Variable Update window, specify the state variable and where to perform the update.
9. Click **OK**.

Adding a Command or Batch File Response

You can add a command or batch file response to any of the following rule types:

- Event rules
- Missing event rules
- Filtering rules (except pre-filters)
- Alert rules
- Measuring rules
- Threshold rules

For more information about command or batch file responses, see the *User Guide for NetIQ Security Manager*.

To add a command or batch file response to a rule:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console**.
4. Expand the processing rule group that contains the processing rule you want to modify.
5. In the right pane, click the processing rule to which you want to add a response.
6. On the Action menu, click **Properties**.

7. On the Responses tab, click **Add** and then select **Execute a command or batch file**.
8. In the Command Wizard, specify the command or batch file to run and required parameters, and any other appropriate information.
9. Click **OK**.

Adding an SNMP Trap Response

You can add an SNMP trap response to alert processing rules and any rule that generates an alert. You can configure Security Manager to generate an SNMP trap when a processing rule match occurs.

For more information about SNMP trap responses, see the *User Guide for NetIQ Security Manager*. For more information about configuring Security Manager support for SNMP, see “Providing Support for SNMP” on page 157.

To add an SNMP response to a rule:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console**.
4. Expand the processing rule group that contains the processing rule you want to modify.
5. In the right pane, click the processing rule to which you want to add a response.
6. On the Action menu, click **Properties**.
7. On the Responses tab, click **Add** and then select **Send an SNMP trap**.
8. On the SNMP Response Editor window, specify where to generate the trap.
9. Click **OK**.

Customizing Security Manager for Modem Paging

Security Manager provides a built-in paging notification option. You can send a paging notification using either SMTP or a modem. For more information about paging, see the *User Guide for NetIQ Security Manager*.

Security Manager provides the `ModemPage.vbs` script for sending paging notifications using a modem. Complete the following tasks to configure modem paging:

- Configuring Hardware for Modem Paging
- Configuring the Modem Paging Script

When you complete the configuration tasks, send a page to test your configuration.

Configuring Hardware for Modem Paging

Ensure you setup the appropriate hardware and Security Manager options for modem paging.

To set up the hardware and Security Manager for modem paging:

1. Ensure you have valid accounts with a third-party modem paging service provider.
2. Connect the modem to the central computer and configure it. Ensure that the modem is functioning. Use HyperTerminal to check modem functionality.
3. Modify the processing rules you want to send a modem paging response. Choose the **Send a Notification to a Notification Group** response, and type the following example custom command on the Command Format tab:

```
cscript.exe ModemPage.vbs /SEND $Operator ID$ $SeverityNum$
"Security Manager Alert: $Description$"
```

Note

The *`$SeverityNum$`* variable is available only for alert processing rules. For an event or performance threshold processing rule, use a hard-coded priority number or leave the field blank to use the default priority.

4. Ensure that the necessary operators have an Operator ID from the third-party paging service provider. To receive a modem page, ensure the operators within the notification groups associated with the processing rules have a paging service Operator ID specified in the operator properties.

Configuring the Modem Paging Script

Security Manager provides the `ModemPage.vbs` script for sending pages to a modem. Customize the script for your enterprise before you use it to page a modem.

To configure the modem paging script, complete the following steps on the central computer:

1. At the command prompt, type the following command:

   ```
   cd /d "C:\Program Files\NetIQ Security Manager\OnePoint"
   ```

2. At the command prompt, type the following command:

   ```
   cscript ModemPage.vbs /CONFIGURE
   ```

3. ***If you are prompted to enter your country and area code,*** do so and click **OK**.
4. On the Dial Parameter and Modem Device tab, select the correct modem or click **Add New** and follow the instructions to add a modem.
5. On the Defined Services tab, click **From File**.
6. Select **Services.inf** in the `C:\Program Files\NetIQ Security Manager\OnePoint` folder and click **Open**.
7. ***If the service provider you want to install is listed,*** select the service provider and click **OK**.

8. ***If the service provider you want to install is not listed,*** click **Cancel** and complete the following steps:

   a. Click **New** and follow the wizard instructions to specify the provider information. For more information about the fields on a window, see the Help.

   b. Make a note of the exact spelling of the service provider name.

   c. When complete, click **Finish**.

9. On the Send Options tab, enable the options your service requires.

10. Click **OK**.

11. Type the following command at the command prompt, where *`Serviceprovider`* is the name of your paging service provider.
    The `/SETPROVIDER` switch is required.

    ```
    cscript ModemPage.vbs /SETPROVIDER "Serviceprovider"
    ```

12. ***If you want to send a test page,*** type the following command replacing *`OperatorID`*, *`Priority`*, and *`Messagetext`* with the appropriate information:

    ```
    cscript ModemPage.vbs /SEND OperatorID [Priority] Messagetext
    ```

13. When the test page is successful, type `Exit` to close the command window.

Note
Pages with higher priority are sent before lower priority-numbered pages.

Customizing Notification Responses

When an event or alert occurs, you can notify operators in a notification group. Specify notification groups when you create a response for a rule.

The Development Console also allows you to customize a response to an alert or event. When you customize an alert or event, you specify the parameters or text substrings to display in the response.

You can customize the following alert responses to notification groups:

Email notifications

Customize the parameters and text in the email subject line or message. For more information about email notifications, see the *User Guide for NetIQ Security Manager*.

Paging notifications

Customize the parameters and text in the page subject line or message. For more information about paging notifications that use SMTP, see the *User Guide for NetIQ Security Manager*.

Command (page) notifications

Specify the command you wan to run and the appropriate parameters. This command is typically used to trigger a paging application for environments that do not use an SMTP paging service. For more information about paging notifications that use a modem or otherwise cannot use SMTP, see the *User Guide for NetIQ Security Manager*.

When you select a parameter, Security Manager displays the field name in the appropriate text box surrounded by dollar sign characters ($). For example, the **Description** parameter is displayed as `$Description$`. If you want to specify a text substring in the response, type the text in the appropriate text box before or after the specified parameters.

To specify a parameter or substring in a notification to a notification group:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.
4. Expand the processing rule group to which you want to add an alert processing rule.
5. Click **Alert Processing Rules** in the left pane.
6. On the Action menu, click **Respond to Alert**.

7. Follow the instructions until you reach the Responses tab. For more information about the fields on a window, see the Help.

8. On the Responses tab, click **Add > Send a notification to a notification group**.

9. On the Notification tab, specify the notification group on the **Notification group** list.

10. ***If you are customizing an email notification***, click the Email Format tab and specify the appropriate parameters and substrings in the **Custom email format** field.

11. ***If you are customizing a page notification***, click the Page Format tab and specify the appropriate parameters and substrings in the **Custom page format** field.

12. ***If you are customizing a command notification***, click the Command Format tab and specify the appropriate parameters and substrings in the **Custom command** field.

13. Click **OK**.

Specifying a Parameter or Substring in a Command

The Development Console allows you to run a command with specified parameters as part of an alert or event response. Security Manager provides default parameters, such as computer name and event ID. You can also create new parameters.

To specify a parameter or substring in a command:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*

2. Start the **Development Console** in the NetIQ Security Manager Program group.

3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups.**

4. Expand the processing rule group to which you want to add an alert processing rule.

5. ***If you are responding to an event,*** complete the following steps:

   a. Click **Event Processing Rules** in the left pane.

   b. On the Action menu, click **Alert on or Respond to Event.**

6. ***If you are responding to an alert,*** complete the following steps:

   a. Click **Alert Processing Rules** in the left pane.

   b. On the Action menu, click **Respond to Alert**.

