User 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 Security Manager Interfaces 23

Chapter 3
Working with Real-Time Views 57

Chapter 4

Working with Events, Alerts, and Responses 75

Chapter 5
Managing and Analyzing Logs 125

Chapter 7
Administering Agents 191

Chapter 8
Configuring Security Manager 231

Appendix B
Configuring Authenticated Communication 309

About This Book and the Library

The user guide provides conceptual information about the NetIQ Security Manager product (Security Manager). This book defines terminology and various related concepts. This book also provides an overview of the user interfaces and step-by-step guidance for many tasks.

Intended Audience

This book provides information for individuals responsible for understanding Security Manager concepts and for individuals designing and implementing a security solution for their enterprise network.

Other Information in the Library

The library provides the following information resources:

Installation Guide
Provides detailed planning and installation information.

Programming Guide
Provides conceptual information about Security Manager rules and step-by-step guidance for rule customization tasks using the Development Console.

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

Trial Guide
Provides product trial and evaluation instructions and a product tour.

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.

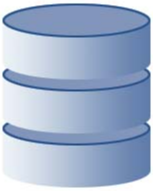
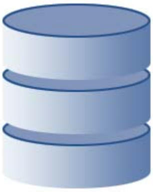
Understanding Product Components

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.

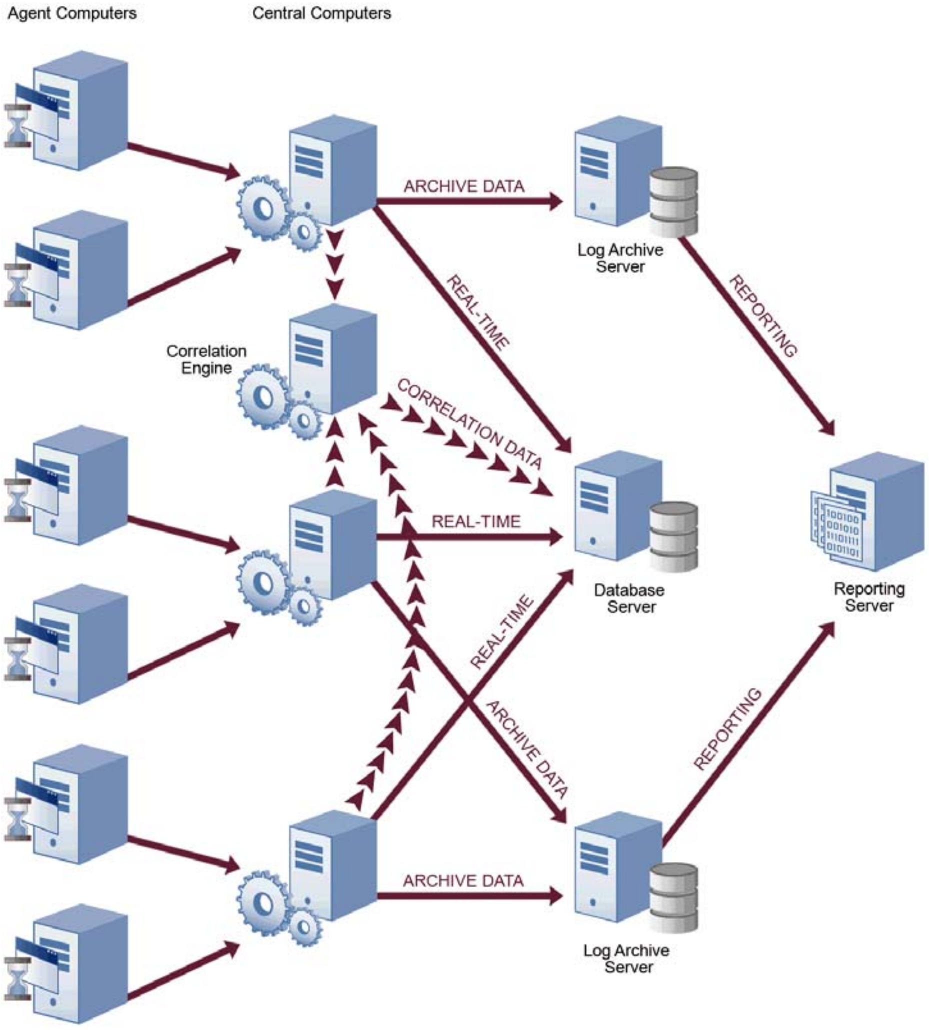
The agent computers, central computers, reporting server, log archive servers, and database server make up a configuration group. You can control where to install various components of the configuration group, including where to install the database server and how many central computers or log archive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

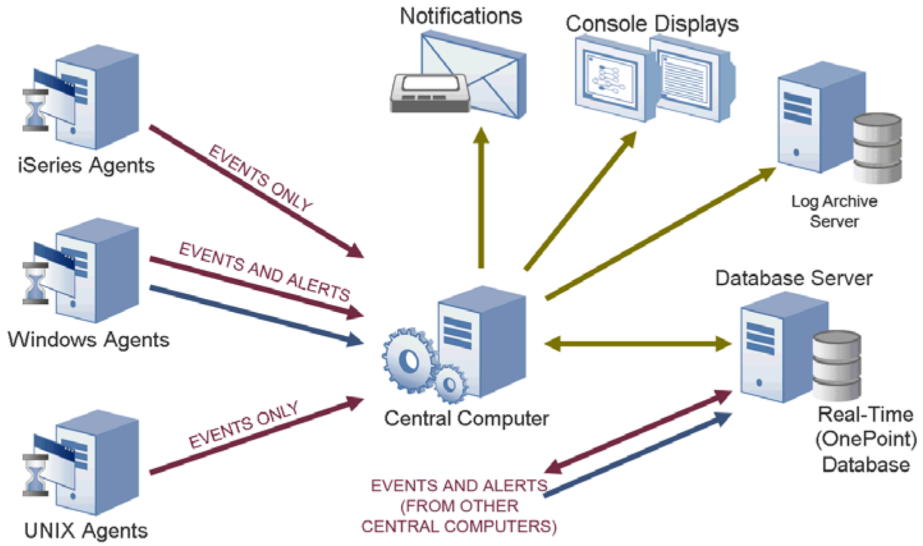
- Inform you about the current state of security (real-time alerts and events)
- Identify events indicating complex threats (correlated real-time events)
- Research significant historical security incidents (log data)
- Understand current security and trends (reporting data)

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.

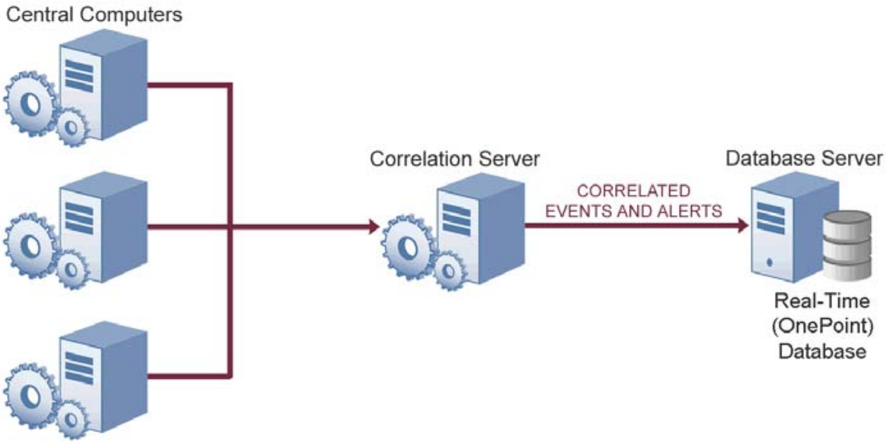
The central computers also send alert and event data to the log archive server for storage in the log archive. You can manage the automatic grooming settings for the log archive from the Log Archive Configuration utility.

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.

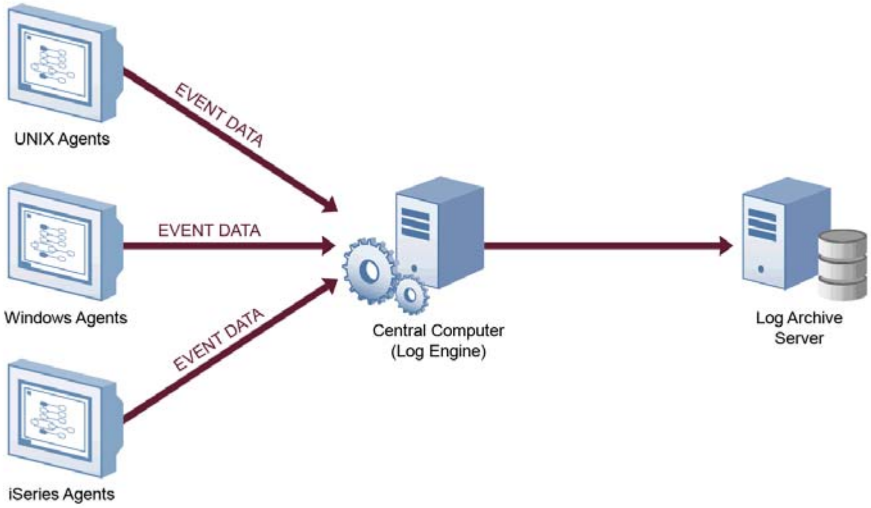


A **correlation rule** is a set of criteria that configures Security Manager to detect a pattern of real-time events and respond accordingly. The Correlation server evaluates collected alerts and events against the correlation rules as data arrives. When a rule match occurs, the Correlation server responds 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.



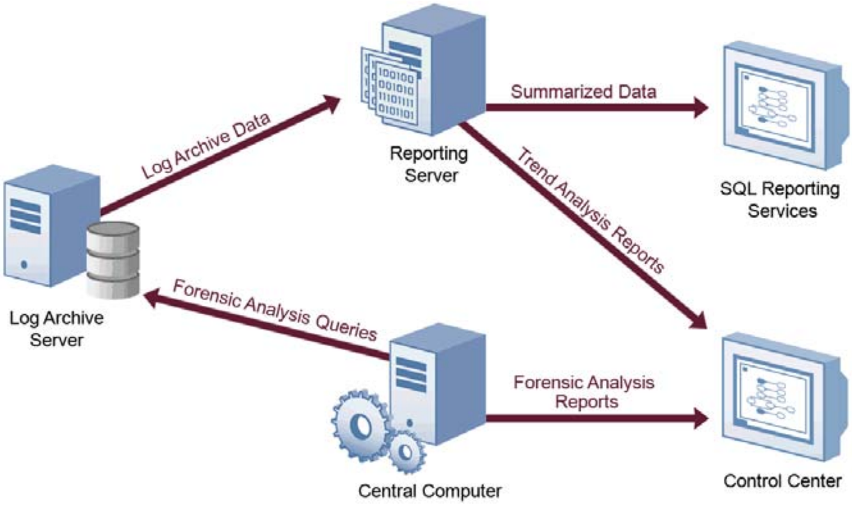
The Log Engine receives the event data and sends it to a log archive for storage. Each central computer receives only a portion of the log data, so the Log Engine on each central computer transfers its portion to a log archive on a dedicated log archive server.

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 Security Manager Interfaces

Security Manager provides several interfaces to help you to monitor the security of your environment:

Security Manager Control Center (Control Center)
Allows you to monitor and resolve alerts about real-time events. Also allows you to create, view, and print Trend Analysis and Forensic Analysis reports of archived log data.

Security Manager Development Console (Development Console)
Allows you to customize and configure Security Manager for your environment using advanced features.

Security Manager Web Console (Web Console)
Allows you to remotely monitor and resolve alerts about real-time events. Also allows you to access Summary reports published using Microsoft SQL Server Reporting Services.

Understanding Requirements and Permissions

Security Manager uses OnePointOp groups and database roles to restrict access to product functionality. These permissions are typically defined at the end of installation with the Security Manager Access Configuration utility (Access Configuration). The **Access Configuration** utility is an interface that allows you to control Security Manager permissions by managing membership in OnePointOp groups.

Access Configuration enforces the use of global or universal domain groups in the OnePointOp groups and creates appropriate database logins. If you need to add a user account, add it to the appropriate domain group you specified with the Access Configuration utility. You can use the Active Directory Users and Computers Administrative Tool to add user accounts to domain groups.

If you need to add an additional domain group, or if you did not specify a domain group at the end of installation, use the Access Configuration utility. For more information about using this utility to modify group memberships, see “Modifying Security Manager OnePointOp Group Membership” on page 301.

For added security, you can also configure security filtering using the Control Center. Security filtering allows you to set permissions for users by computer group, limiting the data users can see or modify depending on your security needs. For more information about security filtering, see the *Installation Guide for NetIQ Security Manager*.

Note

The following Security Manager functions also require you to use an account that is a member of the local Administrators group:

- Installing or upgrading Security Manager
- Uninstalling Security Manager
- Using the Access Configuration utility
- Using the Development Console
- Using the Log Archive Configuration utility
- Using the Configuration Group Password utility

Security Manager Groups

Security Manager provides the following groups to which you can add domain groups during setup.

OnePointOp Reporting

User accounts in the OnePointOp Reporting group have permission to use the Control Center. Reporting users typically use the Control Center to run and view Forensic Analysis reports and view Trend Analysis reports.

Notes

- Members of the OnePointOp Reporting group can also access Summary reports through the Control Center. However, the OnePointOp Reporting group does not control access to Summary reports through either the Microsoft SQL Server Management Studio or the Web Console.

  Use either the Microsoft SQL Server Management Studio or the Report Manager Website to configure permissions for accessing Summary reports. For more information about configuring SQL Server permissions, see the Microsoft SQL Server Management Studio Help.
- In addition, if you want to view or work with Trend Analysis reports, you must use an account that has access to the SQL Server Analysis Services computer used for Security Manager reporting.

OnePointOp Users

User accounts in the OnePointOp Users group have permission to access views in the Control Center. OnePointOp users can monitor the information that Security Manager collects and can resolve alerts but cannot modify product functionality.

OnePointOp Operators

User accounts in the OnePointOp Operators group have all the permissions of the OnePointOp Users group. In addition, operators can modify the information that Security Manager collects and what the product does with the collected information. Operators typically use the Control Center and Development Console.

OnePointOp ConfgAdms

User accounts in the OnePointOp ConfgAdms group have all the permissions of the OnePointOp Operators group. In addition, users in the ConfgAdms group can configure settings in the Configuration Wizard and the Configuration snap-in of the Development Console. Configuration administrators typically use the Control Center, Development Console, Configuration snap-ins, Configuration Wizard, and Agent Administrator.

OnePointOp TrustedServiceAccounts

Accounts from a remotely connected configuration group that are members of the local OnePointOp TrustedServiceAccounts group have access to data in the local configuration group.

You cannot use the Access Configuration utility to add an account to the OnePointOp TrustedServiceAccounts group. Instead use the Active Directory Users and Computers Administrative Tool to add user accounts to the TrustedServiceAccounts group.

OnePointOp System

The OnePointOp System group is created by the installation process and populated with the specified Security Manager service account. Modify the membership in the OnePointOp System group only when you change Security Manager service accounts.

User Interface Requirements

The following list describes the OnePointOp group and database role memberships required to use each Security Manager user interface.

Control Center

To use the Control Center, your user account must be a member of the OnePointOp Reporting group or the OnePointOp Users group. If your user account is a member of the OnePointOp Reporting group, you have access to Forensic Analysis and Trend Analysis reports. If your user account is a member of the OnePointOp Users group, you have access to alert and event views.

Some tasks within the Control Center require membership in other OnePointOp groups.

Task	Group Membership
Launching the Configuration Wizard	OnePointOp ConfgAdms
Creating a processing rule from an existing alert or event	OnePointOp Operators
Viewing the processing rule that generated a specific alert	OnePointOp Operators
Suspending an alert	OnePointOp Operators
Correlating events or alerts	OnePointOp Operators
Launching the Agent Administrator	OnePointOp ConfgAdms
Creating a custom task available to all users	OnePointOp Operators
Modifying a private or public view	OnePointOp ConfgAdms (or the user account that created the view)
Ignoring agent status and stopping ignoring agent status	OnePointOp ConfgAdms
Launching the Module Installer	OnePointOp Operators

Development Console

To use the Development Console, your user account must be a member of the OnePointOp Operators group.

Configuration Snap-in

To use the Configuration snap-in, your user account must be a member of the OnePointOp ConfgAdms group. However, you can still access notification groups if you are a member of OnePointOp Operators group.

Web Console

To use the Web Console, your account must be a member of the OnePointOp Users group. Your account must also have SQL Server permissions to view Summary reports online. For more information about configuring SQL Server permissions, see the Microsoft SQL Server Management Studio Help.

Alert Sentry

To use the Alert Sentry, your account must be a member of the OnePointOp Users, OnePointOp Operators, or OnePointOp ConfgAdms groups.

Understanding the Control Center

The Control Center allows you to monitor and resolve alerts, monitor events, view information about monitored computers, configure Security Manager settings, and create, view, print, and export Trend Analysis or Forensic Analysis reports.

The Control Center can monitor and report on connected **configuration groups**. A configuration group has one database server storing information for a group of monitored computers or devices. The Control Center displays alerts, events, and computers for all connected configuration groups in default or customized views. For more information about creating custom views, see “My Views” on page 61.

The Control Center displays reports for one configuration group at a time. You can easily change configuration groups. For more information about monitoring multiple configuration groups, see “Monitoring Multiple Configuration Groups” on page 256.

The left pane in the Control Center is the **Navigation pane**. When you select a view or folder in the Navigation pane, the center window, called the **Results window**, changes to reflect details for that item. The right pane incorporates both the **Tasks pane** and the **Help pane**. Click the tabs at the top of the Tasks/Help pane to switch between the two panes.

Wizards and Tools

The Control Center also provides wizards and shortcuts to help you configure and begin using Security Manager.