7. Follow the instructions until you reach the Responses tab. For more information about the fields on a window, see the Help.

8. On the Responses tab, click **Add > Execute a command or batch file**.

9. In the **Command** field, type the command response, including the event property variable and substring number. You can also select a variable from the list to the right of the field.

10. Type the initial directory in the **Initial Directory** field.

11. Specify whether you want to run the command locally or centrally.

    Note
    If you specify to run the command locally on the Windows agent computer, ensure the command is stored on the Windows agent computer.

12. Click **OK**.

13. Follow the instructions to finish creating the processing rule. For more information about the fields on a window, see the Help.

Storing a Parameter or Substring in a State Variable

When an alert or event occurs, such as a login failure, you can store information about the alert or event in a state variable. You can retrieve information stored in a state variable using a script. For example, you could record time and user ID to unique state variables for each failed login. A timed script that runs every five minutes could retrieve and analyze the state variable information. If the same user fails more than a specified number of times in five minutes, the script could initiate a response.

To specify a variable or substring in a state variable:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.
4. Expand the processing rule group to which you want to add an alert processing rule.
5. ***If you are responding to an event***, complete the following steps:
    a. Click **Event Processing Rules** in the left pane.

    b. On the Action menu, click **Alert on or Respond to Event**.
6. ***If you are responding to an alert***, complete the following steps:
    a. Click **Alert Processing Rules** in the left pane.

    b. On the Action menu, click **Respond to Alert**.
7. Follow the instructions until the wizard displays the Responses tab. For more information about the fields on a window, see the Help.
8. On the Responses tab, click **Add > Update a state variable**.
9. Under **Perform the operation,** specify to update the state variable locally or centrally.
10. Click **Add**.

11. In the **Operation** list, select the operation to perform.

12. In the **State variable name** field, type the state response, including the event property variable and word substring number. You can also select variables from the list to the right of the field.

13. Click **OK**.

14. Click **OK**.

15. Follow the instructions to finish creating the processing rule. For more information about the fields on a window, see the Help.

Exporting a Custom Module

Modules contain computer groups, processing rules, and views, as well as other information. When you create a custom module you can export the module. Exporting a module allows you to back up your customizations or use the custom module in another configuration group.

To export a custom module:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.

2. Start the **Development Console** in the NetIQ Security Manager program folder.

3. In the left pane, expand **Security Manager Development Console**.

4. Click **Processing Rule Groups**.

5. Click the processing rule group containing the rules you want to export.

6. On the Action menu, click **Export Custom Module**.

7. Specify the appropriate values.

8. Click **OK**.

Importing a Custom Module

Modules contain computer groups and processing rules, as well as other information. You can import custom modules to monitor computers in the configuration group.

To import a custom module:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**.
4. Click **Processing Rule Groups**.
5. On the Action menu, click **Import Custom Module**.
6. Follow the instructions until you finish importing the module. For more information about the fields on a window, see the Help.

Restoring a NetIQ Module

If you customize a NetIQ module and would like to revert all your changes, you can restore the NetIQ module. Restoring a NetIQ module allows you to overwrite all customizations, overwrite all customizations except changes to rules, or overwrite all customizations except changes to rules and the company knowledge base.

Note
It is not recommended that you modify the Security Manager Self-monitoring module in any way. Unlike other Security Manager modules, upgrading the Self-monitoring Module deletes all changes made to it.

For more information about importing NetIQ modules, see the *User Guide for NetIQ Security Manager*.

To restore a NetIQ module to its original state:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**.
4. Select **Processing Rule Groups**.
5. On the Action menu, click **Restore NetIQ Module**.
6. Click **Browse**, and then navigate to the module you want to restore.
7. Click the option for the customizations you want to overwrite.
8. Click **Import**. For more information about restoring a NetIQ module, see the Help.

Chapter 7

Understanding Scripts

Security Manager uses scripts to collect file and state variable information. You can collect information using rules, but scripts allow you to collect information for unique configurations and for applications or files that Security Manager does not monitor automatically. To run a script, specify it within a rule as a response to a specified event. For more information about rules, see “Understanding Processing Rule Groups” on page 63. You can run a script based on an alert from within the same rule or from a different rule. You can also run a script based on a timed event, so that the script runs at a specified interval. The scripts described in the following sections run on Windows computers.

When to Use Scripts

The easiest way to collect information using Security Manager is using processing rules. When you are unable to collect sufficient information using existing rules, you can use a script to collect the additional information. You may want to use scripts in the following scenarios:

- Respond to an event
- Create a response to a timed event
- Collect registry information

- Collect information from a known file
- Retrieve and analyze state variable information

Respond to an Event

Response scripts answer an event, alert, or performance threshold. When you create a processing rule, you can specify a script to run in response to a processing rule match. Response scripts are **synchronous**, meaning that the Windows agent or central computer waits for the script to complete before continuing to process the associated event, alert, or performance data.

Scripts could respond to an event, alert, or performance data with computer configuration changes. Using Windows Management Instrumentation (WMI), a script could change a computer configuration in response to an event.

For example, a company security policy might prohibit employees from using dial-up networking. You can configure Security Manager to watch for an event indicating that dial-up networking is enabled on a computer. A script could respond by using WMI to turn off dial-up networking on that computer, and then display a cautionary message to the computer user.

Note
The `NetIQ Security Manager` service stops if you execute a response script with an interactive process, like `calc.exe`. Security Manager does not display interactive processes launched by a service. They are visible in Process Explorer and remain running until stopped by using Process Explorer.

Create a Response to a Timed Event

You can link a script as a response to a timed event. For example, you could configure Security Manager to create an event that occurs every ten minutes. When the event occurs, Security Manager could run a script that pings the Internet Service Provider (ISP) router. If the ISP connection is down, the script could create an alert that indicates the problem. You can run timed event scripts either on the Windows agent or the central computer.

Note
Scripts that run at intervals of one minute or less may experience problems with the `NetIQ Security Manager` service since some program threads can take longer to complete. Create scripts with intervals greater than one minute to avoid problems with the `NetIQ Security Manager` service.

Collect Registry Information

You can collect file information, such as log data that is specified in the Windows registry. For example, you can use a script to determine the age of a specified file that is defined in the registry. To determine the file age, you can use a script to retrieve the file path from the registry and then retrieve the file time stamp.

Collect Information from a Known File

You can collect information from a known file in a known location to evaluate or to enter as data for a command or batch file. For example, you can determine file age for a file when the file location is defined in the registry. First you use the script to access the registry to determine the correct file location. When you know the file location, use the script to examine the time stamp on the specified file.

Retrieve and Analyze State Variable Information

As a processing rule response, you can update state variables, data stored in memory on the Security Manager central computer. A script can then analyze these state variable data and generate another response, such as issuing an alert.

A state variable can keep track of how many times an event has occurred on one or more monitored computers. For example, you want to monitor logon attempts and page an administrator if an excessive number of logon failures occur within a given period across all computers in your enterprise. A high number of logon failures in a short time might indicate a distributed attempt to break into the network.

You can create a processing rule to increment a state variable every time a logon failure occurs. Security Manager updates the state variables, resulting in minimal performance impact. You can then run a script at regular intervals to check the count. If the number of failures is not excessive, the script can reset the variable. If the number is excessive, the script can page an administrator to take action.

Supported Scripting Languages

You can write scripts using any of the following Active Scripting languages:

- VBScript
- JScript

Note
Other scripting languages may be supported. For more information, see MSDN topic “Hosting Environments and Script Engines.”

Security Manager supports invoking Windows COM objects including objects documented in the WScript reference, such as the WScript.shell, Scripting.FileSystemObject, and WScript.environment objects. For example:

```
set WshShell = CreateObject(“WScript.Shell”).
```

Security Manager does not support the Wscript object embedded in the Windows Scripting Host. For example:

```
set WshShell = WScript.CreateObject(“WScript.Shell”).
```

To specify Security Manager properties, such as alert severity, ensure you use Security Manager objects in your scripts.

Security Manager Objects

Security Manager supports objects that allow you to specify aspects of Security Manager in your scripts, such as alert severity and event type. For example, use the EventType property to specify an event type, such as Warning or Error as in the following example:

```
Dim MYevent
set MYevent = ScriptContext.CreateEvent
MYevent.EventType = "Warning"
```

For more information about Security Manager object syntax, see the Help. If you develop scripts that include Security Manager objects using a third-party tool, test your scripts in the Development Console to ensure your scripts correctly use the objects.

Creating a Script

You can use a third-party tool or the Development Console scripting interface to create a script. When you complete a script, paste it into the Properties Window for the appropriate script in the Development Console.

To create a script within Security Manager:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console > Advanced**.
4. Click **Scripts**.
5. On the Action menu, click **Create New Script**. Follow the instructions until you have finished creating a script. For more information about the fields on a window, see the Help.

Testing a Script

Security Manager does not provide a debugging tool, but you can use parameters and events to work through a script step-by-step in the scripting interface. Working through a script in the scripting interface allows you to test Security Manager objects in your scripts.

A step-by-step testing method requires you to create a parameter and then use the parameter values to identify successful subroutines in your script. This method requires the rule associated with the script to set the parameter value to `true`. Ensure you force the parameter configuration when changing the parameter value.

To implement step-by-step scripting:

1. Define a parameter. For example, create a parameter called `Test Subroutine` to generate an event after each subroutine in your script. Add the local Boolean variable ***`bDiagMsgs`*** and set the default value to `No.`

2. Initialize the parameter in your script. To initialize the parameter, define a local variable in your script called ***`bDiagMsgs`***. Use the parameter value passed to the script by calling the ***`Get`*** method as in the following sample code:

   ```
   bDiagMsgs = fncEvalBool (oParams.Get("Test Subroutine"))
   ```

   The ***`Get`*** method retrieves the parameter value and passes the value to the `fncEvalBool` local functions, which evaluates the value and returns a true or false result.

3. Identify the parameter in subsequent function calls. Consider the following example where the `subCreateEvent` function in this example creates an event only if the `Test Subroutine` parameter returns a true result. `subCreateEvent ERROR_EVENT_ID, ETYPE_INFO, "Short name=" & sProductName & ", Full name=" & sProductFullName, bDiagMsgs`

Running Scripts Locally or Centrally

You can run scripts on the Windows agent computer or the central computer. Because agents can run using a local system account, scripts that run on the Windows agent computer can access information local to the Windows agent computer, but cannot access information in the OnePoint database. For performance optimization, design scripts to run locally on agent computers.

Note
If a script needs access to a network resource that requires a particular security context, the Windows agent needs to use an appropriate service account.

Scripts running on the central computer can access information stored in the OnePoint database. They can also access stored state variable data on the central computer.

Modifying a Script

You can modify a script, including its source code and parameters. If you edit a script, you can add, edit, or delete parameters. If you only need to modify parameter values for one rule, you can modify the values in the rule properties for the appropriate rule. Changing parameter values in one rule does not affect the default parameter values defined in the script properties or the parameter values in other rules that use the same script.

To modify a script:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager Program group.
3. In the left pane, expand **Security Manager Development Console** > **Advanced**.
4. Click **Scripts**.

5. In the right pane, click the script that you want to modify.

6. On the Action menu, click **Properties**.

7. Specify the appropriate values. For more information about fields on a window, see the Help.

8. Click **OK**.

Script Examples

The example scripts in this section highlight the following important scripting concepts. Read the comments in each script for implementation details.

- Script parameters
- Security Manager objects
- Step-by-step testing

Script 1: Testing and Security Manager Objects

The following VBScript code illustrates how to implement step-by-step testing in your scripts. It also illustrates how to use Security Manager Objects to access the registry and the file system and create events.