You can use the **Agent Administrator** to create discovery rules, deploy managed agents, authorize unmanaged agents, and configure agentless Windows monitoring. **Discovery rules** are rules that identify computers on which to install an agent or to exclude from monitoring. You must be a member of the OnePointOp ConfgAdms group to use the Agent Administrator.

For more information about adding or removing monitored Windows computers, see "Understanding Discovery and Managed Windows Agent Deployment" on page 193 and "Understanding Unmanaged Windows Agent Installation" on page 199. For more information about deploying and configuring UNIX agents, see the NetIQ UNIX Agent documentation.

You can use the **Configuration Wizard** to configure Security Manager settings and support for certain platforms. Customizing rule and script parameters enables Security Manager to process events, alerts, and responses. You can run the Configuration Wizard at any time to reconfigure these parameters.

You must be a member of the OnePointOp ConfgAdms group to use the Configuration Wizard. Because the Configuration Wizard writes data to the local Security Manager folder, you must also have write permissions on the Security Manager installation folder.

For more information about using the Configuration Wizard to configure Security Manager settings, see "Using the Configuration Wizard" on page 232.

You can use the **Correlation Wizard** to correlate multiple real-time events and define a relationship between the different events. Correlation can bring forward events that seem innocuous separately but may indicate a concerted attempt to breach your systems when viewed together.

Using the Correlation Wizard, you can define which events you want to correlate and what response you want Security Manager to take when the correlated events occur. For more information about correlating events, see "Correlating Events" on page 84.

You can use the **Module Installer** to install or update NetIQ modules. You can either download modules from the NetIQ AutoSync server or from folders on your network. You must be a member of the OnePointOp Operators group to use the Module Installer. For more information about using the Module Installer, see "Installing New or Updated Modules" on page 183.

You can also access published Summary reports created using Microsoft SQL Server Reporting Services and SQL Server Business Intelligence Development Studio. Before viewing reports, configure the Web address for the Report Manager Website. You must have the appropriate SQL Server permissions to view reports.

For more information about configuring the Report Manager Website address, see "Configuring Web Addresses" on page 294. For more information about custom Summary reports, see "Working with Summary Reports" on page 166.

Starting the Control Center

To work with reports and monitor alerts and events, start the Control Center.

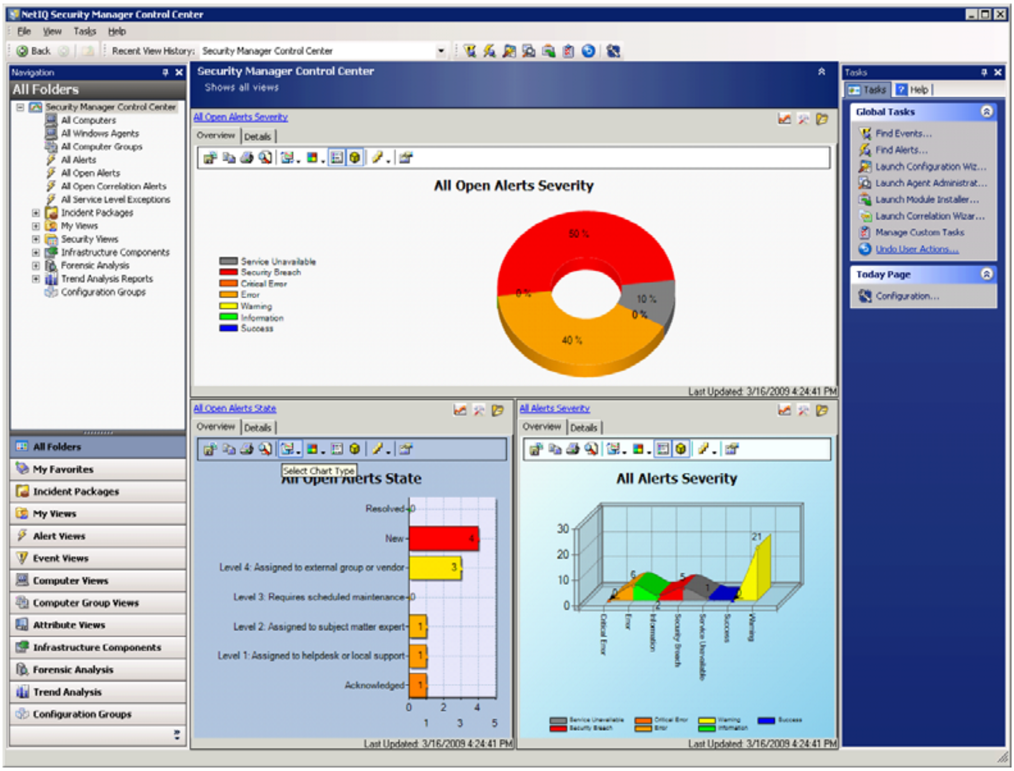
To start the Control Center:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Users, Operators, Reporting, or ConfgAdms groups. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. ***If you are starting Control Center for the first time on a user interface only computer,*** specify the central computer to which you want to connect and click **OK**.

Control Center Today Page

The Control Center Today Page allows you to view high-level graphs and charts displaying the current state of all connected configuration groups.

The following figure illustrates the Control Center Today Page.



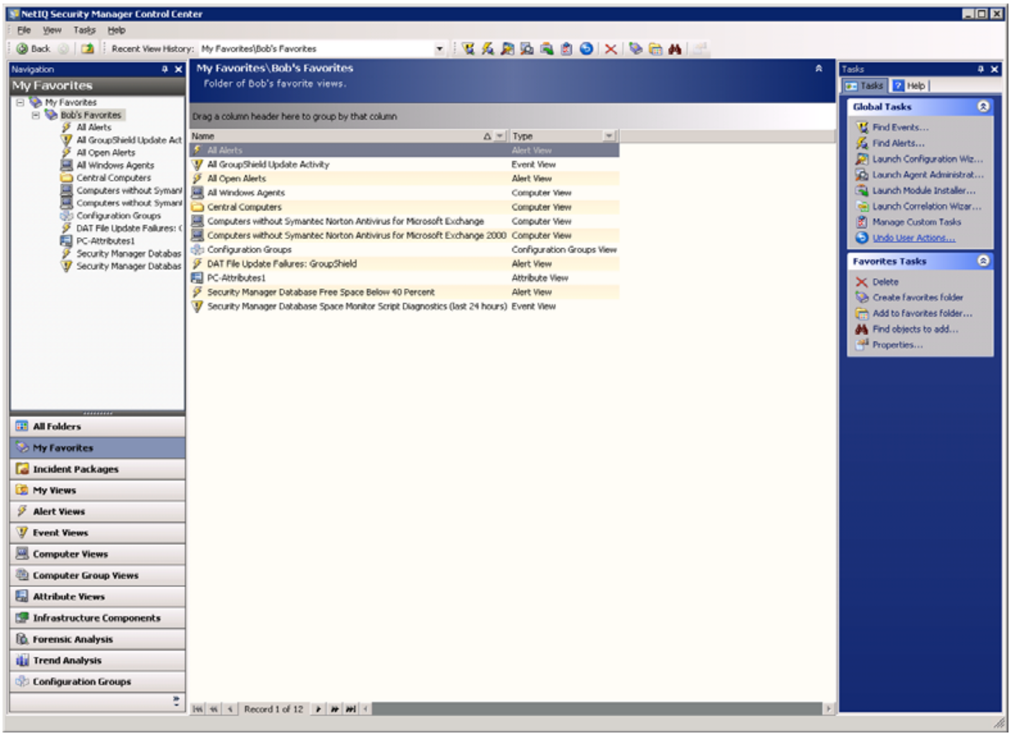
To display the Control Center Today Page, click **All Folders**, and then click **Security Manager Control Center** in the Navigation pane of the Control Center.

You can customize the Today Page to include several different types of charts or graphs. For more information about configuring the Control Center Today Page, see “Customizing the Control Center Today Page” on page 246.

My Favorites

You can use this view to save your most frequently used Security Manager views and reports, including incident packages, alert views, and more. This view acts as your personal work space and lets you organize your favorites as you see fit. For more information about My Favorites, see “Creating a Favorites Folder” on page 253.

The following figure illustrates the My Favorites window.

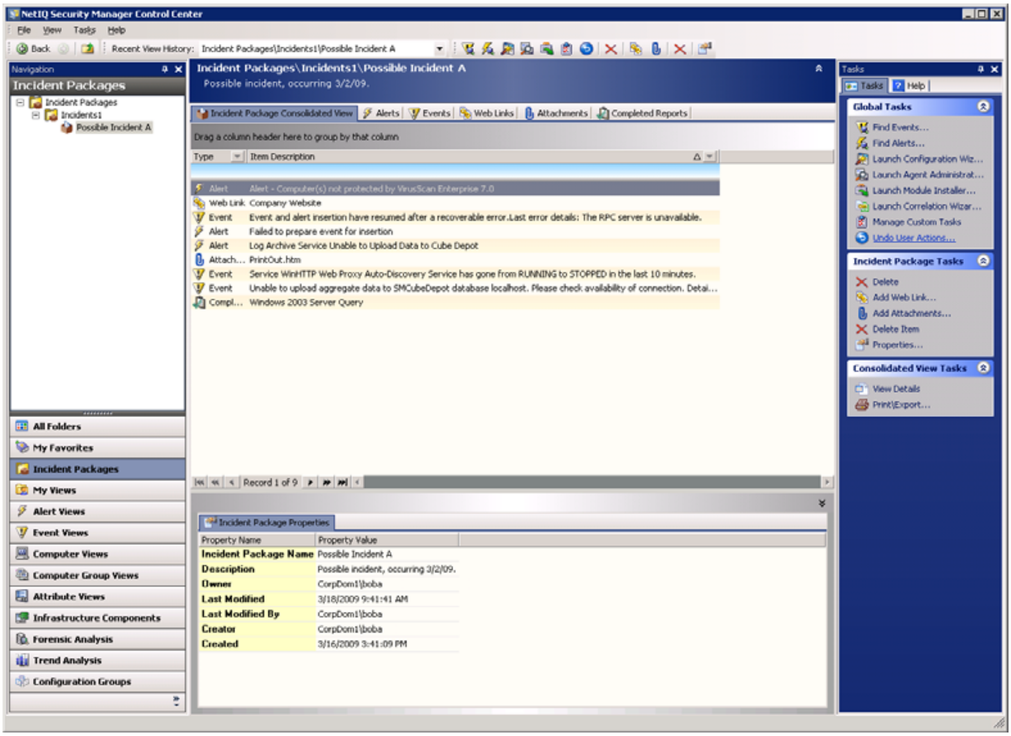


Name	Type
All Alerts	Alert View
All GroupShield Update Activity	Event View
All Open Alerts	Alert View
All Windows Agents	Computer View
Central Computers	Computer View
Computers without Symantec Norton Antivirus for Microsoft Exchange	Computer View
Computers without Symantec Norton Antivirus for Microsoft Exchange 2000	Computer View
Configuration Groups	Configuration Groups View
DAT File Update Failures: GroupShield	Alert View
PC-Attributes1	Attribute View
Security Manager Database Free Space Below 40 Percent	Alert View
Security Manager Database Space Monitor Script Diagnostics (last 24 hours)	Event View

Incident Packages

You can use incident packages to collect and organize all pertinent information relating to an incident, including alerts, events, attachments, Forensic Analysis reports, and Web links. You can then use the incident package for research or investigation and share the incident package with other users, storing it indefinitely in Security Manager. For more information about incident packages, see “Understanding Incident Packages” on page 118.

The following figure illustrates the Incident Packages window.



Type	Item Description
Alert	Alert - Computer(s) not protected by VirusScan Enterprise 7.0
Web Link	Company Website
Event	Event and alert insertion have resumed after a recoverable error.Last error details: The RPC server is unavailable.
Alert	Failed to prepare event for insertion
Alert	Log Archive Service Unable to Upload Data to Cube Depot
Attach...	PrintOut.htm
Event	Service WinHTTP Web Proxy Auto-Discovery Service has gone from RUNNING to STOPPED in the last 10 minutes.
Event	Unable to upload aggregate data to SMCubeDepot database localhost. Please check availability of connection. Detai...
Compl...	Windows 2003 Server Query

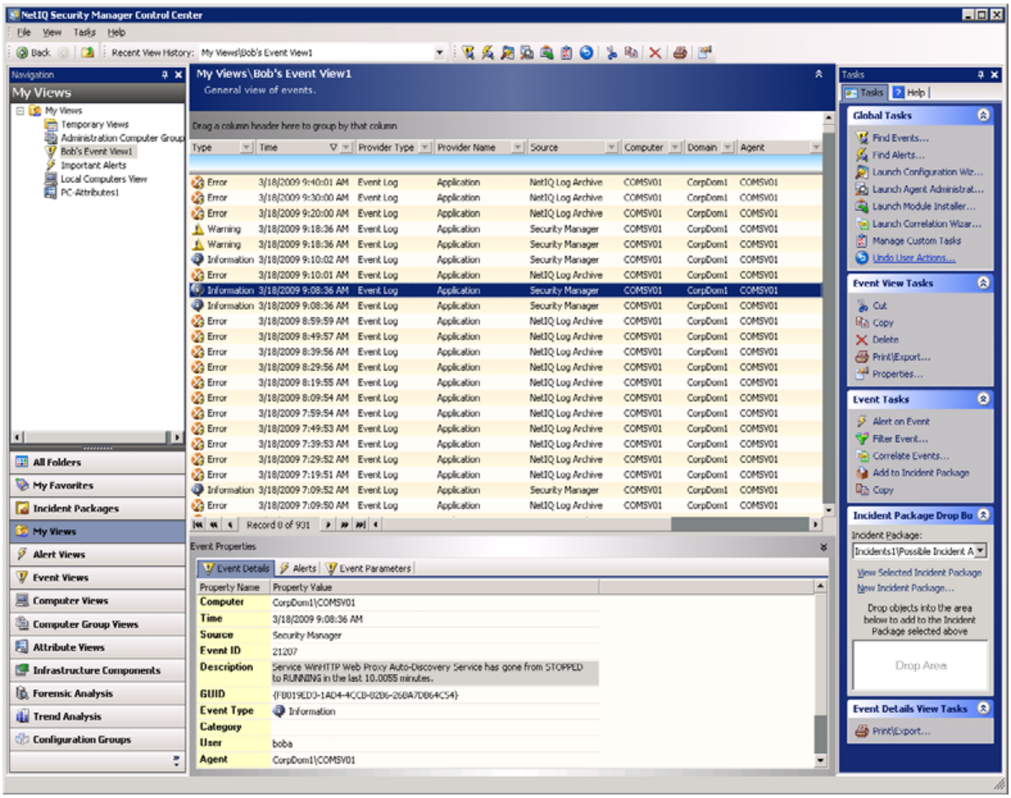
Property Name	Property Value
Incident Package Name	Possible Incident A
Description	Possible incident, occurring 3/2/09.
Owner	CorpDom1\boba
Last Modified	3/18/2009 9:41:41 AM
Last Modified By	CorpDom1\boba
Creator	CorpDom1\boba
Created	3/16/2009 3:41:09 PM

My Views

The My Views folder provides a storage location for private views and temporary views. **Private views** are user-defined views available only to the user who defined them. The user who created private views can access them from any Control Center or Web Console. You can create private views using the Control Center. For more information about private views, see “My Views” on page 61.

Security Manager uses the Temporary Views folder as a temporary storage location during the creation of new views. For example, when you find an event or an alert from the All Computer Groups view, the computer view that Security Manager creates is stored temporarily in the Temporary Views folder. The temporary computer view is removed from the Temporary Views windows when you close Security Manager.

The following figure illustrates the My Views folder.