Note
This script includes only code that highlights the specified concepts and is not complete.

```
. . .
=====================================================================
' Define Your Parameters: Pass the name of each variable to the Get
' method and retrieve the value as the returned value. Use the
' bDiagMsgs parameter to turn testing on and off. If the value is
' Yes or True, then bDiagMsgs is TRUE. Otherwise it is FALSE.


Set oParams     = ScriptContext.Parameters
bDiagMsgs       = fncEvalBool (oParams.Get("Test Subroutine"))
lngNumberOfDays = oParams.Get("Age Threshold")
sProductName    = oParams.Get("Product Short Name")  'New Param -
SMEX, SMEX2K, SPNT


Select Case sProductName
  Case "SMEX"
    sKeyName = "\HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for
Exchange\CurrentVersion\"
    sValueName = "HomeDir"
    sProductFullName = "ScanMail for Exchange"


  Case "SMEX2K"
    sKeyName = "\HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for
Exchange\CurrentVersion\"
    sValueName = "HomeDir"
    sProductFullName= "ScanMail for Exchange 2000"


  Case "SPNT"
    sKeyName =
"\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMFilter\"
    sValueName = "CurrentPatternName"
    sProductFullName = "ServerProtect"
End Select
================================================================
' Define local subroutines as follows:


subCreateEvent ERROR_EVENT_ID, ETYPE_INFO, "Short name=" &
sProductName & ", Full name=" & sProductFullName, bDiagMsgs
```

```
subCreateEvent ERROR_EVENT_ID, ETYPE_INFO, "The registry entry : " &
sKeyName & "\" & sValueName, bDiagMsgs
 ================================================================
' Registry objects are used to access the registry.


'get the value
set oRegistry = CreateObject("Regobj.Registry")
set oRegKey   = oRegistry.RegKeyFromString(sKeyName)
vRegValueData = oRegkey.Values(sValueName).Value 'value is a path.


If Err.Number = 35006 Then
  'The registry entry was not found
  subCreateEvent ERROR_EVENT_ID, ETYPE_ERR, "The registry entry was
not found: " & sKeyName & "\" & sValueName, 1
  Err.Number = 0
Else


  sPatternFileName = vRegValueData  'HomeDir for SMEX & SMEX2K, full
path for SPNT


  If sProductName = "SMEX" OR sProductName = "SMEX2K" Then
      sValueName = "PatternString"
      vRegValueData = oRegkey.Values(sValueName).Value 'get the
pattern string


      If Err.Number = 35006 Then
        'The registry entry was not found
        subCreateEvent ERROR_EVENT_ID, ETYPE_ERR, "The registry entry
was not found: " & sKeyName & "\" & sValueName, 1
        Err.Number = 0
      Else
      End If
      sPatternFileName = sPatternFileName & "lpt$vpn." &
Trim(vRegValueData)
  End If

  subCreateEvent DAT_EVENT_ID, ETYPE_INFO, "Full Path: " &
sPatternFileName, bDiagMsgs
====================================================================
' Use file system objects to access the file system. For
' example, the GetFile method retrieves file properties for a
' specified file.

  Set objFS = CreateObject("Scripting.FileSystemObject")
  Set objFile = objFS.GetFile(sPatternFileName)
  If Err.Number  = 0 then 'no problem
    vDATdate = split(objFile.DateLastModified, " ")
    if ubound(vDATdate) > 1 Then
        sMessage = vDATdate(0) 'first arg
    Else
        sMessage = vDATdate
    End If
    vDATFiledate = Cdate(sMessage)

    vCurrentSystemDate = Date

    nEventType = ETYPE_INFO

    If vCurrentSystemDate - vDATFiledate > cLng(lngNumberOfDays) Then
      'The DAT is older than specified number of days
      'Get context for precipitating event

      'Create a new event
      Set oNewEvent = ScriptContext.CreateEvent


      Select Case sProductName
        Case "SMEX"
          oNewEvent.Message         = Left("The ScanMail for Exchange
pattern file is more than " & lngNumberOfDays & " days old: " &
sMessage , MAX_EVENT_DESCRIPTION_LENGTH)


        Case "SMEX2K"
          oNewEvent.Message         = Left("The ScanMail for Exchange
2000 pattern file is more than " & lngNumberOfDays & " days old: " &
sMessage , MAX_EVENT_DESCRIPTION_LENGTH)


        Case "SPNT"
          oNewEvent.Message         = Left("The ServerProtect pattern
file is more than " & lngNumberOfDays & " days old: " & sMessage ,
MAX_EVENT_DESCRIPTION_LENGTH)
      End Select


      Set oEvent = ScriptContext.Event
==================================================================
' You can create and define new events.


      'Set new event properties
       ''oNewEvent.Message         = ""
       oNewEvent.EventNumber     = DAT_EVENT_ID
       oNewEvent.EventType       = ETYPE_ERR
       oNewEvent.EventSource     = EVENT_SOURCE
       oNewEvent.LoggingComputer = oEvent.LoggingComputer
       oNewEvent.LoggingDomain   = oEvent.LoggingDomain
       oNewEvent.SourceComputer  = oEvent.SourceComputer
       oNewEvent.SourceDomain    = oEvent.SourceDomain
       oNewEvent.UserName        = oEvent.UserName
       oNewEvent.UTCTime         = oEvent.UTCTime

      'Set the parameters for the new event
       oNewEvent.SetEventParameter lngNumberOfDays
=====================================================================
' After you create an event, call the Submit method to submit the
' event into the workflow.

      'Submit the event
       ScriptContext.Submit oNewEvent
       set oNewEvent = Nothing

       'also send out the date
      subCreateEvent DAT_EVENT_ID, nEventType, "Pattern file date for
" & sProductFullName & " : " & sMessage, 1
    Else
       'just send the date out
      subCreateEvent DAT_EVENT_ID, nEventType, "Pattern file date for
" & sProductFullName & " : " & sMessage, 1
    End If

  Else
    nEventType = ETYPE_ERR
    vMessage = "Unable to determine the pattern file."
  End if

'  subCreateEvent DAT_EVENT_ID, nEventType, sMessage, bDiagMsgs

End If
==================================================================
' Remove allocated objects before exiting a script.
```

```
set oRegistry = Nothing
set oRegKey   = Nothing
Set oParams   = Nothing
'End of Main
```

Script 2: Function to Access Registry

The following VBScript code illustrates how to create a local function to access the registry.

Note
This script includes only code that highlights the specified concepts and is not complete.

```
'******************************************************************
' Function    - fncGetValueForRegKey
' Purpose     - Read the specified Registry value
' Assumptions -
' Parameters  - str_KeyName    = name of the key that holds the value
'               str_ValueName  = name of the value
'               var_Value      = used to return the value
'               lng_Type       = used to return the type
'*******************************************************************
Function fncGetValueForRegKey (str_KeyName, str_ValueName, var_Value,
lng_Type, str_NewKey)

  Dim objRegistry, objRegKey, objRegValue, varRegValue, blnKeyFound
  Dim objNewKey, objSubKey
  Dim strTName

  On Error Resume Next
  'Open the Registry:
  set objRegistry = CreateObject("Regobj.Registry")
  set objRegKey   = objRegistry.RegKeyFromString(str_KeyName)
  var_Value       = objRegkey.Values(str_ValueName).Value
  If Err.Number = 35006 Then
     'The registry entry was not found
     Err.Number = 0
     Set objNewKey = objRegistry.RegKeyFromString(str_NewKey)
     For Each objSubKey In objNewKey.SubKeys
        If Err.Number = 0 Then
           var_Value = objSubKey.Name
        End If
     Next
     If IsNumeric(var_value) AND Err.Number = 0 Then
        fncGetValueForRegKey = True
     Else
        fncGetValueForRegKey = False
     End If
     Set objNewKey = Nothing
  Else
     lng_Type        = objRegkey.Values(str_ValueName).Type
     If Err.Number   = 0 Then
        fncGetValueForRegKey = True
     Else
        fncGetValueForRegKey = False
     End If
  End If

  set objRegistry = Nothing
  set objRegKey   = Nothing
End Function
```

Script 3: Function to Create an Event

The following VBScript code illustrates how to create an event using a local function.

Note
This script includes only code that highlights the specified concepts and is not complete.

```
'*******************************************************************
' Script Name - subCreateEvent
' Purpose     - Creates an event in the Windows Application Event Log
' Parameters  - lngCE_EventID   - The event ID
'               lngCE_EventType - The Event Type
'               strCE_Msg       - The event text
'               blnCE_Active    - Y/N determines if event is created
'*******************************************************************
Sub subCreateEvent (lngCE_EventID, lngCE_EventType, strCE_Msg,
blnCE_Active)


   Const MAX_EVENT_DESCRIPTION_LENGTH = 3450
   Dim objCE_NewEvent
   blnCE_Active = Left(UCase(blnCE_Active),1)'


   If blnCE_Active = "Y" OR blnCE_Active = "1" then


     'Create new event and submit event objects
     Set objCE_NewEvent     = ScriptContext.CreateEvent


     ' Set event properties
     objCE_NewEvent.Message     = Left(strCE_Msg,
MAX_EVENT_DESCRIPTION_LENGTH)
     objCE_NewEvent.EventNumber = lngCE_EventID
     objCE_NewEvent.EventType   = lngCE_EventType
     ' Submit the event
     ScriptContext.Submit objCE_NewEvent
     set objCE_NewEvent    = Nothing
  End If
End Sub
. . .
End Function
```

Appendix A
Providing Support for SNMP

The Simple Network Management Protocol (SNMP) is a network management standard that helps security personnel manage remote TCP/IP networks. SNMP has two primary elements, the **SNMP agent** and the **SNMP management system**. These two elements communicate by routing messages using internet protocol (TCP/IP). One of the SNMP message types is an **SNMP trap**. An SNMP trap is an unsolicited message that the SNMP agent sends to the management system if the SNMP agent detects certain events on a managed element. An SNMP agent on a router would send a trap, for example, if it detected a problem with a network interface.

Security Manager can act as an SNMP management system to catch SNMP traps from a third-party SNMP agent, or as an SNMP agent to send traps to a third-party management system.

Catching SNMP Traps

Security Manager employs Windows Management Instrumentation (WMI) to enable SNMP management capability.

Sending SNMP Traps

When Security Manager processes an alert, it can also send an SNMP trap to a third-party management system.

The steps in this section describe the process to configure SNMP traps for Security Manager Windows computers. UNIX and iSeries agents also can send SNMP traps. For more information, see the agent product documentation.

Installing the SNMP Service

Install the SNMP service on each Security Manager Windows agent or central computer that will catch or send SNMP traps. SNMP is a TCP/IP protocol. To perform any SNMP functions, configure TCP/IP as a transport protocol. For more information about installing the SNMP service, see the SNMP documentation for your version of Windows.

Configuring the SNMP Service

Configure the SNMP service on the computer sending or catching SNMP traps. If you want Security Manager to send SNMP traps, you need the IP address or the name of the SNMP host computer, which is the computer that catches SNMP traps. Consult your security specialist for this information. For more information about configuring the SNMP service, see the SNMP documentation for your version of Windows.

Catching SNMP Traps from Third-Party SNMP Agents

The following procedure documents how to configure a Security Manager Windows agent or central computer to catch SNMP traps.

To use Security Manager to catch SNMP traps from third-party SNMP agents, complete the following steps:

1. Ensure the SNMP Service is installed on each computer that will catch SNMP traps. For more information, see the SNMP documentation for your version of Windows.
2. Ensure the SNMP service is configured to accept traps from your community name and SNMP hosts.

Note
Security Manager use the first community name listed in the **Community Name** list when handling SNMP traps.

3. Ensure the WMI SNMP Provider is installed on the Security Manager Windows agent or central computer. Start both the SNMP and the SNMP Trap services. For more information, see the SNMP documentation for your version of Windows.
4. Compile the appropriate third-party Management Information Bases (MIBs) into WMI. For more information about compiling MIBs, see “Compiling MIBs in WMI” on page 160.

Note
Because Security Manager uses WMI, MIBs must be compiled to WMI, not to the SNMP agent.

5. Verify the SNMP service is correctly installed and configured.
6. Configure a third-party SNMP agent to send SNMP traps to the Security Manager Windows agent or central computer. For more information, consult the third-party documentation.
7. Configure the Security Manager Windows agent or central computer to catch SNMP traps. For more information about configuring agents and central computers, see “Configuring an Agent or Central Computer to Catch SNMP Traps” on page 161.

Compiling MIBs in WMI

A Management Information Base (MIB) is a file that contains information about a managed networked device. Because SNMP traps use numerical codes similar to IP addresses, you must use MIBs to translate the codes into understandable messages, much like the way a DNS server translates IP addresses. Any managed component on a network could have a MIB.

You can download MIBs from `ftp://ftp.isi.edu/mib` or obtain MIBs from device manufacturers.

Use the `SMI2SMIR` WMI command to compile a MIB for each managed device that could cause an SNMP agent to send an SNMP trap. The `SMI2SMIR` command compiles the MIB into the `\\.\root\snmp\smir` namespace. The syntax for the `SMI2SMIR` command is as follows:

```
SMI2SMIR {/V1|/V2C} /A /T MIB_FileName
```

For example:

```
"SMI2SMIR /V1 /A /T "\PROGRAM FILES\COMPANYXYZ\COMPANYXYZ.MIB""
```

Options for compiling third-party MIBS are defined as follows:

/V1

Specifies strict conformance to the SNMP version 1 Structure of Management Information (SMI) schema. The compiler reports an error if it detects statements other than SNMP version 1 statements. Specify `/V1` when compiling SNMP version 1 MIBs.

/V2C

Specifies strict conformance to the SNMP version 2 Structure of Management Information (SMI) schema. The compiler reports an error if it detects statements other than SNMP version 2 statements. Specify `/V2C` when compiling SNMP version 2 MIBs.

/A

Performs local and external checks and loads the MIB module in the SMIR.

/T

Generates the SnmpNotification classes.

MIB_FileName

Specifies the full path to the third-party MIB file, such as `\PROGRAM FILES\`*`COMPANY`*`\`*`COMPANY`*`.MIB`.

For more information about the `SMI2SMIR` command, see "Running the SNMP Compiler" in the Microsoft MSDN Online Library at `msdn.microsoft.com.`

Configuring an Agent or Central Computer to Catch SNMP Traps

The following procedure documents how to configure a Security Manager Windows agent or central computer to catch SNMP traps. Install the SNMP service, the WMI provider, and the WMI SNMP Provider on the Security Manager Windows agent or central computer before the agent can catch SNMP traps.

To configure a Security Manager Windows agent or central computer to catch SNMP traps:

1. Log on to a Development Console computer with an account that is a member of the OnePointOp Operator group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager program folder.
3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.
4. Expand the processing rule group that you want to catch SNMP traps.
5. Select **Event Processing Rules**.
6. On the Action menu, click **New > Event Processing Rule**.
7. Select an event processing rule type.
   - ***If you want the rule to generate an alert,*** select **Alert on or Respond to Event**.
   - ***If you want the rule to collect events,*** but not generate alerts, select **Collect Specific Events (Collection)**.

8. Select the appropriate SNMP trap catcher from the Provider name list.
   - ***If you want to catch SNMP version 1 traps,*** select **SNMP Trap Catcher**.
   - ***If you want to catch SNMP version 2 traps,*** select **SNMP Extended Trap Catcher**.

   Note
   If you want to catch traps for all SNMP events, you must create two rules: one rule using SNMP Trap Catcher as a provider and one using SNMP Extended Trap Catcher as a provider.

9. Click **Next**.
10. Follow the instructions until you have finished creating the event processing rule.
11. Configure the SNMP agent computer to recognize SNMP traps sent from the Security Manager Windows agent or central computer. The SNMP host computer catches SNMP traps. For more information, see the SNMP documentation for your version of Windows.

    Note
    You can create an event processing rule that uses a class-defined WMI data provider that filters on class definitions from specific MIBs.

Sending SNMP Traps to a Third-Party SNMP Management System

The following procedure documents how to configure a Security Manager agent or central computer to send SNMP traps.

To use Security Manager to send SNMP traps to a third-party management system:

1. Ensure the SNMP Service is installed on each computer that will send SNMP traps. For more information, see SNMP documentation for your operating system.
2. Ensure the SNMP service is configured to accept traps from your community name and trap destinations.

   Note
   Security Manager use the first community name listed in the **Community Name** list when handling SNMP traps.

3. Compile the MIB using the compiler provided by your third-party SNMP management system. For more information about compiling MIBs, see "Compiling the MIB" on page 163.
4. Configure a Security Manager Windows agent or central computer to send SNMP traps. For more information about configuring agents or central computers, see "Configuring an Agent or Central Computer to Send a Trap for an Event" on page 164 and "Configuring an Agent or Central Computer to Send Traps for All Events" on page 165.
5. Configure the SNMP host computer to recognize SNMP traps sent from the Security Manager Windows agent or central computer. The SNMP host computer catches SNMP traps. For more information, see the SNMP documentation for your version of Windows.

Compiling the MIB

A Management Information Base (MIB) is a file that contains information about a managed networked device. Because SNMP traps use numerical codes similar to IP addresses, you must use MIBs to translate the codes into understandable messages, much like the way a DNS server translates IP addresses. Any managed component on a network could have a MIB.