Type	Time	Provider Type	Provider Name	Source	Computer	Domain	Agent
Error	3/18/2009 9:40:01 AM	Event Log	Application	NetIQ Log Archive	COMSV01	CorpDom1	COMSV01
Error	3/18/2009 9:30:00 AM	Event Log	Application	NetIQ Log Archive	COMSV01	CorpDom1	COMSV01
Error	3/18/2009 9:20:00 AM	Event Log	Application	NetIQ Log Archive	COMSV01	CorpDom1	COMSV01
Warning	3/18/2009 9:18:36 AM	Event Log	Application	Security Manager	COMSV01	CorpDom1	COMSV01
Warning	3/18/2009 9:18:36 AM	Event Log	Application	Security Manager	COMSV01	CorpDom1	COMSV01
Information	3/18/2009 9:10:02 AM	Event Log	Application	Security Manager	COMSV01	CorpDom1	COMSV01
Error	3/18/2009 9:10:01 AM	Event Log	Application	NetIQ Log Archive	COMSV01	CorpDom1	COMSV01
Information	3/18/2009 9:08:36 AM	Event Log	Application	Security Manager	COMSV01	CorpDom1	COMSV01
Information	3/18/2009 9:08:36 AM	Event Log	Application	Security Manager	COMSV01	CorpDom1	COMSV01
Error	3/18/2009 8:59:59 AM	Event Log	Application	NetIQ Log Archive	COMSV01	CorpDom1	COMSV01
Error	3/18/2009 8:49:57 AM	Event Log	Application	NetIQ Log Archive	COMSV01	CorpDom1	COMSV01
Error	3/18/2009 8:39:56 AM	Event Log	Application	NetIQ Log Archive	COMSV01	CorpDom1	COMSV01
Error	3/18/2009 8:29:56 AM	Event Log	Application	NetIQ Log Archive	COMSV01	CorpDom1	COMSV01
Error	3/18/2009 8:19:55 AM	Event Log	Application	NetIQ Log Archive	COMSV01	CorpDom1	COMSV01
Error	3/18/2009 8:09:54 AM	Event Log	Application	NetIQ Log Archive	COMSV01	CorpDom1	COMSV01
Error	3/18/2009 7:59:54 AM	Event Log	Application	NetIQ Log Archive	COMSV01	CorpDom1	COMSV01
Error	3/18/2009 7:49:53 AM	Event Log	Application	NetIQ Log Archive	COMSV01	CorpDom1	COMSV01
Error	3/18/2009 7:39:53 AM	Event Log	Application	NetIQ Log Archive	COMSV01	CorpDom1	COMSV01
Error	3/18/2009 7:29:52 AM	Event Log	Application	NetIQ Log Archive	COMSV01	CorpDom1	COMSV01
Error	3/18/2009 7:19:51 AM	Event Log	Application	NetIQ Log Archive	COMSV01	CorpDom1	COMSV01
Information	3/18/2009 7:09:52 AM	Event Log	Application	Security Manager	COMSV01	CorpDom1	COMSV01
Error	3/18/2009 7:09:50 AM	Event Log	Application	NetIQ Log Archive	COMSV01	CorpDom1	COMSV01

Property Name	Property Value
Computer	CorpDom1\COMSV01
Time	3/18/2009 9:08:36 AM
Source	Security Manager
Event ID	21207
Description	Service WinHTTP Web Proxy Auto-Discovery Service has gone from STOPPED to RUNNING in the last 10.0055 minutes.
GUID	{F8019ED3-1AD4-4CCB-8286-26BA7D864C54}
Event Type	Information
Category	
User	boba
Agent	CorpDom1\COMSV01

Alert and Event Views

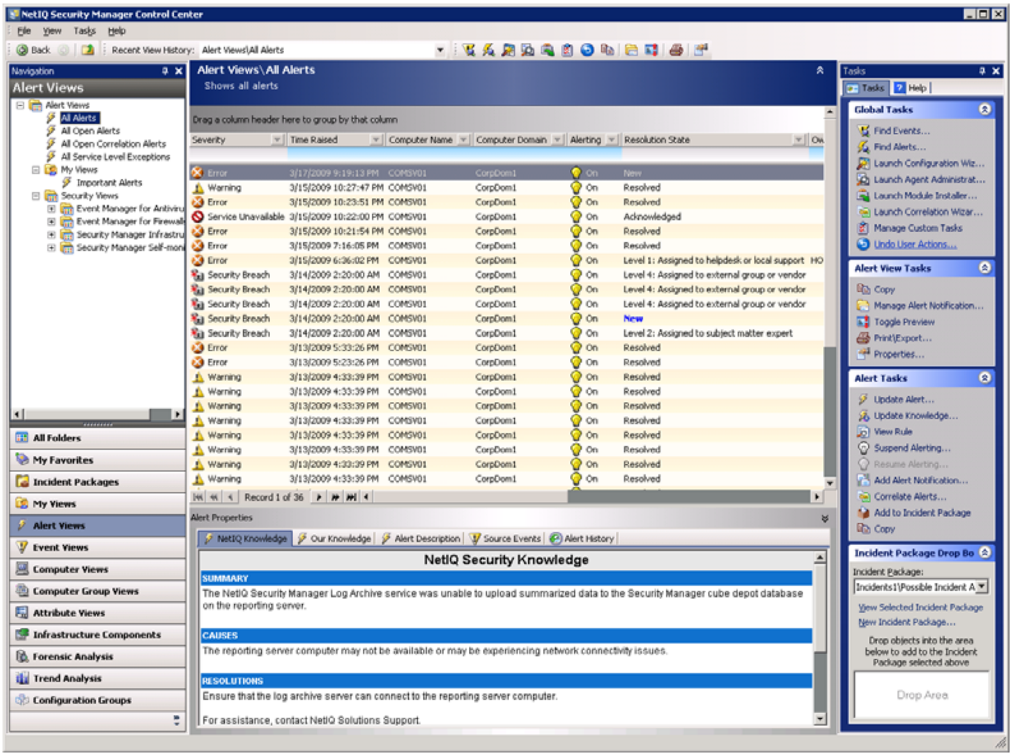
The Control Center provides alert and event views. An alert view is a window that displays a group of alerts that all match a specific set of criteria. An event view is a window that displays all significant occurrences on a computer that match a specific set of criteria. These views allow you to quickly view and resolve real-time alerts from multiple configuration groups. You can also use these views to analyze security data, monitor potential problems, and ensure that no alerts go unresolved.

Security Manager provides default views of the information in the OnePoint database. Default views are specifically the top-level views displayed in the All Folders window, such as All Open Alerts or All Service Level Exceptions. For more information about default views, see “Default Views” on page 59.

In addition to the default Security Manager views, you can install modules that contain Security views. You can install modules for different security-related products, including antivirus software, databases, and firewalls. The Security Views folder in the All Folders window provides a storage location for public alert or event views for Security Manager.

Standard views and any customized views users create in the Security Views folder are public views. **Public views** are views available to any user from any Control Center or Web Console. You can create views using the Control Center. For more information about security views, see “Security Views” on page 60.

The following figure illustrates the default All Alerts view.



Severity	Time Raised	Computer Name	Computer Domain	Alerting	Resolution State	Ow
Error	3/17/2009 9:19:13 PM	COMSV01	CorpDom1	On	New	
Warning	3/15/2009 10:27:47 PM	COMSV01	CorpDom1	On	Resolved	
Error	3/15/2009 10:23:51 PM	COMSV01	CorpDom1	On	Resolved	
Service Unavailable	3/15/2009 10:22:00 PM	COMSV01	CorpDom1	On	Acknowledged	
Error	3/15/2009 10:21:54 PM	COMSV01	CorpDom1	On	Resolved	
Error	3/15/2009 7:16:05 PM	COMSV01	CorpDom1	On	Resolved	
Error	3/15/2009 6:36:02 PM	COMSV01	CorpDom1	On	Level 1: Assigned to helpdesk or local support	HO
Security Breach	3/14/2009 2:20:00 AM	COMSV01	CorpDom1	On	Level 4: Assigned to external group or vendor	
Security Breach	3/14/2009 2:20:00 AM	COMSV01	CorpDom1	On	Level 4: Assigned to external group or vendor	
Security Breach	3/14/2009 2:20:00 AM	COMSV01	CorpDom1	On	Level 4: Assigned to external group or vendor	
Security Breach	3/14/2009 2:20:00 AM	COMSV01	CorpDom1	On	New	
Security Breach	3/14/2009 2:20:00 AM	COMSV01	CorpDom1	On	Level 2: Assigned to subject matter expert	
Error	3/13/2009 5:33:26 PM	COMSV01	CorpDom1	On	Resolved	
Error	3/13/2009 5:23:26 PM	COMSV01	CorpDom1	On	Resolved	
Warning	3/13/2009 4:33:39 PM	COMSV01	CorpDom1	On	Resolved	
Warning	3/13/2009 4:33:39 PM	COMSV01	CorpDom1	On	Resolved	
Warning	3/13/2009 4:33:39 PM	COMSV01	CorpDom1	On	Resolved	
Warning	3/13/2009 4:33:39 PM	COMSV01	CorpDom1	On	Resolved	
Warning	3/13/2009 4:33:39 PM	COMSV01	CorpDom1	On	Resolved	
Warning	3/13/2009 4:33:39 PM	COMSV01	CorpDom1	On	Resolved	
Warning	3/13/2009 4:33:39 PM	COMSV01	CorpDom1	On	Resolved	
Warning	3/13/2009 4:33:39 PM	COMSV01	CorpDom1	On	Resolved	

NetIQ Security Knowledge

SUMMARY

The NetIQ Security Manager Log Archive service was unable to upload summarized data to the Security Manager cube depot database on the reporting server.

CAUSES

The reporting server computer may not be available or may be experiencing network connectivity issues.

RESOLUTIONS

Ensure that the log archive server can connect to the reporting server computer.

For assistance, contact NetIQ Solutions Support.

Computer and Computer Group Views

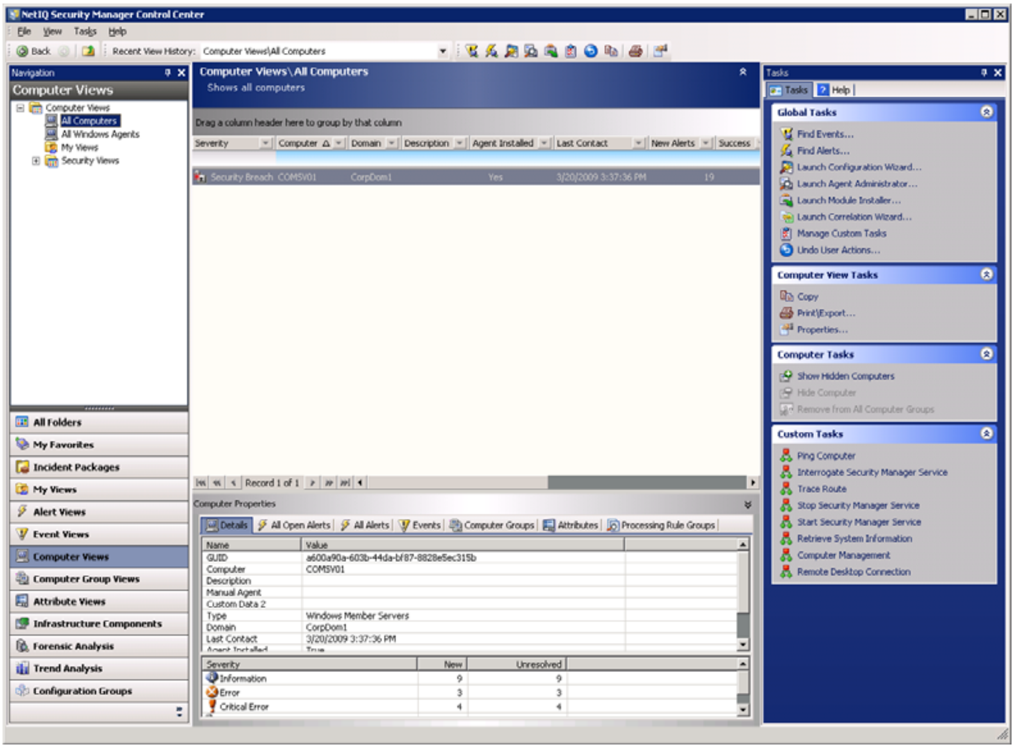
In addition to alert and event views, the Control Center provides computer and computer group views. A computer view is a window that displays information about specified computers in the configuration group. A computer group view displays information about computers in a computer group, such as all Secure IIS Web Servers.

These views allow you to quickly see the status of specific computers and computer groups in your configuration group, including high-priority alerts, agent status, and detailed information about your computers. You can use these views to monitor security issues with a particular set of computers, ensure that alerts in a computer group are promptly resolved, and verify that agent computers are sending data to the central computer.

Security Manager provides default views of the information in the OnePoint database. Default views are specifically the top-level views displayed in the All Folders window, such as All Windows Agents or All Computer Groups. For more information about default views, see “Default Views” on page 59.

In addition to the default Security Manager views, you can install modules that contain Security views. You can install modules for different security-related products, including antivirus software, databases, and firewalls. The Security Views folder in the All Folders window provides a storage location for public computer or computer group views for Security Manager. You can also create public or private computer and computer group views using the Control Center. For more information about security views, see “Security Views” on page 60.

The following figure illustrates the default All Computers view.



Severity	Computer	Domain	Description	Agent Installed	Last Contact	New Alerts	Success
Security Breach	COMSV01	CorpDom1		Yes	3/20/2009 3:37:36 PM	19	

Name	Value
GUID	a600a90a-603b-44da-bf87-8828e5ec315b
Computer	COMSV01
Description	
Manual Agent	
Custom Data 2	
Type	Windows Member Servers
Domain	CorpDom1
Last Contact	3/20/2009 3:37:36 PM
Agent Installed	True

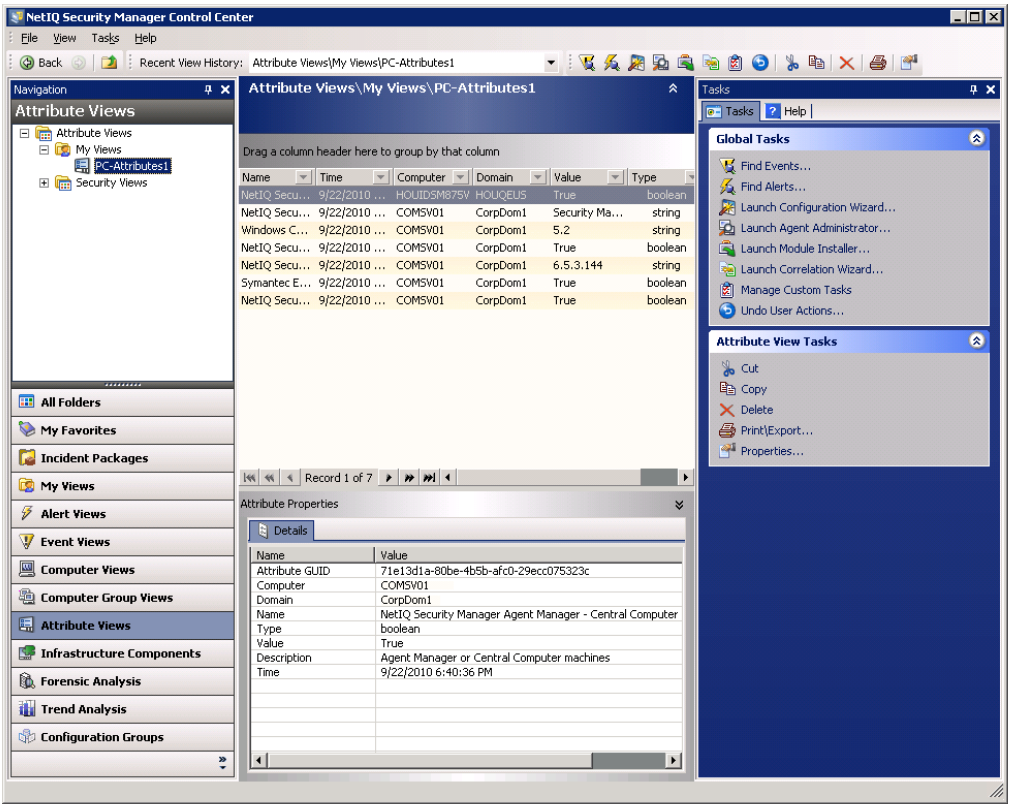
Severity	New	Unresolved
Information	9	9
Error	3	3
Critical Error	4	4

Attribute Views

The Control Center also provides attribute views. An attribute view is a window that displays computer attributes that meet specified criteria. This view type provides information about computer attributes collected on Windows computers in the configuration group. This information includes the date and time when the attribute was collected, and the value of the attribute.

Security Manager does not provide default attribute views. However, you can install modules that contain Security views. You can install modules for different security-related products, including antivirus software, databases, and firewalls. The Security Views folder in the All Folders window provides a storage location for public attribute views for Security Manager. You can also create public or private attribute views using the Control Center. For more information about security views, see “Security Views” on page 60.

The following figure illustrates a typical attribute view.



Name	Time	Computer	Domain	Value	Type
NetIQ Secu…	9/22/2010 …	HOUIDSM875V	HOUQEUS	True	boolean
NetIQ Secu…	9/22/2010 …	COMSV01	CorpDom1	Security Ma…	string
Windows C…	9/22/2010 …	COMSV01	CorpDom1	5.2	string
NetIQ Secu…	9/22/2010 …	COMSV01	CorpDom1	True	boolean
NetIQ Secu…	9/22/2010 …	COMSV01	CorpDom1	6.5.3.144	string
Symantec E…	9/22/2010 …	COMSV01	CorpDom1	True	boolean
NetIQ Secu…	9/22/2010 …	COMSV01	CorpDom1	True	boolean

Name	Value
Attribute GUID	71e13d1a-80be-4b5b-afc0-29ecc075323c
Computer	COMSV01
Domain	CorpDom1
Name	NetIQ Security Manager Agent Manager - Central Computer
Type	boolean
Value	True
Description	Agent Manager or Central Computer machines
Time	9/22/2010 6:40:36 PM

Infrastructure Components

This window provides an overview of the product architecture. You can use the views in the Infrastructure Components window to learn about your deployed Windows agents, central computers, and agentless monitored computers. The Agents, Central Computers, Agentless Monitored Computers, and Ungrouped Computers views allow you to monitor these components.

In these views, you can view Windows agent and central computer status, as well as the status of any agentless monitored computers. You can also configure Security Manager to ignore a specific computer's status. If you know that the agent computer is offline for service reasons, or if you expect one of the computers in your enterprise to be frequently offline, you can specify that the agent status on that computer is ignored. For more information about ignoring agent status, see "Ignoring Agent Status" on page 221.

Security Manager determines the status of the computer using the agent heartbeat. When Security Manager does not receive an expected heartbeat from an agent, the agent status is `Stopped`. The status of an agent is recorded in the Agent Status column. For more detailed information about a particular agent computer, select the computer in the Agents view and review the information in the Computer Views pane.

The following views provide information about Security Manager infrastructure components:

Agents view

Lists all Windows computers in the configuration group on which an agent is installed. The Results window also displays the control level, or **Managed Type**, of the associated central computer.

Agentless Monitored Computers view

Lists all agentless monitored Windows computers or endpoints that proxy agent computers monitor in the configuration group. For more information about agentless monitored computers and proxy agents, see "Understanding Agentless Monitoring and Proxy Agents" on page 200.