The MIB file, `MissionCritical.mib,` describes the traps sent by the agent and under what conditions traps are sent. The MIB file is contained in the `OnePoint` folder.

You can compile the `MissionCritical.mib` file using the third-party SNMP management system you use to catch SNMP traps. Consult the documentation provided by the SNMP management system for more information.

Configuring an Agent or Central Computer to Send a Trap for an Event

This procedure documents how to configure a Security Manager Windows agent or central computer to send an SNMP trap as a response to a specific event.

To configure a Security Manager Windows agent or central computer to send SNMP traps for a specific event:

1. Log on to a Development Console computer with an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager.*
2. Start the **Development Console** in the NetIQ Security Manager program folder.
3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.
4. Expand the processing rule group that contains the rule for which you want to send an SNMP trap.
5. Select the processing rule for which you want to send an SNMP trap.
6. On the Action menu, click **Properties**.
7. Click the Responses tab.
8. Click **Add**.
9. Select **Send an SNMP trap**.

10. Specify the computer from which you want the SNMP trap to be sent.

    - To send an SNMP trap from the Security Manager Windows agent computer, select **Locally on the agent computer**.
    - To send an SNMP trap from the central computer, select **On the central computer**.

11. Click **OK** on the SNMP Response Editor window.
12. Click **OK** on the Properties window.
13. Configure the SNMP host computer to recognize SNMP traps sent from the Security Manager Windows agent or central computer. The SNMP host computer catches SNMP traps. For more information, see the SNMP documentation for your version of Windows.

Configuring an Agent or Central Computer to Send Traps for All Events

This procedure documents how to configure Security Manager Windows agent or a central computer to send SNMP traps as a response to all events in a processing rule group.

To configure a Security Manager Windows agent or central computer to send SNMP traps for all events in a processing rule group:

1. Log on to a Development Console computer with an account that is a member of the OnePointOp Operator group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager program folder.
3. In the left pane, expand **Security Manager Development Console > Processing Rule Groups**.
4. Expand the processing rule group for which you want to create a new alert processing rule.
5. Click **Alert Processing Rules**.

6. On the **Action** menu, click **New > Alert Processing Rule**.
7. Select the **only match alerts generated by the rules in the following group** check box on the Response Rule Properties, Alert Criteria window, and then click **Next**.
8. Specify an alert schedule on the Response Rule Properties, Schedule window, and then click **Next**.
9. Click **Add** on the Response Rule Properties, Responses window.
10. On the Add menu, click **Send an SNMP Trap**.
11. Specify the computer from which you want the SNMP trap to be sent.
    - To send an SNMP trap from the Security Manager Windows agent computer, select **Locally on the agent computer**.
    - To send an SNMP trap from the central computer, select **On the central computer**.
12. Click **Next**.
13. Follow the instructions until you have finished creating the alert processing rule.
14. Configure the SNMP host computer to recognize SNMP traps sent from the Security Manager Windows agent or central computer. The SNMP host computer catches SNMP traps. For more information, see the SNMP documentation for your version of Windows.

Appendix B

Understanding WMI

Microsoft Windows Management Instrumentation (WMI) provides a means for collecting and accessing data from Windows computers in an enterprise network. Security Manager can use WMI to extend its monitoring capabilities by collecting and monitoring WMI information. Security Manager can also integrate with other systems management solutions by publishing its own alerts as WMI events.

WMI is the Microsoft implementation of the Web-Based Enterprise Management (WBEM) initiative. WBEM is an industry initiative to develop a standard for collecting, accessing, and sharing management information in an enterprise network.

Object-oriented constructs, such as classes, represent the managed objects. The classes include properties that describe data, and methods that describe behavior. The managed objects include hardware or software system components that are represented as instances of WMI classes. Through the class hierarchy, developers can create associations between different domains by providing a standard, uniform model to represent and access management information.

WMI Architecture

WMI architecture includes the following components:

CIM-compliant object repository

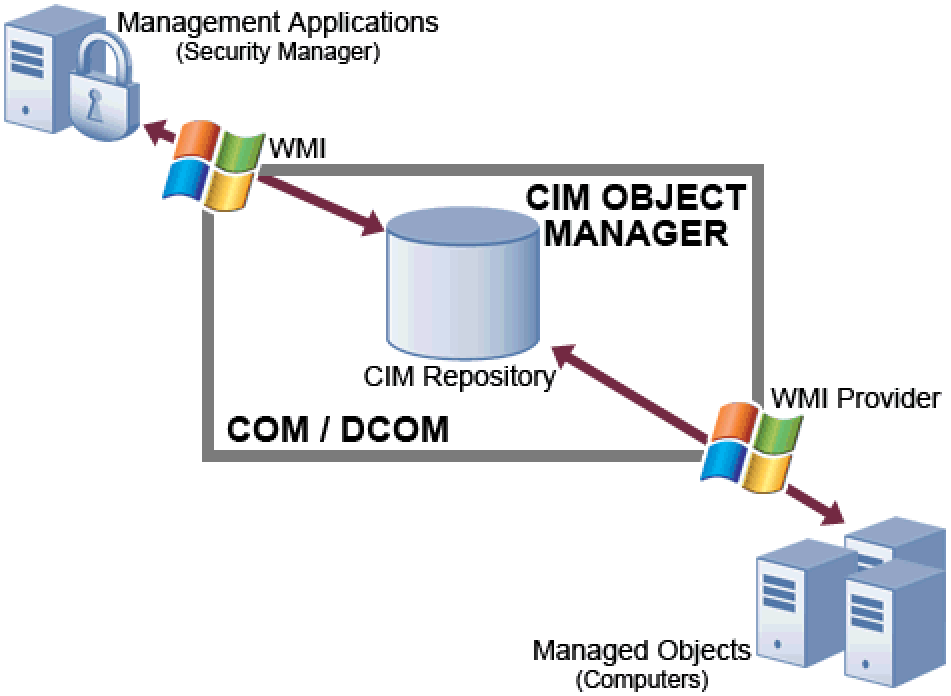
Used for the storage of managed objects on each computer.

CIM Object Manager
Used to handle the interaction between management applications and WMI providers.

WMI providers
Used as intermediaries between the CIM object manager and the managed objects.

Distributed Component Object Model (DCOM)
Used as the protocol for obtaining and disseminating the data within the managed network, by allowing software components to communicate directly with each other across networks.

The following figure illustrates the interaction between WMI components.



The object-oriented schema allows data from diverse sources to be represented in a consistent, logical way and enables associations between the management data regardless of type, content, or source of origin.

You can use the WMI Query Language (WQL), a query language based on SQL, to access data from WMI. WMI also provides a powerful event handling mechanism for developers. WMI uses **extrinsic** and **intrinsic** events to describe the changes that occur in a managed environment. These events are defined in the following sections.

Intrinsic Events

Intrinsic events occur when a WMI provider generates a response to a change in data within the managed environment. The creation, deletion, and modification of data create intrinsic events. These changes in data are represented by a set of **system classes.** Examples of system classes include **services,** such as the Win32_Service class, and **processes,** such as the Win32_Process class.

When WMI or a WMI provider generates an intrinsic event, an instance of a system class is defined to represent that type of event. WMI then sends the instance to the **consumers** that have registered for that event.

For example, Security Manager can monitor service status changes through intrinsic WMI events. A service is a program or routine that provides support to other programs. A WMI event is generated when a service changes from one of the following states to another state:

- Stopped
- Starting
- Stopping
- Running
- Continuing
- Pausing
- Paused

For example, you can use Security Manager and WMI to monitor the RemoteAccess service on a managed computer. You can create a processing rule that monitors WMI for an intrinsic event indicating that the RemoteAccess service on the computer has started. When the intrinsic event occurs, Security Manager can generate an alert and a response, such as sending an email to an administrator.

Extrinsic Events

Extrinsic events are user-defined events that are not previously described by an intrinsic event. These events relate to changes that can occur within and beyond the scope of the managed environment, through third-party applications. Extrinsic events are not limited by a certain set of system classes. WMI providers define the event classes describing the changes that occur in the environment.

For example, Security Manager can monitor SNMP traps through WMI extrinsic events. An SNMP trap is a packet of information sent by a network device that is running the Simple Network Management Protocol (SNMP). SNMP is a protocol based on TCP/IP and is used to monitor and manage network devices, such as a router or a computer running any operating system. An SNMP trap is usually sent in response to an event, such as a service stopping. However, some SNMP traps indicate normal system operation.

For more information about configuring Security Manager to monitor SNMP traps, see “Providing Support for SNMP” on page 157.

WMI/Security Manager Interaction

Security Manager and WMI work together to provide configuration and event-related information about monitored computers. Security Manager monitors WMI information using Security Manager data providers, processing rules, and scripts. This section describes these components.

Data providers

Registered with WMI as consumers of WMI events. Security Manager processing rules use data providers to collect specific information. You can create **WMI event providers** and **WMI numeric providers** that are sources of WMI event-related and performance information.

Processing rules

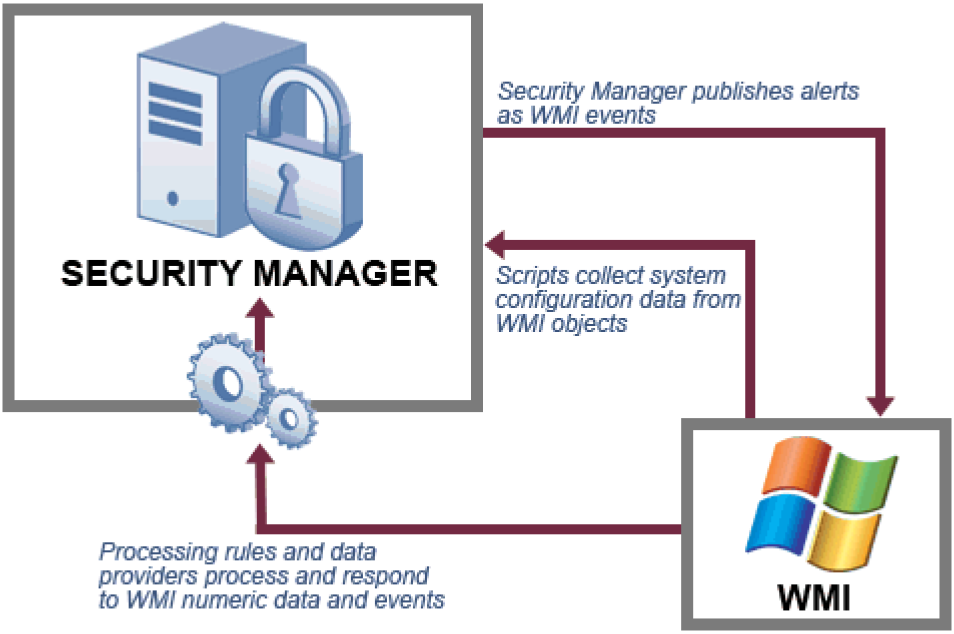
Defines how Security Manager collects, processes, and responds to collected information. You can create event and performance processing rules to handle data obtained through WMI event providers and WMI numeric providers.

Scripts

Provides flexible and customized monitoring. You can use scripts to collect configuration data from WMI objects on a scheduled basis.

To integrate with other systems management solutions, Security Manager can also publish its own alerts as WMI events. For more information about integrating Security Manager using WMI, see “Publishing Alerts as WMI Events” on page 179.

The following figure illustrates interactions between Security Manager and WMI.


SECURITY MANAGER
Security Manager publishes alerts as WMI events
Scripts collect system configuration data from WMI objects
Processing rules and data providers process and respond to WMI numeric data and events
WMI

When Security Manager receives information through a WMI event provider or WMI numeric provider that matches a particular processing rule, a **processing rule match** occurs. When a processing rule match occurs, Security Manager performs the actions and the response defined in the processing rule. The information corresponding to the match may also be stored in the OnePoint database. You can use the Control Center to view event-related information.

For example, using an event processing rule, you can use Security Manager and WMI to monitor dial-up networking on a computer. When dial-up networking starts, a WMI event provider detects the event and sends the event-related information to Security Manager. Security Manager analyzes the event data and a processing rule match occurs. Security Manager responds by storing the event-related information in the OnePoint database, generating an alert, and then paging or sending an email to a network administrator.

Note
You can view the event or an associated alert using the Security Manager Control Center.

You can also use Security Manager and WMI to monitor numeric data on a computer. For example, Security Manager can monitor the free disk space on a computer. You can use a performance processing rule to alert an administrator when the free disk space on an FTP server is lower than a defined threshold, which may indicate that the server is being used for unauthorized storage of sensitive materials. A WMI numeric provider samples the free disk space at a defined interval and Security Manager analyzes the disk space data. When a processing rule match occurs Security Manager can alert an administrator.

Security Manager can use scripts to monitor configuration data on a computer. For example, a script could use WMI to collect data about computer hardware, such as network adaptor settings, on a specific schedule. At a specified interval, the script collects data and stores it in the OnePoint database. You can view this data using default views, or by creating a custom view. For more information about using scripts with WMI, see “Using Scripts to Monitor Configuration Data” on page 179.

Note
For information about the Microsoft WMI SDK, which includes a WMI object browser, see the Microsoft Web site at msdn.microsoft.com.

Monitoring Data with WMI

Security Manager can monitor computers for WMI events and WMI performance data. The following sections provide instructions for creating computer groups and processing rules in Security Manager.

Creating WMI Computer Groups

Security Manager allows you to group similar computers for monitoring and management. **Computer grouping rules** define these groups of computers. To monitor computers with WMI, you must define a computer group that includes the computers that have WMI installed.

WMI is installed by default on Windows 2000 and Windows XP computers. For example, to monitor Windows 2000 computers with WMI, you can simply create a computer group that contains all Windows 2000 computers. However, depending on the modules you have installed, this computer group may already exist.

You could also create a customized computer group that contains a combination of specific computers you want to monitor.

For more information about creating a computer group, see “Creating a Windows Computer Group” on page 48.

Event and Performance Monitoring

You can use the WMI event and numeric providers to gather specific information on the computers you monitor. The processing rules you create define how Security Manager collects, handles, and responds to WMI event and performance information from managed computers.

WMI event providers gather event-related information about monitored computers. Security Manager can detect WMI events that are either changes to WMI data (intrinsic events) or are provided to WMI through third-party applications (extrinsic events).