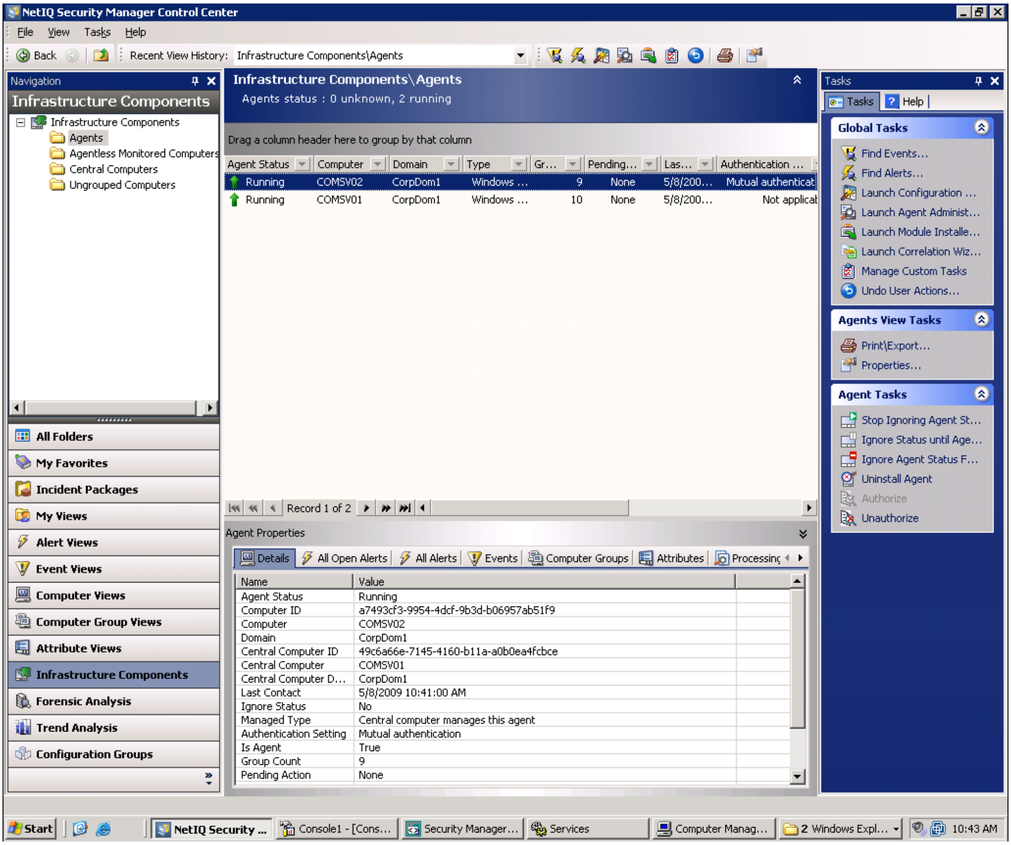
Central Computers view

Lists all computers in the configuration group on which central computer components are installed.

Ungrouped Computers view

Lists all computers or endpoints in the configuration group that do not belong to a computer group. Before an agent computer receives configuration information from the central computer, Security Manager displays information about that computer in the Ungrouped Computers view. Ungrouped computers do not yet belong to any computer group.

The following figure illustrates the Agents view.



Agent Status	Computer	Domain	Type	Gr...	Pending...	Las...	Authentication ...
Running	COMSV02	CorpDom1	Windows ...	9	None	5/8/200...	Mutual authenticat
Running	COMSV01	CorpDom1	Windows ...	10	None	5/8/200...	Not applicat

Name	Value
Agent Status	Running
Computer ID	a7493cf3-9954-4dcf-9b3d-b06957ab51f9
Computer	COMSV02
Domain	CorpDom1
Central Computer ID	49c6a66e-7145-4160-b11a-a0b0ea4fcbce
Central Computer	COMSV01
Central Computer D...	CorpDom1
Last Contact	5/8/2009 10:41:00 AM
Ignore Status	No
Managed Type	Central computer manages this agent
Authentication Setting	Mutual authentication
Is Agent	True
Group Count	9
Pending Action	None

Forensic Analysis

This window allows you to create and view Forensic Analysis reports for network nodes in your enterprise and run saved Forensic Analysis queries. **Network nodes** are network elements with an address that is identifiable on the network and can be a computer, server, firewall, intrusion detection system (IDS) device, router, or switch for which you have configured Security Manager to collect logs.

This window provides links to folders and a wizard to perform Forensic Analysis tasks. The links are defined as follows:

Completed Reports

Allows you to view the results of Forensic Analysis queries.

Pending Reports

Allows you to view a list of pending Forensic Analysis reports and cancel a pending query.

Scheduled Queries

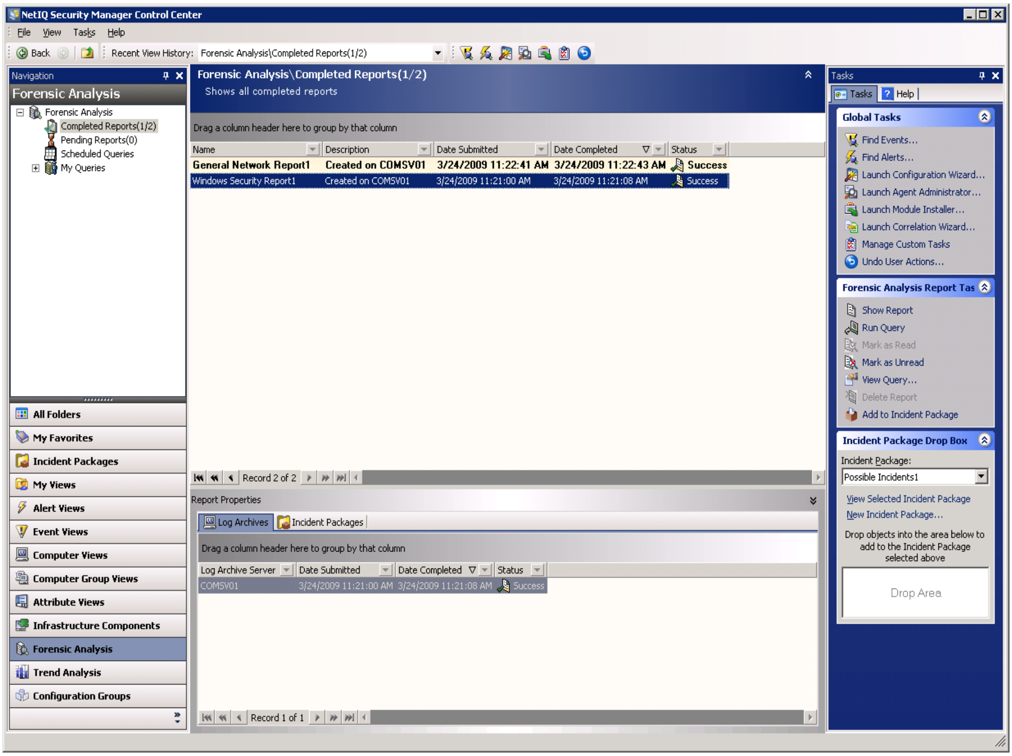
Allows you to view, modify, enable, and disable schedules for Forensic Analysis reports.

My Queries

Allows you to view and run Forensic Analysis queries that you create and save using the Forensic Analysis Wizard. The **Forensic Analysis Wizard** allows you to run Forensic Analysis reports and create report templates. To launch the Forensic Analysis Wizard, on the Tasks menu, click **Forensic Analysis Tasks > Create New Forensic Analysis Query**.

You can filter, sort, and print completed Forensic Analysis reports and export this data to file. For more information about working with Forensic Analysis reports, see "Working with Forensic Analysis Queries and Reports" on page 154.

The following figure illustrates the Forensic Analysis window.



Name	Description	Date Submitted	Date Completed	Status
General Network Report1	Created on COMSV01	3/24/2009 11:22:41 AM	3/24/2009 11:22:43 AM	Success
Windows Security Report1	Created on COMSV01	3/24/2009 11:21:00 AM	3/24/2009 11:21:08 AM	Success

Log Archive Server	Date Submitted	Date Completed	Status
COMSV01	3/24/2009 11:21:00 AM	3/24/2009 11:21:08 AM	Success

Trend Analysis

This window allows you to view and create Trend Analysis reports of log data. Trend Analysis reports allow you to analyze trends using highly interactive graphs of summarized log data stored in a multi-dimensional database called the reporting cube. The reporting cube uses online analytical processing (OLAP) to provide rapid query response of interrelated, summarized data collected daily from network nodes in your enterprise. Trend Analysis reports represent an overall trend rather than up-to-the-moment data.

This window provides links to folders or default Trend Analysis reports. The links are defined as follows:

Saved Reports
Displays a folder containing Trend Analysis reports that you have modified and saved.

Severity Analysis
Displays a Trend Analysis report of the number of log events by severity for all network nodes.

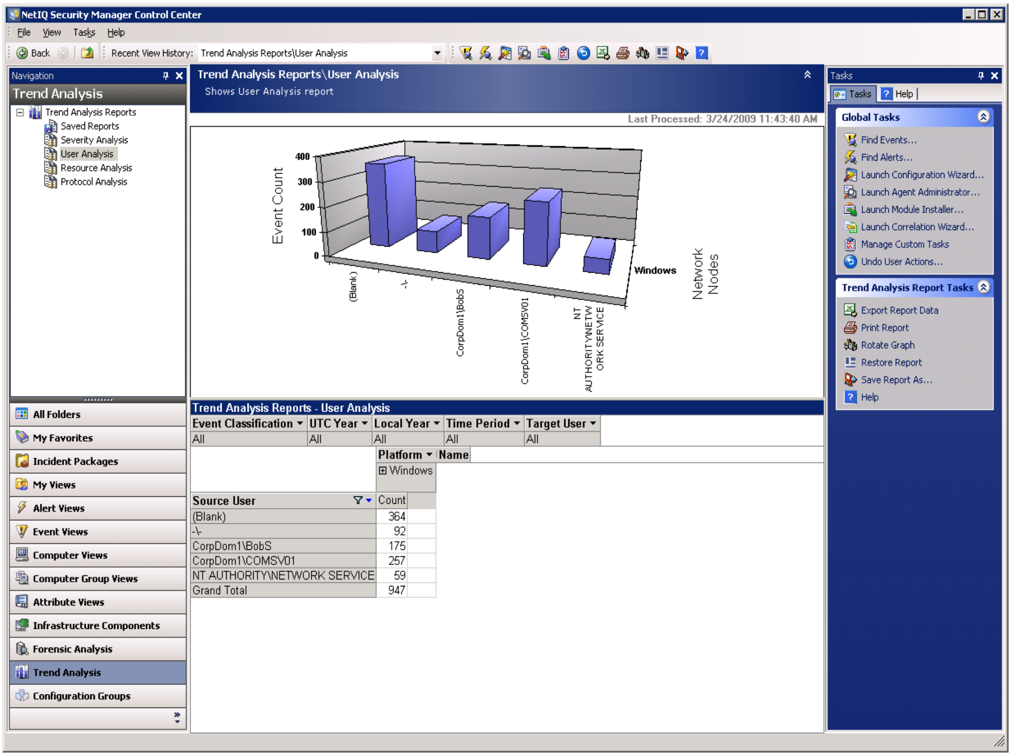
User Analysis
Displays a Trend Analysis report of the number of log events by source user account for all network nodes.

Resource Analysis
Displays a Trend Analysis report of the number of log events caused by a source IP address for all network nodes.

Protocol Analysis
Displays a Trend Analysis report of the number of log events by communication protocol for all network nodes. The network node can provide the communication protocol by acronym, such as TCP, or by the IP protocol number. For more information about the numbers certain network nodes assign to certain protocols, see the documentation for that network node.

You can modify, save, and print Trend Analysis reports, and export report data to a file. For more information about working with Trend Analysis reports, see "Working with Trend Analysis Reports" on page 143.

The following figure illustrates the Trend Analysis window.



Trend Analysis Reports - User Analysis

Event Classification	UTC Year	Local Year	Time Period	Target User
All	All	All	All	All

Source User	Platform: Windows Count
(Blank)	364
-\-	92
CorpDom1\BobS	175
CorpDom1\COMSV01	257
NT AUTHORITY\NETWORK SERVICE	59
Grand Total	947

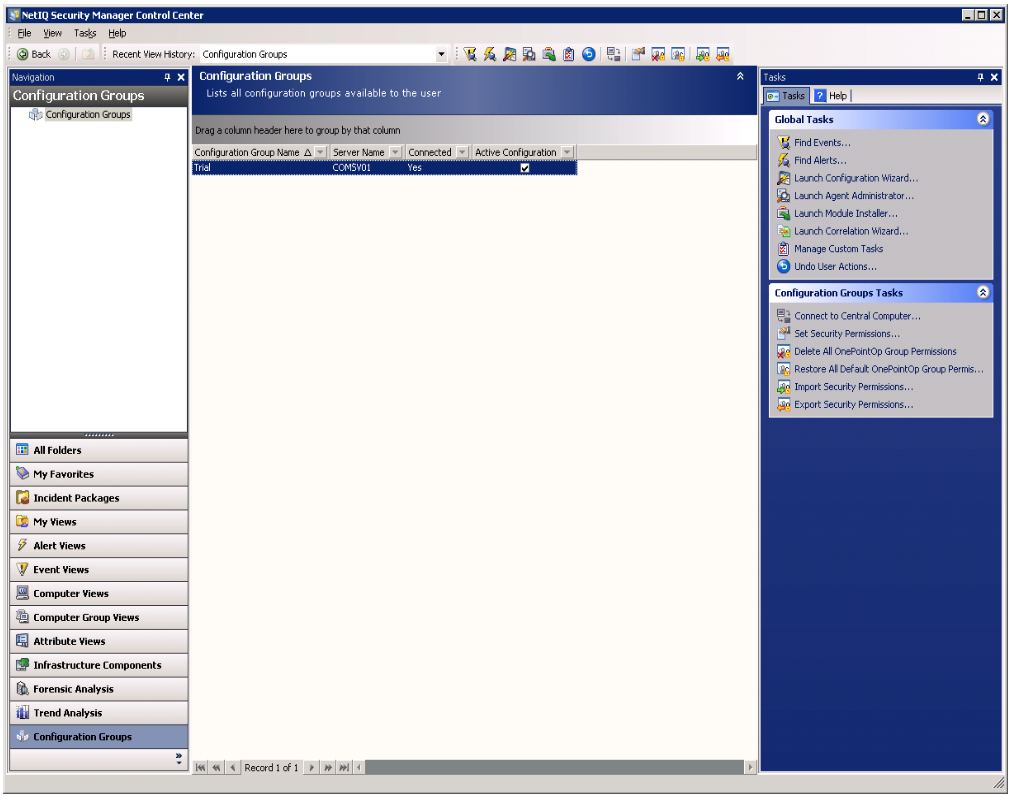
Configuration Groups

This window indicates the status of each configuration group monitored by the Control Center. You can change the central computer to which the Control Center is connected and can also deactivate configuration group connections. For more information about changing your central computer, see “Connecting to a Different Central Computer” on page 245.

The Configuration Groups window allows you to set or review security permissions for different computer groups in Security Manager. You can specify which Windows groups can see information in incident packages, views, or reports. For more information about configuring security filtering, see the *Installation Guide for NetIQ Security Manager*.

You can also select specific different configuration groups on which to run the Configuration Wizard or Agent Administrator. For more information about using the Configuration Wizard, see “Using the Configuration Wizard” on page 232. For more information about using the Agent Administrator to deploy agents, see “Understanding Discovery and Managed Windows Agent Deployment” on page 193.

The following figure illustrates the Configuration Groups window.



Configuration Groups
Lists all configuration groups available to the user

Drag a column header here to group by that column

Configuration Group Name	Server Name	Connected	Active Configuration
Trial	COMSV01	Yes	☑

Record 1 of 1

NetIQ Security Manager Control Center
File
View
Tasks
Help
Back
Recent View History:
Configuration Groups
Navigation
Configuration Groups
Configuration Groups
All Folders
My Favorites
Incident Packages
My Views
Alert Views
Event Views
Computer Views
Computer Group Views
Attribute Views
Infrastructure Components
Forensic Analysis
Trend Analysis
Configuration Groups
Tasks
Tasks
Help
Global Tasks
Find Events...
Find Alerts...
Launch Configuration Wizard...
Launch Agent Administrator...
Launch Module Installer...
Launch Correlation Wizard...
Manage Custom Tasks
Undo User Actions...
Configuration Groups Tasks
Connect to Central Computer...
Set Security Permissions...
Delete All OnePointOp Group Permissions
Restore All Default OnePointOp Group Permis...
Import Security Permissions...
Export Security Permissions...

Understanding the Development Console

The Development Console is a custom Microsoft Management Console (MMC) snap-in used by Security Manager.

The Development Console displays Windows, UNIX, and iSeries computer groups, processing rule groups, notification groups, and advanced rule functionality for a single configuration group. You can create or modify computer groups and processing rules using the Development Console.

You can create or modify **computer attributes**, which are computer characteristics, typically defined by registry keys or values, that you can use when creating Windows computer groups. **Computer groups** are collections of computers with some attribute in common. **Processing rule groups** are collections of related processing rules grouped together for categorization purposes. Processing rule groups allow you to associate more than one rule at a time with a computer group.

You can also create or modify notification groups, scripts, and data providers, which you can use when creating processing rules.

Starting the Development Console

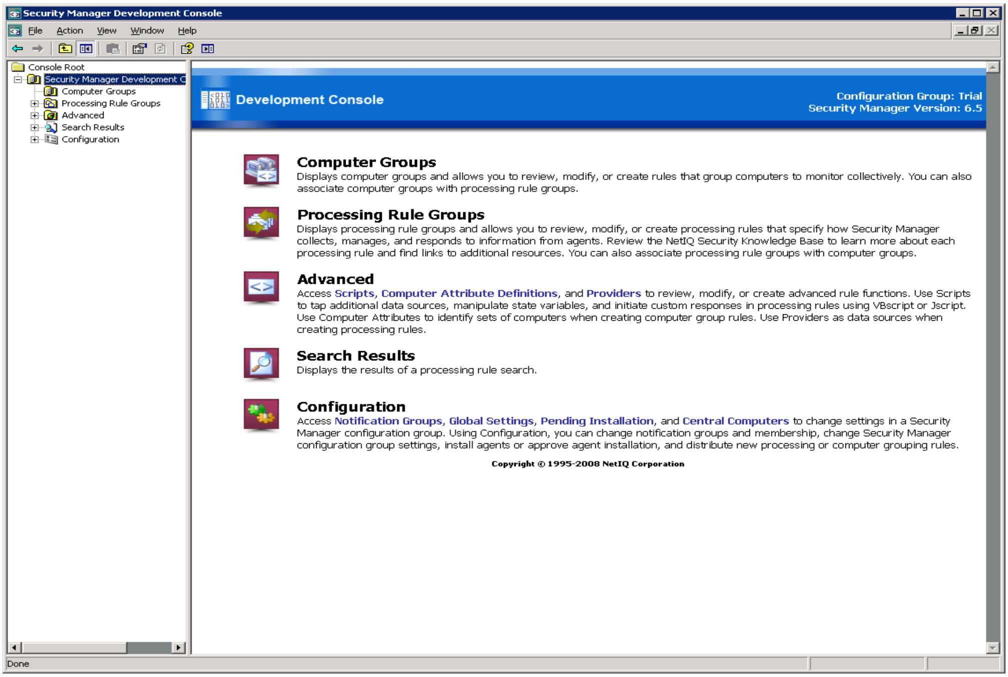
To work with computer groups, computer attributes, notification groups, data providers, or scripts, start the Development Console.

To start the Development Console:

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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.

Development Console Main Page

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

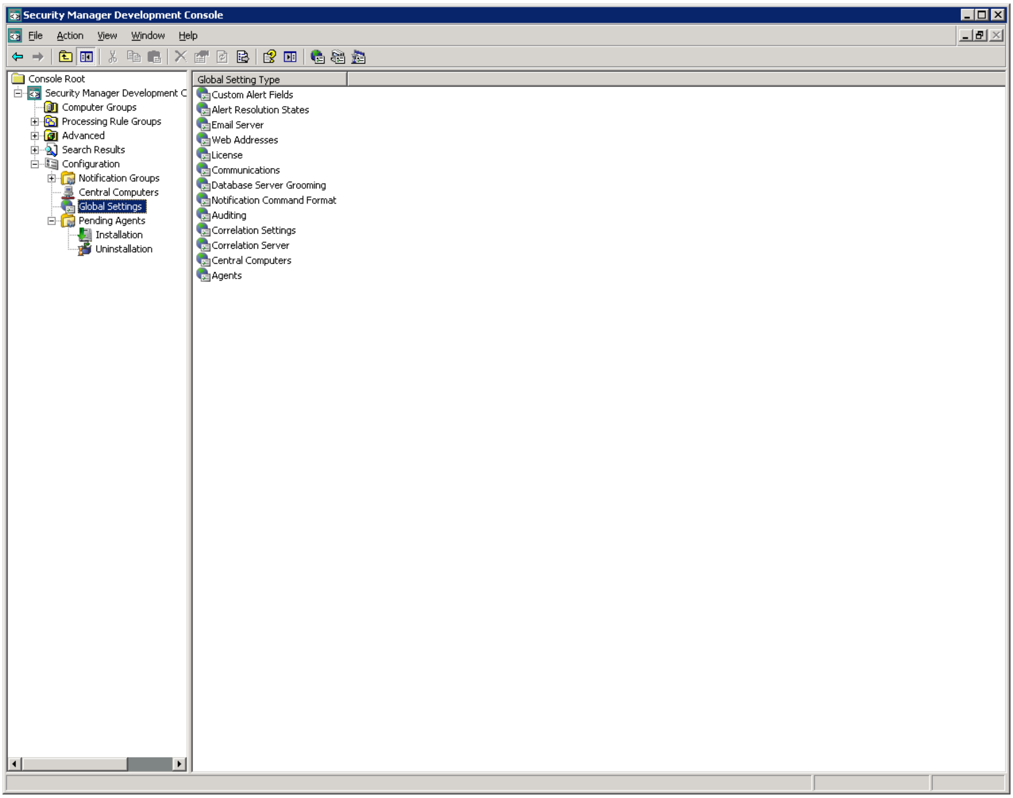
For more information about the Development Console, see the *Programming Guide for NetIQ Security Manager*.

Configuration Snap-In

The Configuration snap-in allows you to manage Windows agents and central computer settings within a single configuration group. You can view and modify global configuration group settings, as well as configure settings for individual central computers or agents. You can also add operators to a notification group. If you want to manage components for several configuration groups, you can add other Configuration snap-ins to the Development Console.

The Configuration snap-in also allows you to view and approve Windows agents before they are automatically installed on computers within the configuration group. The Configuration snap-in also allows you to view and disapprove Windows agents before they are automatically uninstalled from computers within the configuration group.

The default Configuration snap-in is illustrated in the following figure.



When you select Configuration in the left pane, the details pane displays descriptions of the different windows in the Configuration snap-in. Clicking an icon or link in the details pane displays the related window.

Notification Groups Window

Part of a processing rule is a defined response, which specifies the action Security Manager will perform if a specified event, alert, or threshold occurs. Email and paging responses require a notification group.

The Notification Groups window lists all notification groups for the configuration group. You can create new notification groups in this window. In each notification group window, you can create operators for the group and modify notification group properties. To use the Notification Groups window, you must be a member of the OnePointOp Operators group. For more information about adding operators to a notification group, see "Adding Operators to a Notification Group" on page 235.

Central Computers Window

Central computers manage Security Manager components. The central computer installs, uninstalls, and configures Windows agents, distributes rules to agent computers, and controls data flow between all agents and the database server. The central computer can also collect logs for archival and reporting.

The Central Computers window lists all central computers in the configuration group. You can view details of each central computer, including the agents it manages. You can specify when an individual central computer scans the agents assigned to it. You can also specify the service account used by the agents that a central computer installs on Windows computers. A **service account** is a Windows security account used by services to log on to a Windows computer.

Central computers perform managed computer scans to discover Windows computers that match the discovery rules. Central computers also scan agent computers to collect computer attributes older than 24 hours, place computers in or remove computers from computer groups, and install or uninstall Windows agents as appropriate.

You can perform a managed computer scan on demand using the Central Computer window. You can also immediately uninstall a Windows agent on demand.

Note

Security Manager does not automatically deploy agents on UNIX computers. To deploy an agent to a UNIX computer, you must use the UNIX Agent Manager.

For more information about deploying UNIX agents, see the NetIQ UNIX Agent documentation.

You can also approve and install agents using the Agent Administrator. For more information about installing Windows, UNIX, or iSeries agents or modifying central computer properties, see “Administering Agents” on page 191.

Global Settings Window

The Global Settings window allows you to configure Security Manager settings that apply throughout the configuration group. To configure Security Manager settings, you must be a member of the OnePointOp ConfgAdms group. For more information about configuring Security Manager settings, see “Configuring Security Manager” on page 231.

Pending Agents Window

The Pending Agents window allows you to view and either approve or disapprove pending Windows agent installations or uninstallations. This window contains the Installation and Uninstallation windows.

Note

You cannot use the Development Console to approve or disapprove pending UNIX agent installations or uninstallations. For more information about deploying and configuring UNIX agents, see the NetIQ UNIX Agent documentation.

Installation window

Lists Windows computers the central computer has identified as requiring an agent installation or update. Pending installations are disapproved by default. This window is also called the **Pending Agents Installation list**.

Uninstallation window

Lists Windows agents you have selected to uninstall. Pending uninstallations are approved by default.This window is also called the **Pending Agents Uninstallation list**.

Security Manager tracks when an agent needs to be installed on a Windows computer and then adds it to the Pending Agents Installation list, such as in the following instances:

- If you create a computer group
- If you change a computer grouping rule
- If you add a discovery rule
- If you add a new computer that conforms to the selection criteria of a discovery rule
- If a computer configuration changes so that it matches a computer grouping rule or discovery rule

You can specify in the Global Settings window whether you want Windows agents added to the Pending Agents Installation or Uninstallation lists with an approved or disapproved status. Security Manager installs or uninstalls approved agents at the next managed computer scan. Disapproved agents remain in the list until you remove them or exclude them.

You can use the Pending Agents Installation and Uninstallation lists to approve or disapprove all pending installations or uninstallations or approve or disapprove them one at a time.

You can also choose to immediately install or uninstall approved Windows agents. Otherwise, Security Manager installs or uninstalls Windows agents at the next managed computer scan.

For more information about installing Windows agents, see "Understanding Discovery and Managed Windows Agent Deployment" on page 193. For more information about uninstalling Windows agents, see "Uninstalling Windows Agents" on page 223.

You can also approve and install agents using the Agent Administrator. For more information about deploying agents, see "Configuring Security Manager" on page 231.

Understanding the Alert Sentry

The **Alert Sentry** displays a color-coded pop-up message whenever an alert occurs. This message allows you to quickly access the alert information in the Control Center and respond as needed. The Alert Sentry resides in the system tray.

The following figure illustrates the Alert Sentry icon.

The Alert Sentry uses different colors to denote levels of alert severity. **Alert severity** is the property of an alert indicating its seriousness. Examples include Service Unavailable, Security Breach, Critical Error, Error, Warning, Information, and Success.

The colors are defined as follows:

Yellow

A yellow background indicates that the alert is a Warning.

Orange

An orange background indicates that the alert is an Error.

Red

A red background indicates that the alert is a Critical Error, Security Breach, or Service Unavailable alert.

To start the Alert Sentry:

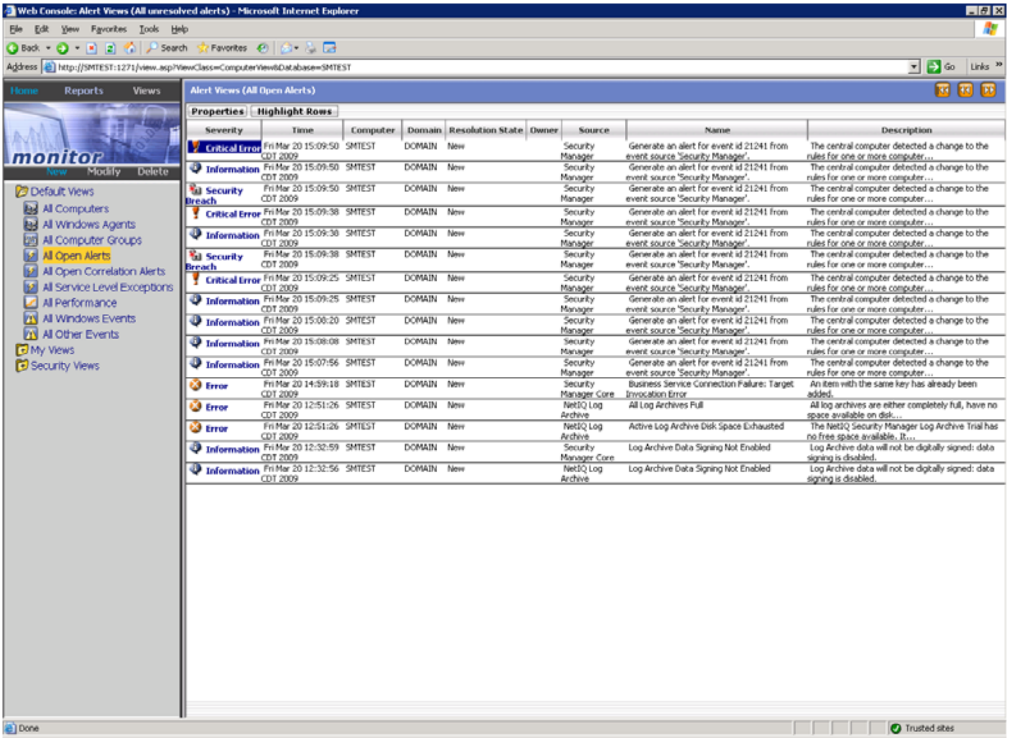
1. Log on to the central computer with a user account that is a member of any OnePointOp group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Click **Alert Sentry** in the NetIQ Security Manager program group.

When Alert Sentry is started, it automatically begins displaying color-coded pop-up messages as alerts occur. If you do not want to receive pop-up messages whenever an alert occurs, close the Alert Sentry using the Alert Sentry icon in the system tray.

Understanding the Web Console

The Web Console provides remote monitoring and easy access for roaming administrators. The Web Console allows you to view real-time data using any Windows platform that supports Microsoft Internet Explorer. For more information about Web Console requirements, see the *Installation Guide for NetIQ Security Manager.*

The following figure illustrates the Web Console.


Web Console: Alert Views (All unresolved alerts) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://SMTEST:1271/view.asp?ViewClass=ComputerView&Database=SMTEST
Go Links
Home Reports Views
monitor
New Modify Delete
Default Views
All Computers
All Windows Agents
All Computer Groups
All Open Alerts
All Open Correlation Alerts
All Service Level Exceptions
All Performance
All Windows Events
All Other Events
My Views
Security Views
Alert Views (All Open Alerts)
Properties
Highlight Rows
Done
Trusted sites

Severity	Time	Computer	Domain	Resolution State	Owner	Source	Name	Description
Critical Error	Fri Mar 20 15:09:50 CDT 2009	SMTEST	DOMAIN	New		Security Manager	Generate an alert for event id 21241 from event source 'Security Manager'.	The central computer detected a change to the rules for one or more computer…
Information	Fri Mar 20 15:09:50 CDT 2009	SMTEST	DOMAIN	New		Security Manager	Generate an alert for event id 21241 from event source 'Security Manager'.	The central computer detected a change to the rules for one or more computer…
Security Breach	Fri Mar 20 15:09:50 CDT 2009	SMTEST	DOMAIN	New		Security Manager	Generate an alert for event id 21241 from event source 'Security Manager'.	The central computer detected a change to the rules for one or more computer…
Critical Error	Fri Mar 20 15:09:38 CDT 2009	SMTEST	DOMAIN	New		Security Manager	Generate an alert for event id 21241 from event source 'Security Manager'.	The central computer detected a change to the rules for one or more computer…
Information	Fri Mar 20 15:09:38 CDT 2009	SMTEST	DOMAIN	New		Security Manager	Generate an alert for event id 21241 from event source 'Security Manager'.	The central computer detected a change to the rules for one or more computer…
Security Breach	Fri Mar 20 15:09:38 CDT 2009	SMTEST	DOMAIN	New		Security Manager	Generate an alert for event id 21241 from event source 'Security Manager'.	The central computer detected a change to the rules for one or more computer…
Critical Error	Fri Mar 20 15:09:25 CDT 2009	SMTEST	DOMAIN	New		Security Manager	Generate an alert for event id 21241 from event source 'Security Manager'.	The central computer detected a change to the rules for one or more computer…
Information	Fri Mar 20 15:09:25 CDT 2009	SMTEST	DOMAIN	New		Security Manager	Generate an alert for event id 21241 from event source 'Security Manager'.	The central computer detected a change to the rules for one or more computer…
Information	Fri Mar 20 15:08:20 CDT 2009	SMTEST	DOMAIN	New		Security Manager	Generate an alert for event id 21241 from event source 'Security Manager'.	The central computer detected a change to the rules for one or more computer…
Information	Fri Mar 20 15:08:08 CDT 2009	SMTEST	DOMAIN	New		Security Manager	Generate an alert for event id 21241 from event source 'Security Manager'.	The central computer detected a change to the rules for one or more computer…
Information	Fri Mar 20 15:07:56 CDT 2009	SMTEST	DOMAIN	New		Security Manager	Generate an alert for event id 21241 from event source 'Security Manager'.	The central computer detected a change to the rules for one or more computer…
Error	Fri Mar 20 14:59:18 CDT 2009	SMTEST	DOMAIN	New		Security Manager Core	Business Service Connection Failure: Target Invocation Error	An item with the same key has already been added.
Error	Fri Mar 20 12:51:26 CDT 2009	SMTEST	DOMAIN	New		NetIQ Log Archive	All Log Archives Full	All log archives are either completely full, have no space available on disk…
Error	Fri Mar 20 12:51:26 CDT 2009	SMTEST	DOMAIN	New		NetIQ Log Archive	Active Log Archive Disk Space Exhausted	The NetIQ Security Manager Log Archive Trial has no free space available. It…
Information	Fri Mar 20 12:32:59 CDT 2009	SMTEST	DOMAIN	New		Security Manager Core	Log Archive Data Signing Not Enabled	Log Archive data will not be digitally signed: data signing is disabled.
Information	Fri Mar 20 12:32:56 CDT 2009	SMTEST	DOMAIN	New		NetIQ Log Archive	Log Archive Data Signing Not Enabled	Log Archive data will not be digitally signed: data signing is disabled.

Using the Web Console, you can see many different views of real-time data. You can see views related to events, alerts, Windows computers, and Windows performance. You can create custom views for specific situations, such as all Critical Error alerts.

You can also use the Web Console to access Summary reports created and published using SQL Server Reporting Services. For more information about Summary reports, see “Working with Summary Reports” on page 166.

The Web Console front page is a portal, which provides customizable, preconfigured views for specific management areas. The Web Console provides monitoring capabilities. It does not provide the capability to define rules or configure product components.

To start the Web Console:

1. Log on to a computer with a user account that is a member of the OnePointOp Users group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.

2. Start **Internet Explorer** in the programs menu.

3. Type `http://`*`WebConsoleServerName`*`:1271` in the **Address** field. *`WebConsoleServerName`* is the central computer acting as the Web Console server.

   Note
   If you are using secure HTTP, type `https://`*`WebConsoleServerName`*`:1271` in the **Address** field.

4. Click **Go**.

5. ***If Internet Explorer prompts you for your user account and password,*** specify the user account and password for the domain in which the Web Console server is located and click **OK**.

6. ***If you want to view reports,*** click **Reports**. You must have the SQL Server Reporting Services Report Server configured before you can access published Summary reports. For more information about configuring the Report Server Web address, see “Configuring Web Addresses” on page 294.

Chapter 3
Working with Real-Time Views

Security Manager enables you to monitor the real-time security of your network using views. Views are collections of related information from the OnePoint database that enable you to monitor and analyze the security status of your network as events occur.