WMI numeric providers allow Security Manager to monitor performance information and gather numeric data about managed computers. You can identify trends by collecting values at specified intervals and then graphing the data in the Monitor. Security Manager can also monitor computers for performance thresholds using WMI numeric data. Security Manager generates the appropriate response when a specified event occurs or performance threshold is reached.

Note

If you create a processing rule that obtains data from a WMI event provider, do not specify any properties in the Properties list. Whether you specify properties or leave this field blank, all properties are returned in the notification object.

To create a WMI processing rule in Security Manager:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see the *Installation Guide for NetIQ Security Manager*.
2. Start the **Development Console** in the NetIQ Security Manager program folder.
3. In the left pane, expand **Security Manager Development Console > Processing Rules Groups**.
4. Expand the processing rule group where you want to add the new processing rule.

   The processing rule group should be associated with a computer group that contains the WMI computers you want to monitor. For more information about WMI computer groups, see “Creating WMI Computer Groups” on page 174. For more information about creating a processing rule group, see “Creating a Processing Rule Group” on page 68.
5. ***If you want to create an event processing rule,*** click **Event Processing Rules**.
6. ***If you want to create a performance processing rule,*** click **Performance Processing Rules**.
7. On the Action menu, click the type of processing rule you want to create.

For example, to create an event processing rule, click **Alert on or Respond to Event**. To create a performance processing rule that samples WMI numeric data, click on **Sample Performance Data.** You can create other types of performance or event related rules. For more information about processing rules, see "Understanding Processing Rules" on page 77.

8. Click **New** in the **Properties** window.
9. Select **WMI Events** or **WMI Numeric Events** depending on the type of processing rule you are creating, and then click **OK**.
10. Type the appropriate properties into each field.
11. Click **Finish**.
12. Follow the instructions until you have finished creating the processing rule. The Rule Wizard allows you to specify alert generation and response information. Make selections based on your network enterprise environment. For more information about the fields on a window, see the Help.

Event Monitoring Examples

You can use Security Manager and WMI to monitor when certain applications are started on any of the monitored machines. For example, you could create an event processing rule that monitors the Registry Editor application and generates a WMI event when the application is started.

The following table lists the properties that you would need to set.

Field	Description	Example
Name	WMI event provider name	`Registry Editor 32 Process Watcher`
Namespace	WMI namespace to which the class of the WMI data belongs	`root\CIMV2`

Field	Description	Example
Query	WQL query for WMI event notification.	`select * from __InstanceCreationEvent within 5 where TargetInstance is a "Win32_Process" and TargetInstance.Name = "regedt32.exe"`
Property List	List of properties to view for the notification object. Separate the properties with a comma. If you want all of the properties returned, leave the Property List field blank.	`__Namespace, CreationDate`

You can create many different types of WMI providers to monitor different types of information in your network. For example, WMI providers that track services can be very useful in monitoring a network.

The following table shows the properties required to create an event processing rule that monitors the RemoteAccess service. It provides a WMI intrinsic event when the RemoteAccess service changes from Stopped to Running.

Field	Example
Name	`RemoteAccess Service Watcher`
Namespace	`root\CIMV2`
Query	`select * from __InstanceOperationEvent within 5 where TargetInstance is a "Win32_Service" and TargetInstance.Name = "RemoteAccess" and TargetInstance.State = "Running"`
PropertyList	`__Namespace, __Path`

Installing software programs can add new namespaces to a computer. The number of properties in the property list of an object varies with the object type. For more information about the different namespaces and object property lists that you can access through WMI, see the Microsoft WMI SDK documentation.

Performance Monitoring Examples

You can use Security Manager and WMI to monitor performance information and gather numeric data on any of the monitored computers. For example, you could create a performance processing rule that monitors the free disk space on an FTP server and generates a WMI event when free disk space goes below a defined threshold, which may indicate that the server is being used for unauthorized storage of sensitive materials. The following table lists the properties that you would need to set.

Field	Description	Example
Name	WMI event provider name	`Free Disk Space`
Namespace	WMI namespace to which the class of the WMI data belongs	`root\CIMV2`
Class	WMI class to which the numeric data belongs. Class defines the basic unit of management. Each class acts as a template that is used by all its instances.	`Win32_LogicalDisk`
Object Instance Expression	Instance to measure that contains the actual data. You can use the same operators as those used in the WMI where clause. Leave this field blank to collect all instances.	`DeviceID=”C:”`
Numeric Property	Numeric property to measure	`FreeSpace`
Instance Text Property	Object property used to differentiate the instance from others	`DeviceID`
Sample Every	How often to sample the WMI numeric data	`5 minutes`

Using Scripts to Monitor Configuration Data

Security Manager provides scripting capabilities for flexible, customized monitoring and response to events, alerts, and performance thresholds. Scripts can extend Security Manager event management functions and can provide additional data collection capabilities. Security Manager can run response scripts for events and alerts on a scheduled basis.

For more information about Security Manager scripting capabilities, see "Understanding Scripts" on page 139.

Publishing Alerts as WMI Events

In addition to monitoring WMI information and creating alerts, Security Manager can publish its alerts as WMI events. As Windows 2000, Windows XP, and WMI are more widely adopted, Security Manager alerts published through WMI can be easily integrated into other system management solutions.

When you install Security Manager, the setup program copies the Security Manager Managed Object Format (MOF) file `SM.MOF` into the `NetIQ Security Manager\OnePoint` folder on the central computer. An MOF file is a text file that contains definitions of classes and instances in the MOF language.

WMI needs specific information about Security Manager alerts to pass the information to WMI clients. To configure WMI so that it has the necessary information, compile `SM.MOF` on the central computer using the WMI compiler `MOFCOMP.EXE.` Compiling `SM.MOF` in WMI creates the WMI namespace `ROOT/NetIQ,` the `SM_ALERT` class, and the Security Manager alert provider for WMI.

The properties of an `SM_ALERT` object mimic the properties of a Security Manager alert:

AlertID

The globally unique identifier (GUID) of an alert. The GUID is a unique identification string used with remote procedure calls. Every interface and object class uses a GUID for identification.

EventID

Specifies the Windows event number.

AlertLevel

Provides access to the severity of the alert, such as 0 or 51.

AlertLevelName

Specifies the text associated with the severity of the alert. Severity numbers are mapped to meaningful text, such as `Service Unavailable` or `Success` in Security Manager.

Server

Specifies the agent that the alert occurred on.

Source

Provides access to the source of the alert. The source of an alert is a user-defined name. If no name is defined, the event source is typically used.

Owner

Provides access to the name of the owner of the alert. The owner can be someone responsible for tracking and resolving the alert.

Description

Provides access to the description of the alert. The description of an alert is typically the description of the event that generated the alert.

CustomField

Provides a user-defined custom field of the alert.

AlertURL

Provides details about the alert that can be accessed through the Web Console. The Web Console allows you to view database information from any Windows platform that supports Microsoft Internet Explorer.

EventURL

Provides details about the event that can be accessed through the Web Console.

WorkItemData

For internal use only.

WMI alert publishing is not enabled until a WMI client subscribes to WMI events representing Security Manager alerts. To configure the subscription for WMI clients, use your third-party WMI-enabled management system to specify the **ROOT/NetIQ** namespace and the appropriate WQL query. For example, to configure the WMI client to receive all Security Manager alerts, specify the following WQL query:

```
Select * from SM_Alert
```

For more information about compiling MOF files, consult the documentation for WMI and for your third-party management system.