Understanding Views

A **view** is a window in the Control Center and Web Console that displays specified data from the OnePoint database.

Views can contain alerts, which indicate security incidents happening in real-time. You can use views as part of your daily routine to monitor and resolve alerts. You can also use views to analyze and correlate related security data. For example, you can examine the All Open Alerts view to monitor all alerts that still have a status of Open. You can also examine the All Service Level Exceptions view to ensure no alerts are going unresolved. When a critical security alert occurs, you can examine other views to determine if an attack is in progress.

The Control Center provides the following view types:

Alert View

Displays alerts that meet specified criteria from computers in the configuration group. This view type provides information about alerts that have occurred in the configuration group. The All Service Level Exceptions view displays alerts that do not meet service level agreements. Alert information includes the alert severity, resolution state, and owner.

Event View

Displays events that meet specified criteria from computers in the configuration group. This view type provides information about events that have occurred in the configuration group. This information includes the event type, the time the event occurred, and the computer on which the event occurred.

Computer Group View

Displays information about computers in a computer group, such as all Secure IIS Web Servers. This view type provides information about computer groups in the configuration group. This information includes the most severe unresolved alert on a computer in the computer group.

Computer View

Displays information about specified computers in the configuration group. This information includes the highest severity alert on the computer, the last time the agent contacted a central computer, and the number of alerts with a resolution state of New.

Attribute View

Displays computer attributes that meet specified criteria. This view type provides information about computer attributes collected on Windows computers in the configuration group. This information includes the date and time when the attribute was collected, and the value of the attribute.

Default Views

The Control Center provides the following default views of the information in the Security Manager database. These views are available at the top level of the Navigation pane, in the All Folders window. You can also access some default views in the Web Console.

All Computers

Computer view that shows summary data from every agent computer and network node in the configuration group monitored by Security Manager. Each row in the Results window represents one agent computer or network node. The Severity column identifies the highest current unresolved alert on each agent computer or network node. You can view the properties of an agent computer or network node you select in the Computer Views pane. To see all outstanding alerts for the agent computer or network node, click the All Open Alerts tab in the Computer Views pane.

All Windows Agents

Computer view that shows summary data from every Windows agent computer in the configuration group. Each row in the Results window represents one computer. The Severity column identifies the highest current unresolved alert on each computer. You can view the properties of a computer you select in the Computer Views pane. To see all outstanding alerts for the agent computer or network node, click the All Open Alerts tab in the Computer Properties pane.

All Computer Groups

Computer group view that shows a list of computer groups in the configuration group. Each row in the Results window represents one computer group, with the Severity column identifying the highest current unresolved alert in the computer group. You can view details of the computers within the computer group in the Computer Group Properties pane.

All Open Alerts

Alert view that shows a list of alerts that do not have a resolution state of Resolved from all computers in the configuration group. Each row in the Results window represents one alert, with an icon indicating the alert severity. This window can include more than one alert from any computer. You can view the properties of an alert, view the alert knowledge base, change the alert resolution state, configure notification for the alert, or stop alerting on the condition that caused the alert.

All Open Correlation Alerts

Alert view that shows a list of correlation alerts that do not have a resolution state of Resolved for all correlated conditions in the configuration group. Each row in the Results window represents one correlation alert, with an icon indicating the correlation alert severity. You can view the properties of a correlation alert, change the alert resolution state, configure notification for the alert, or stop alerting on the condition that caused the correlation alert. You can also view the correlated events that caused the alert.

All Service Level Exceptions

Alert view that shows all Service Unavailable alerts and all alerts that have been in their current resolution state past the service level agreement time. This view does not include Information or Success alerts. Each row in the Results window represents an alert, with an icon representing the alert severity. You can view the properties of an alert and change the alert resolution state in this view.

Security Views

Each Security Manager product provides additional views. Security views are public views accessible by any user from any Control Center or Web Console.

Security Manager can provide views for several Security Manager products, including Change Guardian for Group Policy, Change Guardian for Windows, Security Manager for Antivirus, Security Manager for Databases, Security Manager for Firewalls, Security Manager for IDS, Security Manager for Routers and Switches, Security Manager for IP Telephony, and Security Manager Self-monitoring.

My Views

Using the Control Center, you can create views that you can access from any Control Center or Web Console in the configuration group. These views can be **private** or **public**.

Private views are accessible only by the user who created them, and are saved in the My Views folder. The user who created these views can access them from any Control Center or Web Console. The Web Console provides some private views by default.

Public views are accessible by anyone and are saved in the Security Views folder. Any user can access these views from a Control Center or Web Console.

You can create views within the My Views and Security Views folders or you can create views and move or copy them into these folders. Moving or copying a view into the My Views folder makes it a private view. Moving or copying a view into the Security Views folder publishes the view for other users to access through any Control Center or Web Console. For more information about creating views, see “Creating Views” on page 66.

Displaying Views

Security Manager provides numerous views that you can access with the Control Center.

When you select a view in the Navigation pane of the Control Center, the Results window displays the name, description, and contents of the view, as well as the relevant properties of the selected alert or event.

Note

You can only view data for monitored computers to which you have access. If the central computer has security filtering configured, you may not be able to view data for all computers in the configuration group.

For more information about security filtering, see “Restricting Information Using Security Filtering” on page 245.

To display a view with the Control Center:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**, and then expand the subfolders until you reach the view you want to see.
4. Click the view.

Working with Computer Group Properties

While you must use the Development Console to perform most tasks related to computer groups, you can use the Control Center to view and modify the properties of existing computer groups.

You can perform several tasks in the Control Center, including specifying computers to include in or exclude from a computer group, associating processing rules with a computer group, or modifying the computer group formula.

Note
You cannot use the Control Center to create new computer groups. Use the Development Console to create new computer groups.

To view or modify the properties of a computer group:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Computer Group Views**.

4. Click **All Computer Groups**.

5. In the Results window, click the computer group you want to view or modify.

6. On the Tasks menu, click **Computer Group Tasks > Properties**.

7. Review properties for the selected computer group.

8. ***If you want to modify the properties of the computer group,*** make changes as necessary, then click **Apply**.

9. After you have finished viewing or modifying computer group properties, click **Close**.

Modifying View Properties

Using the Control Center, you can change the properties of a view, such as limiting the number of items in the view. To modify the properties of a private or public view, you must be the creator of the view, or your user account must be a member of the OnePointOp ConfgAdms group.

To modify the properties of a view:

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 "Understanding Requirements and Permissions" on page 24.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

3. In the Navigation pane, click **All Folders**.

4. ***If you want to modify a private view***, expand **My Views** in the Navigation pane.

5. ***If you want to modify a public view***, expand **Security Views** in the Navigation pane.

6. Expand lower-level folders as necessary.

7. Click the view you want to modify.

8. On the Tasks menu, click ***Type* View Tasks > Properties**, where ***Type*** is the type of view you want to modify.
9. ***If you want to modify the name, description, or number of records displayed for a view,*** click the General tab.
10. ***If you want to modify the view criteria,*** click the Criteria tab.
11. Modify the properties you want to change and click **Finish**. For more information about the fields on a window, see the Help.

Note

You cannot permanently modify the properties of a default Security Manager view. If you modify the properties of a module or top-level view, the modified view reverts to its default properties the next time you open the Security Manager Control Center.

Copying a View

Using the Control Center, you can copy and paste views into the My Views or Security Views folders, or into folders you have created. You can create a new view by copying and pasting an existing view and then modifying the pasted view. You can only copy and paste a view within the current Control Center.

To copy a view:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.
4. ***If you want to copy a public view,*** click **Security Views**.
5. ***If you want to copy a private view,*** click **My Views**.
6. Expand lower-level folders as necessary and click the view you want to copy.

7. On the Tasks menu, click ***Type*** **View Tasks > Copy**, where ***Type*** is the type of the view you want to copy.
8. ***If you want to paste the copied view to a public folder,*** click **Security Views**.
9. ***If you want to paste the copied view to a private folder,*** click **My Views**.
10. Expand lower-level folders as necessary.
11. In the Navigation pane, click the appropriate folder.
12. On the Tasks menu, click **Folder Tasks > Paste**.
13. ***If you want to rename the pasted view***, complete the following steps:
    1. Click the pasted view in the Navigation pane.
    2. On the Tasks menu, click ***Type*** **View Tasks > Properties**, where ***Type*** is the type of the view you want to modify.
    3. Click the General tab.
    4. Type a new name for the copied view in the **View name** field. For more information about the fields on a window, see the Help.
    5. Click **Finish**.
14. Close the Control Center.

Pasting a view into the My Views folder creates a private view accessible only by the person pasting the view. Private views are accessible using any Control Center or Web Console in the configuration group. Pasting a view into the Security Views folder creates a view accessible by anyone using this or other Control Centers or Web Consoles in the configuration group.

Creating Views

You can create views to display specific information from the Security Manager database. You can create views and make them available in the following ways:

- Accessible only by you (private)
- Accessible by any user (public)

Creating Alert Views

Using the Control Center, you can create private or public custom alert views in the My Views or Security Views folders. For more information about alert views, see “Understanding Views” on page 57.

To create an alert view:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Alert Views**.
4. ***If you want to create a private view***, click **My Views** in the Navigation pane.
5. ***If you want to create a public view***, click **Security Views** in the Navigation pane.

   Note

   Views in the **My Views** folder are private and accessible only by the user who created them. Drag and drop views from **My Views** into **Security Views** to make them accessible to all users.

6. Expand lower-level folders as necessary.
7. In the Navigation pane, click the folder where you want to create a new view.
8. On the Tasks menu, click **Folder Tasks > New Alert View**.

9. Type the name of the new Alert View in the **View name** field.
10. Type a short description of the new Alert View in the **Description** field.
11. Specify the number of records to display in the **Number of records** field and click **Next**.
12. Select the criteria for the new Alert View by selecting the appropriate check boxes.
13. In the **View description** pane, click an underlined value to edit each selected criteria.
14. Click **Finish**.

Creating Event Views

Using the Control Center, you can create private or public custom event views in the My Views or Security Views folders. For more information about event views, see "Understanding Views" on page 57.

Notes

- If an event view returns more than the configured maximum number of events, Security Manager may not display the same set of events each time a user accesses the view. To view a consistent set of events, you can increase the maximum number of events displayed, use specific criteria to return a more focused set of events, or modify the configured time period used to filter events.
- Security Manager automatically assigns a default time period criterion of one week to new event views.

To create an event view:

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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Event Views**.

4. ***If you want to create a private view***, click **My Views** in the Navigation pane.

5. ***If you want to create a public view***, click **Security Views** in the Navigation pane.

Note
Views in the **My Views** folder are private and accessible only by the user who created them. Drag and drop views from **My Views** into **Security Views** to make them accessible to all users.

6. Expand lower-level folders as necessary.

7. In the Navigation pane, click the folder where you want to create a new view.

8. On the Tasks menu, click **Folder Tasks > New Event View**.

9. Type the name of the new event view in the **View name** field.

10. Type a short description of the new event view in the **Description** field.

11. Specify the number of records to display in the **Number of records** field and click **Next**.

12. Select the criteria for the new event view by selecting the appropriate check boxes.

13. In the **View description** pane, click an underlined value to edit each selected criteria.

14. Click **Next**.

15. ***If you want to modify the default event view time period,*** specify a particular time range or number of previous days, hours, minutes, or seconds for which you want to display events.

16. Click **Finish**.

Creating Computer Views

Using the Control Center, you can create private or public custom computer views in the My Views or Security Views folders. For more information about computer views, see “Understanding Views” on page 57.

To create a computer view:

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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Computer Views**.
4. ***If you want to create a private view***, click **My Views** in the Navigation pane.
5. ***If you want to create a public view***, click **Security Views** in the Navigation pane.

   Note
   Views in the **My Views** folder are private and accessible only by the user who created them. Drag and drop views from **My Views** into **Security Views** to make them accessible to all users.

6. Expand lower-level folders as necessary.
7. In the Navigation pane, click the folder where you want to create a new view.
8. On the Tasks menu, click **Folder Tasks > New Computer View**.
9. Type the name of the new computer view in the **View name** field.
10. Type a short description of the new computer view in the **Description** field.
11. Specify the number of records to display in the **Number of records** field and click **Next**.
12. Select the criteria for the new computer view by selecting the appropriate check boxes.
13. In the **View description** pane, click an underlined value to edit each selected criteria.
14. Click **Finish**.

Creating Computer Group Views

Using the Control Center, you can create private or public custom computer group views in the My Views or Security Views folders. For more information about computer group views, see “Understanding Views” on page 57.

To create a computer group view:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Computer Group Views**.
4. ***If you want to create a private view***, click **My Views** in the Navigation pane.
5. ***If you want to create a public view***, click **Security Views** in the Navigation pane.

   Note
   Views in the **My Views** folder are private and accessible only by the user who created them. Drag and drop views from **My Views** into **Security Views** to make them accessible to all users.

6. Expand lower-level folders as necessary.
7. In the Navigation pane, click the folder where you want to create a new view.
8. On the Tasks menu, click **Folder Tasks > New Computer Group View**.
9. Type the name of the new Computer Group View in the **View name** field.
10. Type a short description of the new Computer Group View in the **Description** field, and then click **Next**.
11. Select the criteria for the new Computer Group View by selecting the appropriate check boxes.

12. In the **View description** pane, click an underlined value to edit each selected criteria.

13. Click **Finish**.

Creating Attribute Views

Using the Control Center, you can create private or public custom attribute views in the My Views or Security Views folders. For more information about attribute views, see "Understanding Views" on page 57.

To create an attribute view:

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 "Understanding Requirements and Permissions" on page 24.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

3. In the Navigation pane, click **Attribute Views**.

4. ***If you want to create a private view***, click **My Views** in the Navigation pane.

5. ***If you want to create a public view***, click **Security Views** in the Navigation pane.

   Note
   Views in the **My Views** folder are private and accessible only by the user who created them. Drag and drop views from **My Views** into **Security Views** to make them accessible to all users.

6. Expand lower-level folders as necessary.

7. In the Navigation pane, click the folder where you want to create a new view.

8. On the Tasks menu, click **Folder Tasks > New Attribute View**.

9. Type the name of the new Attribute View in the **View name** field.

10. Type a short description of the new Attribute View in the **Description** field.

11. Specify the number of records to display in the **Number of records** field and click **Next**.
12. Select the criteria for the new Attribute View by selecting the appropriate check boxes.
13. In the **View description** pane, click an underlined value to edit each selected criteria.
14. Click **Finish**.

Creating View Folders

You can create view folders within the main My Views and Security Views folders in the Control Center, in order to better organize your views. You can create folders and make them available in the following ways:

- Accessible only by you (private)
- Accessible by any user (public)

For more information about views, see “Understanding Views” on page 57.

To create a view folder:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.
4. ***If you want to create a private view folder***, expand **My Views** in the Navigation pane.

5. ***If you want to create a public view folder***, expand **Security Views** in the Navigation pane.

Note
Folders in the **My Views** folder are private and accessible only by the user who created them. Drag and drop folders from **My Views** into **Security Views** to make them accessible to all users.

---

6. Expand lower-level folders as necessary.
7. In the Navigation pane, click the folder where you want to create a new view folder.
8. On the Tasks menu, click **Folder Tasks > New Folder**.
9. Type the name of the new folder in the **Name** field.
10. Click **OK**.

Chapter 4
Working with Events, Alerts, and Responses

Security Manager enables you to monitor real-time, enterprise security events and alerts you to serious conditions. Security Manager is preconfigured to generate alerts based on specific events. You can also configure Security Manager to generate alerts based on events that may be specific to your enterprise.

Security Manager is preconfigured to respond automatically to specific alerts. You can also configure Security Manager to respond to alerts in your specific environment.

Security Manager uses **rules** to process events, alerts, and responses for Windows, UNIX, and iSeries computers. Rules identify, collect, and process information and define the responses Security Manager takes when specific events occur. For more information about rules, see the *Programming Guide for NetIQ Security Manager*.

Understanding Events

Events make up the majority of the information Security Manager collects. An **event** is a significant occurrence in the system or in an application. Security Manager can perform the following event management functions:

- Monitor events logged in Windows event logs, third-party application logs, and syslog
- Correlate events
- Respond to timed events, missing events, and script-generated events

Security Manager is preconfigured to collect specific events. You can use the Development Console to create rules that configure Security Manager to collect events not already collected by default.

For more information about creating rules, see the *Programming Guide for NetIQ Security Manager.* For more information about working with events, see “Monitoring Events” on page 79.

Windows Events

Windows computers log events in specific event logs, and Security Manager can collect events from these logs. 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. Security Manager collects all events from the Security event log.

DNS Server

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

Directory Service

Records events from the Active Directory service on Windows.

You can use the Development Console to create rules to collect events from Windows logs. For more information about creating rules, see the *Programming Guide for NetIQ Security Manager*.

Correlated Events

Security Manager allows you to correlate detected events and detected events based on alerts or define events that you want Security Manager to collect and correlate.

Detected events are real-time events. You can see detected events and alerts in views. You can use the Correlation Wizard to correlate detected events and detected events based on alerts. For more information about correlating events in a view, see “Correlating Events in a View” on page 85.

If you do not see events or alerts in a view for a condition you want to correlate, you can define the event using the Correlation Wizard. Defining events configures Security Manager to begin detecting and correlating the events. For more information about correlating events or alerts, see the *Programming Guide for NetIQ Security Manager*.

Application Log Events

Some software applications create their own text log files. Security Manager can collect events from application logs. For example, Security Manager can monitor the following application log files:

- IIS World Wide Web Service
- IIS FTP Service

You can use the Development Console to create rules to collect events from application logs. For more information about creating rules, see the *Programming Guide for NetIQ Security Manager*.

Syslog Messages

Systems using syslog can forward syslog messages to another computer, and Security Manager can collect these messages as events. For example, you can collect specific syslog messages from UNIX computers. For more information about collecting syslog messages, see the module documentation for products you want to monitor.

You can also use the Development Console to create rules to collect syslog messages. For more information about creating rules, see the *Programming Guide for NetIQ Security Manager*.

Consolidated Events

Security Manager can consolidate duplicate events using consolidation rules. **Consolidation rules** are processing rules for grouping multiple real-time events from a computer into a single summary event. Consolidating events reduces unnecessary repetition of events that typically occur in a short time. **Event consolidation** combines multiple real-time events into one event to replace many similar events generated in a short time.

For example, by default Security Manager consolidates all IIS 401.1 errors that occur within two minutes. IIS 401 errors are typically the result of permission problems encountered when another computer tries to access a Web page. If ten or more of these events occur in two minutes, an IIS intrusion may be occurring. When ten or more of these events occur, Security Manager can deny the offending computer access to the IIS server.

The consolidated event shows the number of duplicate events that were consolidated during a specified time, as well as 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 consolidated events.

You can create consolidation rules using the Development Console. For more information about creating rules, see the *Programming Guide for NetIQ Security Manager*.

Missing Events

A **missing event** is an event that is supposed to occur within a specified time interval but does not. A **missing event rule** is an event processing rule for generating an alert when particular events do not occur within a specified interval.

For example, you can create a missing event rule to check if an event occurred indicating that a system or file backup operation completed successfully. If the event did not occur, Security Manager can generate an alert.

You can use the Development Console to create rules for events that you expect to occur within a specific time interval. If the event does not occur within the specified interval, it is considered to be missing. For more information about creating rules, see the *Programming Guide for NetIQ Security Manager*.

Timed Events

Security Manager can create **timed events**, which are events automatically created on a timed basis. For example, Security Manager for Antivirus generates a timed event using the DAT File Version Verification (Configuration Wizard) rule. This rule generates an event that triggers a response. The response runs a script that verifies the latest definitions for the configured antivirus software have been installed.

Timed events are not stored in the OnePoint database. For more information about creating rules to generate timed events, see the *Programming Guide for NetIQ Security Manager*.

Monitoring Events

This section provides tasks to help you monitor real-time events using the Control Center. You can also view archival events in the Control Center using Forensic Analysis reports. For more information about Forensic Analysis reports, see “Working with Forensic Analysis Queries and Reports” on page 154. You can also create rules in the Development Console to detect events. For more information about monitoring events, see the *Programming Guide for NetIQ Security Manager*.

Viewing Real-Time Events

Using the Control Center, you can view real-time events collected from all configuration groups, or you can create custom views that let you specify the events you want to see.

To view events:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Event Views**.
4. ***If you want to view specific events,*** complete the following steps:
   a. Expand the appropriate My Views or Security Views folders for the event you want to see.
   b. Click the event view to display all matching events in the Results window. For more information about fields on a window, see the Help.
5. ***If you want to view all events,*** expand **Security Manager Self-monitoring** and click **All Events**. For more information about fields on a window, see the Help.

Finding an Event

Using the Control Center, you can create custom views that display specific real-time events.

To find an event:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

3. In the Tasks pane, click **Find Events**.

4. Follow the instructions until you have finished creating a specified event view. For more information about the fields on a window, click **Help**.

Note
Security Manager creates new views in the Temporary Views folder located in the My Views folder. Views remain in the Temporary Views folder for the duration of your session. To save a temporary view as a custom view, copy or move it from the Temporary Views folder to the My Views folder before you end your session.

Viewing Event Properties

Using the Control Center, you can view the properties for real-time events.

To view event properties:

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 “Understanding Requirements and Permissions” on page 24.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

3. Display the event. For more information about viewing events, see “Viewing Real-Time Events” on page 80.

4. In the Results window, click the event.

5. In the Event Properties window, click the appropriate tab for the properties you want to see. You can view event details, alerts generated from the event, or parameters from events. For more information about the fields on a window or tab, see the Help.

Alerting on or Responding to an Event

Using the Control Center, you can create an event processing rule that generates an alert based on an existing event, and respond with a notification or Simple Network Management Protocol (SNMP) trap.

You can also create an event processing rule using the Development Console. For more information about creating rules, see the *Programming Guide for NetIQ Security Manager*.

Note
If you alert on or specify a response to a particular event using the Control Center, Security Manager creates an event processing rule in the User Actions processing rule group. For more information about working with processing rule groups, see the *Programming Guide for NetIQ Security Manager*.

To generate an alert when an event occurs:

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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Display the event. For more information about viewing events, see "Viewing Real-Time Events" on page 80.
4. In the Results window, click the event.
5. On the Tasks menu, click **Event Tasks > Alert on Event**.
6. Specify the appropriate information. For more information about the fields on a window, click **Help**.

   Note
   If you specify to send an SNMP trap for an alert originating on a UNIX computer, Security Manager generates the SNMP trap on the central computer, regardless of which computer you specify to generate the SNMP trap.

   ---

7. Click **OK**.

8. ***If you want the change to occur immediately,*** select **Apply changes immediately**. Otherwise, the change may take considerably longer to occur, depending on the central computer polling interval and agent heartbeat interval specified in Global Settings.

9. Click **OK**.

Filtering a Real-Time Event

You can use the Control Center to configure Security Manager to ignore specific real-time events. You can create a basic filtering rule based on a particular event you do not consider significant.

Filtering rules help you manage the large number of real-time events that Security Manager collects. You can use filtering rules to selectively store important events and reduce the time spent monitoring low-priority events in your environment. For example, if you do not want to see a specific recurring Information event in your event view, you can filter the event.

When you create a filtering rule, Security Manager does not store events matching the rule in the OnePoint database. However, Security Manager stores all event data in the log archive, regardless of real-time event filtering rules.

An event filtering rule created using the Control Center allows you to filter events based only on the event source and globally unique identifier (GUID). You can create more sophisticated event filtering rules or expand existing event filter rules using the Development Console. For more information about creating or modifying rules, see the *Programming Guide for NetIQ Security Manager*.

Note
You cannot disable or delete an event filtering rule using the Control Center. For more information about working with filtering rules, see the *Programming Guide for NetIQ Security Manager*.

To filter a real-time event:

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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Display the event. For more information about viewing events, see "Viewing Real-Time Events" on page 80.
4. In the Results window, click the event.
5. On the Tasks menu, click **Event Tasks > Filter Event**.
6. ***If you want the change to occur immediately,*** select **Apply changes immediately**. Otherwise, the change may take considerably longer to occur, depending on the central computer polling interval and agent heartbeat interval specified in Global Settings.
7. Click **OK**.

Correlating Events

Correlating events helps you determine if seemingly unimportant events have occurred that, when considered together, indicate a security breach. You can correlate real-time events using the Correlation Wizard either by selecting specific events in the Control Center and clicking **Correlate Events** or by opening the Correlation Wizard directly and adding or defining events using the wizard.

You can also define events to correlate. Defining events to correlate allows you to customize Security Manager to begin detecting and correlating events that Security Manager does not detect by default. For more information about correlating events, see the Help or the *Programming Guide for NetIQ Security Manager*.

You can also define a response for Security Manager to initiate when the correlated events occur. Security Manager can respond to correlated events by generating a correlation alert or by sending a notification to a notification group. By default, Security Manager sends notifications to the Security Specialists notification group installed with the Correlation for Security Manager module for all correlation alerts with a severity of Critical Error or higher. For more information about responses, see “Understanding Responses” on page 94.

Correlating Events in a View

You can select events or alerts in a view to launch the Correlation Wizard. Selecting events in a view allows you to launch the Correlation Wizard with those events. Selecting an alert in a view allows you to correlate the event that generated the alert.

To correlate events in a view:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Display the event. For more information about viewing events, see “Viewing Real-Time Events” on page 80.
4. In the Results window, select the events you want to correlate.
5. On the Tasks menu, click **Event View Tasks > Correlate Events** to launch the Correlation Wizard.
6. Complete the wizard to correlate events. For more information about fields on a window, see the Help.
7. Click **Finish** to save the correlation rule. 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.

For more information about forcing the processing rule changes to take immediate effect, see the Help or the *Programming Guide for NetIQ Security Manager*.

Adding Events to a Correlation Rule

You can also create a correlation rule without selecting events in the Control Center by adding events or alerts directly using the Correlation Wizard. You can select specific events or alerts or configure the Correlation server to match all events against specific criteria.

For more information about defining events using the Correlation Wizard or adding events or alerts to a correlation rule, see the *Programming Guide for NetIQ Security Manager*.

To add events to a correlation rule:

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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Tasks pane, click **Global Tasks > Launch Correlation Wizard**.
4. Complete the wizard to correlate events. For more information about fields on a window, see the Help.
5. Click **Finish** to save the correlation rule. 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.

For more information about forcing the processing rule changes to take immediate effect, see the Help or the *Programming Guide for NetIQ Security Manager*.

Understanding Alerts

An alert indicates the severity, or importance, of an event or performance threshold. Typically, alerts indicate potential problems. Alerts can also indicate informational events or events classified as "None." Alerts help you prioritize conditions.

Alerts help you analyze events and performance thresholds to detect conditions and ensure Security Manager brings the condition to your attention. Security Manager is preconfigured to provide alerts about Security Manager events and other important events and thresholds.

You can also customize Security Manager to create alerts for other events or to create correlation alerts for multiple events. **Correlation alerts** indicate the severity of a condition detected by analyzing a stream of events.

An alert lifecycle encompasses several stages, from origination to resolution. For more information about monitoring and resolving alerts, see “Monitoring Alerts” on page 100. For more information about performance thresholds, see the *Programming Guide for NetIQ Security Manager.*

Alert Severity

Security Manager assigns an alert severity to alerts. The alert severity allows you to determine at a glance the importance of the indicated condition. Alert severities are defined as follows:

Icon	Definition
🚫	**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.
ℹ	**Information.** Identifies an alert that simply provides information.

Icon	Definition
✓	**Success.** Identifies an alert that indicates a successful event or operation.
[Blank]	**No alerts.** Indicates that no alerts are present.

Correlation alert severities are defined as follows:

Icon	Definition
🚫	**Service Unavailable.** Identifies correlation alerts generated for missed agent heartbeats and other events indicating that an application or service is unavailable to its users.
✱	**Security Breach.** Identifies a correlation alert that indicates a security compromise has occurred. Systems on the network are at risk.
!	**Critical Error.** Identifies a correlation alert that indicates a serious problem needing attention immediately.
⊗	**Error.** Identifies a correlation alert that is important and needs attention soon.
⚠	**Warning.** Identifies a correlation alert that might indicate future problems or lower priority issues requiring research.
ℹ	**Information.** Identifies a correlation alert that simply provides information.
✓	**Success.** Identifies a correlation alert that indicates a successful event or operation.
[Blank]	**No alerts.** Indicates that no alerts are present.

Archival events have different severity levels that map to alert severities. For more information about archival event severity levels, see “Archival Event Severity Levels” on page 134.

Duplicate Alert Suppression

Event floods 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 flood, receiving multiple alerts for the same event within a short time is more annoying than useful. Security Manager can provide duplicate alert suppression. **Duplicate alert suppression** is a configuration setting that combines multiple identical alerts that occur within a specified period of time into one alert.

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 the Web Console then display only a single alert. The alert properties indicate the number of alerts that were combined in the **Repeat Count** field. For more information about viewing alert properties, see “Viewing Alert Properties” on page 110.

You can enable duplicate alert suppression when you create a rule or by modifying an existing rule that generates an alert. You can specify the fields in the alerts, the events, or the thresholds that generated the alerts that must be the same for the alert to be considered a duplicate. For more information about creating rules, see the *Programming Guide for NetIQ Security Manager.*

Alert Response

Rules can define **responses** to an alert. Responses help resolve the issue indicated by the event or alert. Responses can include the following actions:

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

Rules can define more than one response. For example, if a Security Breach alert indicates that a security violation has occurred on a Windows computer, Security Manager can respond by running a batch file that locks out an offending user account and by paging a network administrator. Using the Control Center you can define notification and SNMP responses for alerts generated for Windows and UNIX computers. For more information about responses, see “Understanding Responses” on page 94.

Alert Resolution

When an event or threshold occurs that matches an alert-generating rule, Security Manager generates an alert. You can monitor alerts using the Control Center and the Web Console.

When you monitor alerts, you can read important information about each alert that helps you determine your next action. An alert includes the following properties, among others:

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

For more information about resolving alerts, see “Resolving Alerts” on page 113.

Resolution State

Resolution state is the status of the alert in the alert resolution cycle. Resolution state indicates whether you have begun to resolve the alert. You can change the resolution state of an alert to track resolution progress. For more information about changing a resolution state, see “Changing Alert Resolution States” on page 115. 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 helpdesk or local support is now responsible for this alert.

Level 2: Assigned to subject matter expert

Indicates that a subject matter expert is now responsible for this alert.

Level 3: Requires scheduled maintenance

Indicates that the alert identifies a condition requiring maintenance, which has been scheduled.

Level 4: Assigned to external group or vendor

Indicates that an external group or vendor is now responsible for this alert.

Resolved

Indicates that the condition that generated this alert has been handled or solved.

You can modify or delete the default resolution states (except New and Resolved) and also create your own to meet the needs of your network enterprise. Example custom resolution states might include In Progress or Deferred.

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 before it becomes a **service level exception**.

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 to be a service level exception. The Control Center provides views of all service level exceptions.

Notes

- Security Manager can autoresolve alerts, depending on database server grooming settings. Security Manager automatically resolves and deletes alerts from the OnePoint database after a specified time period. For more information about configuring grooming settings, see “Configuring Database Grooming” on page 262.
- Scripts can also change alert resolution states. For example, if you run a script to resolve an alert condition, the script can also change the resolution state to Resolved. For more information about scripts, see the *Programming Guide for NetIQ Security Manager.*

Resolution History

Security Manager automatically tracks and records all changes to alert properties, including changes made by a rule, changes made by scripts, and any automatic responses that have occurred. The **alert resolution history** is an automatic audit trail that tracks an alert through the Security Manager alert management work flow.

You cannot edit the automatic alert resolution history. It provides a record of alert resolution. However, you can add your own 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. For more information about adding comments to the resolution history, see “Modifying the Resolution History of an Alert” on page 116.

Knowledge Base

Rules can contain information about a specified event, alert, or performance condition. This information can describe the condition, its importance, or its significance and provide details to help administrators resolve it. This information is stored with the rule and is called the **knowledge base**. When you view the properties of an alert, you can examine the knowledge base. You can add information to the company knowledge base when you create a rule and when you resolve an alert. The **company knowledge base** is information added to alerts or processing rules about resolving the indicated condition.

Some knowledge base information is already provided with Security Manager. This information is the **NetIQ Knowledge Base**. You cannot edit this information.

Over time, the company knowledge base can become invaluable to an organization. It reflects specific knowledge gained through experience, and is available to benefit others in your organization.

Custom Alert Fields

You can create your own custom alert property fields. You can view these fields when you view the properties of any alerts. Custom alert fields might include the following examples:

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

For more information about creating custom alert fields, see “Configuring Custom Fields for Alerts” on page 288.

Other Alert Properties

You can assign an Owner to an alert. The owner is typically the person responsible for tracking and resolving the indicated problem. You can assign an Owner when you create a processing rule that generates an alert, or you can assign an Owner when the alert occurs. Alerts can also contain the source of the alert and an alert description. For more information about assigning an owner to an alert, see "Assigning an Alert" on page 114.

Understanding Responses

A **response** is an action initiated by Security Manager when a specific event or alert occurs, or when a threshold is crossed. Responses help resolve the issue indicated by the event. You can configure Security Manager to automatically respond to a detected condition.

Using the Control Center you can define the following responses to events or alerts:

- Send a notification to a notification group
    - Send an email
    - Send a page
    - Send an external command notification to a Windows computer
- Send an SNMP trap

For more information about configuring Security Manager to respond to alerts or events, see "Alerting on or Responding to an Event" on page 81 and "Defining a Response for an Alert" on page 102.

Security Manager can initiate a subset of responses to events or alerts occurring for UNIX computers. Security Manager can initiate the following responses for UNIX:

- Send a notification to a notification group
  - Send an email
  - Send a page
- Send an SNMP trap

However, if you specify to send an SNMP trap for an alert originating on a UNIX computer, Security Manager generates the SNMP trap on the central computer, regardless of which computer you specify to generate the SNMP trap.

You can also use the Development Console to create or edit rules to define responses. For more information about creating rules, see the *Programming Guide for NetIQ Security Manager.*

Notifications

Sending a notification to security personnel is one way Security Manager can respond when an alert occurs. Notification responses include the following actions:

- Sending an email
- Sending a page
- Sending a notification by external command to a Windows computer

For more information about configuring Security Manager to respond to an alert or event with a notification, see “Alerting on or Responding to an Event” on page 81 and “Defining a Response for an Alert” on page 102.

For notification responses to occur, you must also use the Development Console to configure **notification groups** and specify notification type, operators, and schedules.

Notification Groups

A **notification group** specifies **operators**. An operator is someone who can receive and respond to a notification. Operator properties specify schedule and notification type: email, page, or external command. Schedules indicate the days of the week and hours of the day when the person can be reached by email, page, or external command notification. Using notification groups enables shift-based responsibility for handling responses.

Security Manager provides default notification groups to which you add operators to receive notification from preconfigured rules. For more information about default notification groups, see "Built-in Notification Groups" on page 234. Using the Configuration snap-in, you can also create notification groups and then create operators within the notification group. Operators can belong to more than one notification group. For more information about adding operators to a notification group, see "Adding Operators to a Notification Group" on page 235.

For complete coverage, at least one operator in each notification group must be scheduled to receive an email or page for every hour in every day. If specific times are not included in at least one operator's schedule, then no one is notified if the processing rule match occurs during that time.

For example, a default notification group is titled Security Manager Administrators. Alert responses can include notifying the Security Manager Administrators notification group. The operators within the Security Manager Administrators notification group are individuals whose schedules indicate when they can receive a notification. When an alert or event associated with a notification response occurs, Security Manager notifies the operators whose schedules indicate their availability.

Email

Security Manager can send an email to a notification group when an associated alert or processing rule match occurs. Security Manager supports SMTP for email notifications. Security Manager also supports additional authentication options for email notifications, including SSL.

You can configure email notifications in the Global Settings area of the Configuration Wizard. For more information about starting and using the Configuration Wizard, see "Using the Configuration Wizard" on page 232.

Note

If you want to use SSL to authenticate SMTP email notifications, you must install a valid server certificate on the SMTP server.

For more information about configuring SMTP and SSL, see the documentation for your email server.

For example, you might want a network administrator to receive an email each time an alert occurs indicating a computer is not protected by antivirus software. You can configure Security Manager to send a notification response to the Network Administrators notification group each time the alert occurs. You can set the notification type to email in the operator properties.

You can also create an alert processing rule that sends an email response to a specified notification group for every alert of a particular type from a processing rule group.

You can specify information to include in the email, including, but not limited to, the following information. For more information about customizing email notifications, see the *Programming Guide for NetIQ Security Manager.*

- Computer name generating the alert or event
- Alert description
- Time of the alert or event
- Alert severity
- Alert resolution state

If an application or computer produces an event flood, and the event is one that calls for an email response, you could potentially receive hundreds of identical emails. Security Manager can suppress duplicate alerts so that you will see only one alert and receive only one email. For more information about duplicate alert suppression, see "Duplicate Alert Suppression" on page 89. For more information about event consolidation, see "Consolidated Events" on page 78.

Paging

Security Manager can send a page to designated operators when an alert occurs. A third-party paging service is required. Your paging service must provide an SMTP email service for Security Manager paging to work. Security Manager paging works by sending an email to the paging service, which forwards the email to the appropriate paging recipient. The email address and times during which Security Manager can send page notifications is defined in the properties for each operator.

For example, you might want a network administrator to be paged each time an alert occurs indicating a computer is not protected by antivirus software. You can set the notification type to page in the operator properties. When the alert occurs, Security Manager could page the Network Administrators notification group. The pager message could include the name of the computer generating the alert and the event text.

You can also customize the parameters and text in a paging notification. For more information about customizing paging notifications, see the *Programming Guide for NetIQ Security Manager.*

External Command

Security Manager provides paging through the SMTP email service. You might also want to use another paging software application to avoid paging through the SMTP email service.

You can use third-party paging applications to notify operators of a detected condition. Third-party paging applications typically require access to a modem. You can configure Security Manager to use an external command line to run paging software. You can configure Security Manager by specifying a notification response to the alert and setting the notification type to external command in the operator properties. For more information about running a third-party paging application from the command line, see the paging software documentation.

For more information about configuring modem paging, see the *Programming Guide for NetIQ Security Manager.*

Command or Batch Files

You can view a rule to add a command or batch file response to an existing event processing rule. The next time the alert occurs, Security Manager runs the batch file or command. For more information about viewing rules, see “Viewing the Rule that Generated an Alert” on page 112.

You can also use the Development Console to create a rule that configures Security Manager to run a command or batch file when a specified alert or event occurs. You can run the command or batch file on the agent or central computer.

For example, you can create a rule that detects if a Windows service has stopped. The rule can generate an alert and respond by running a command or a batch file that restarts the service. For more information about creating rules using the Development Console, see the *Programming Guide for NetIQ Security Manager.*

State Variables

Security Manager provides state variables to allow you to correlate events. You can create a rule to add a state variable response to an existing event processing rule. The next time the alert occurs, Security Manager updates the state variable, allowing you to track how frequently the alert and the triggering event occur. For more information about viewing rules, see “Viewing the Rule that Generated an Alert” on page 112.

You can also use the Development Console to create a rule that configures Security Manager to set or change state variables when a specified event or alert occurs. For more information about rules, see the *Programming Guide for NetIQ Security Manager.*

Scripts

Security Manager runs scripts on Windows computers in response to alerts or events. Scripting capabilities provide advanced monitoring and responses. You can use standard Microsoft scripting languages to create scripts for Security Manager to implement, or you can use the scripts included with Security Manager. For more information about scripts, see the Help or the *Programming Guide for NetIQ Security Manager.*

SNMP Traps

Security Manager provides SNMP capabilities to allow integration with other network monitoring applications. You can configure the Security Manager to generate an SNMP trap when an alert or an event occurs. An SNMP-ready monitoring application can then capture these traps. You can ensure the event information is captured and stored in the database, as well as passed on to other network monitoring applications.

For example, you can configure Security Manager to send an SNMP trap whenever an alert occurs indicating that a vital Windows service has stopped. The product then sends an SNMP trap that contains all the event information in the SNMP trap variable bindings.

You can configure Security Manager to send SNMP traps from the Windows agent or central computer. The advantage of sending a trap from the Windows agent computer is that in most cases the trap originates on the computer experiencing a problem. This is a requirement if you are integrating Security Manager with other monitoring tools. This solution requires SNMP installation and configuration of SNMP on each agent computer. Sending a trap from the central computer reduces SNMP installation and configuration. For more information about configuring Security Manager to capture SNMP traps, see the *Programming Guide for NetIQ Security Manager*.

If you specify to send an SNMP trap for an alert originating on a UNIX computer, Security Manager generates the SNMP trap on the central computer, regardless of which computer you specify to generate the SNMP trap.

For more information about configuring Security Manager to respond to an alert or event with a notification, see “Alerting on or Responding to an Event” on page 81 and “Defining a Response for an Alert” on page 102.

Monitoring Alerts

Security Manager provides predefined alerts specific to the monitored environment or application. You can monitor alerts using the Control Center or the Web Console.

Monitoring alerts lets you respond immediately to indicated problems. Alerts provide detailed information about security conditions. You can read an alert, its associated knowledge bases, and its resolution history to see what responses have been performed and to determine what further actions you need to take to resolve the indicated condition.

Monitoring alerts requires completing specific tasks that encompass an alert's lifecycle. The lifecycle of an alert comprises several stages:

Defining alerts

Creating alerts and defining automatic responses to alerts. For more information about creating and defining alerts, see "Defining Alerts" on page 102.

Viewing alerts

Viewing alert properties and knowledge bases to understand the issue causing the alert and determine a resolution. For more information about viewing alerts, see "Viewing Alerts" on page 109.

Resolving alerts

Tracking alerts and changing resolution states. You can also assign an owner to track alerts. For more information about resolving alerts, see "Resolving Alerts" on page 113.

Creating alert knowledge

Adding to the resolution history and company knowledge base. For more information about adding alert knowledge, see "Creating Alert Knowledge" on page 116.

You can monitor alerts using default alert views or custom alert views you created. The Control Center provides default views of alerts, including All Open Alerts and All Service Level Exceptions. You can also create custom views matching criteria you specify, such as Open alerts from a specified source and Alerts that are not Resolved.

Defining Alerts

Security Manager can generate alerts for enterprise conditions that require attention or special action. Security Manager provides predefined alerts for specific monitored environments. These alerts can indicate the following conditions:

Events

When specific events occur.

Missing events

When a specific event does not occur during a specified time.

Crossed thresholds

When a Windows performance counter or WMI numeric value crosses a defined threshold.

Using either the Control Center, you can configure Security Manager to generate an alert based on an event. For more information about generating an alert based on an event, see “Alerting on or Responding to an Event” on page 81.

You can use the Development Console to create rules that define alerts based on events, missing events, and crossed thresholds. For more information about creating processing rules, see the *Programming Guide for NetIQ Security Manager.*

You can also configure Security Manager to initiate a response when an alert occurs. For more information about defining an alert response, see “Defining a Response for an Alert” on page 102.

Defining a Response for an Alert

Security Manager can initiate **responses** to an alert. Responses help resolve the issue indicated by the event or alert. Responses can include the following actions:

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

You can use the Control Center to generate a notification or SNMP trap response.

Security Manager can initiate a subset of responses to alerts occurring for UNIX computers. Security Manager can initiate the following responses for UNIX:

- Send a notification to a notification group
    - Send an email
    - Send a page
- Send an SNMP trap

If you specify to send an SNMP trap for an alert originating on a UNIX computer, Security Manager generates the SNMP trap on the central computer, regardless of which computer you specify to generate the SNMP trap.

Note
If you specify a response for a particular alert using the Control Center, Security Manager creates an alert processing rule in the User Actions processing rule group. For more information about working with processing rule groups, see the *Programming Guide for NetIQ Security Manager*.

For more information about responses, see "Understanding Responses" on page 94.

Notify on Alert

To notify a particular notification group when an alert occurs, you must ensure the notification group contains operators. For more information about adding operators to a notification group, see "Adding Operators to a Notification Group" on page 235.

Note
You can only receive notifications for monitored computers to which you have access. If the central computer has security filtering configured, you may not be able to receive alert notifications for all computers in the configuration group.

For more information about security filtering, see "Restricting Information Using Security Filtering" on page 245.

To notify on an alert:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Display the alert. For more information about viewing alerts, see “Viewing Alerts” on page 109.
4. In the Results window, click the alert on which you want to notify.
5. On the Tasks menu, click **Alert Tasks > Add Alert Notification**.
6. Select the notification type you would like to initiate:
   - **Notify via SNMP trap**
   - **Notify a notification group**
7. Complete the appropriate fields for the specified notification type, and then click **OK**. For more information about the fields on a window, see the Help.

   Note
   If you specify to send an SNMP trap for an alert originating on a UNIX computer, Security Manager generates the SNMP trap on the central computer, regardless of which computer you specify to generate the SNMP trap.

8. ***If you want the change to occur immediately,*** select **Apply changes immediately**. Otherwise, the change may take considerably longer to occur, depending on the central computer polling interval and agent heartbeat interval specified in Global Settings.
9. Click **OK**.

   Note
   Using the Control Center, you can also modify or delete previously created alert notifications.

Modifying Alert Notifications

Using the Control Center, you can also modify or delete previously created alert notifications.

To modify or delete alert notifications:

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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Display the alert. For more information about viewing alerts, see "Viewing Alerts" on page 109.
4. In the Results window, click the alert on which you want to notify.
5. On the Tasks menu, click **Alert View Tasks > Manage Alert Notifications**.
6. Select the appropriate notification from the Alert Notifications list.
7. ***If you want to delete an alert notification,*** click **Delete**.
8. ***If you want to modify an alert notification,*** complete the following steps:
   a. Click **Modify**.

   b. Select the notification type you would like to initiate:

   - **Notify via SNMP trap**
   - **Notify a notification group**

   c. Complete the appropriate fields for the specified notification type, and then click **OK**. For more information about the fields on a window, see the Help.

Note
If you specify to send an SNMP trap for an alert originating on a UNIX computer, Security Manager generates the SNMP trap on the central computer, regardless of which computer you specify to generate the SNMP trap.

9. ***If you want the change to occur immediately,*** select **Apply changes immediately**. Otherwise, the change may take considerably longer to occur, depending on the central computer polling interval and agent heartbeat interval specified in Global Settings.

10. Click **OK**.

Preventing an Alert

Security Manager provides predefined processing rules that generate alerts. Because every enterprise environment is different, you may not care to be alerted for some of the default alerts.

To prevent an alert from occurring again, you can suspend alerting using the Control Center by disabling the processing rule that generates the alert. If you disable a processing rule that has a response specified, such as an email or page notification or a script, the response will no longer run.

If you have configured Security Manager to insert only events matching a processing rule into the database, then the event associated with a disabled processing rule is not inserted into the database.

Disabling the processing rule also means that the central computer will not send that processing rule to agents, reducing traffic.

To disable the rule that generates the alert:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Display the alert. For more information about viewing alerts, see “Viewing Alerts” on page 109.
4. In the Results window, click the alert you want to suspend.
5. On the Tasks menu, click **Alert Tasks > Suspend Alerting**.

6. ***If you want the change to occur immediately,*** select **Apply changes immediately**. Otherwise, the change may take considerably longer to occur, depending on the central computer polling interval and agent heartbeat interval specified in Global Settings.

7. Click **OK**.

Re-enabling a Disabled Alert

In addition to suspending alerts, you can also use the Control Center to re-enable a disabled processing rule that generates an alert.

To re-enable a disabled rule that generates an alert:

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 “Understanding Requirements and Permissions” on page 24.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

3. Display the alert. For more information about viewing alerts, see “Viewing Alerts” on page 109.

4. In the Results window, click the alert you want to re-enable.

5. On the Tasks menu, click **Alert Tasks > Resume Alerting**.

6. ***If you want the change to occur immediately,*** select **Apply changes immediately**. Otherwise, the change may take considerably longer to occur, depending on the central computer polling interval and agent heartbeat interval specified in Global Settings.

7. Click **OK**.

Undoing an Action for an Alert or Event

When you perform an action on an event or alert in the Control Center, Security Manager creates an event processing rule in the User Actions processing rule group. You can use the Development Console to modify a User Actions processing rule, but you can also undo or modify actions performed on some events or alerts using the Control Center.

For example, you can modify an event processing rule you created that generates a particular alert, undo a real-time event filtering rule, modify the notification group to which notifications are sent, or stop notifications from being sent.

Using the Control Center, you can modify actions or processing rules performed or created by any user within the configuration group.

Note
You cannot undo an action or delete a processing rule associated with an existing alert.

For more information about creating rules, see the *Programming Guide for NetIQ Security Manager.*

To undo or modify an action performed on an alert or an event:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. On the Tasks menu, click **Global Tasks > Undo User Actions**.
4. Select the action you want to undo or modify.

5. ***If you want to modify the action,*** complete the following steps:

    a. Click **Modify**.

    b. Specify the appropriate changes. For more information about the fields on a window, click **Help**.

    c. Click **OK**.

    Note
    The modify option is only available for actions involving notifications.

6. ***If you want to completely reverse the action***, click **Undo**.

7. ***If you want the change to occur immediately***, select **Apply change immediately**. Otherwise, the change may take considerably longer to occur, depending on the central computer polling interval and agent heartbeat interval specified in Global Settings.

8. Click **OK**.

9. Click **Close**.

Viewing Alerts

When you monitor alerts using the Control Center or the Web Console, the alert severity tells you at a glance the importance of the indicated condition. The severity of the alert can include the following severities:

- Security Breach
- Critical Alert
- Success
- Information.

Using the Control Center, you can view all alert views. For more information about alert views, see “Understanding Views” on page 57.

To view 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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Alert Views**.
4. ***If you want to view all alerts,*** click **All Alerts**.
5. ***If you want to view all open alerts,*** click **All Open Alerts**.
6. ***If you want to view all open correlation alerts,*** click **All Open Correlation Alerts**. For more information about fields on a window, see the Help.

Viewing Alert Properties

Alert properties show specific information about an alert, including events associated with the alert and a description of the alert.

Using the Control Center, you can view alert properties.

To view alert properties:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Display the alert. For more information about viewing alerts, see “Viewing Alerts” on page 109.

4. In the Results window, click the alert.

5. In the Alert Properties window, click the appropriate tab for the properties you want to see. You can view alert details, events that generated the alert, or knowledge about the alert. For more information about the fields on a window or tab, see the Help.

Viewing Events Associated with an Alert

Alerts are often associated with event occurrences. When the specific event occurs, an event processing rule generates an alert.

Using the Control Center, you can view events associated with an alert.

Note
The Control Center only displays the first 100 instances of a repeated source event associated with a particular alert.

To view the events associated with an alert:

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 “Understanding Requirements and Permissions” on page 24.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

3. Display the alert. For more information about viewing alerts, see “Viewing Alerts” on page 109.

4. In the Results window, click the alert.

5. In the Alert Properties window, click the Source Events tab. For more information about fields on a window, see the Help.

Viewing the Rule that Generated an Alert

If you would like to review the properties of a rule that generates an alert, you can view the rule using the Control Center. Viewing a rule can be useful when you would like to see detailed information about the criteria used to generate the alert, such as the event source or ID. You can also view a rule to add responses that Security Manager initiates when the event or alert occurs.

To view a rule:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Display the alert. For more information about viewing alerts, see “Viewing Alerts” on page 109.
4. In the Results window, click the alert.
5. On the Tasks menu, click **Alert Tasks > View Rule**. For more information about fields on a window, click **Help**.

For more information about rules, see the *Programming Guide for NetIQ Security Manager.*

Viewing the Knowledge Base

To learn about the event or condition leading to the alert and about ways to resolve the condition, you can view the alert knowledge base. The knowledge base can include information provided with Security Manager or from your company. You can view the knowledge base in the alert properties using the Control Center.

To view the knowledge base for an alert:

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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Display the alert. For more information about viewing alerts, see "Viewing Alerts" on page 109.
4. In the Results window, click the alert.
5. ***If you want to view the default knowledge base***, click the NetIQ Knowledge tab in the Alert Properties window. For more information about fields on a window or tab, see the Help.
6. ***If you want to view information and comments personnel in your company have provided***, click the Our Knowledge tab in the Alert Properties window. For more information about fields on a window or tab, see the Help.

Resolving Alerts

Using the Control Center or Web Console, you can track alerts throughout the resolution process. The alert resolution state indicates the alert's current point in the resolution process. The default resolution state for alerts is **New**. You can change the resolution state to match the current state of the process. For more information about default resolution states, see "Resolution State" on page 91.

Alerts can indicate that a condition or occurrence on your network needs to be addressed. Resolving alerts is a process that includes several tasks.

To resolve an alert:

1. Display the alert. For more information about viewing alerts, see "Viewing Alerts" on page 109.
2. View the alert properties to find out details about the indicated condition. For more information about viewing alert properties, see "Viewing Alert Properties" on page 110.

3. ***If you want to assign the alert to the person responsible for resolving the indicated condition***, assign the owner. For more information about assigning alerts, see "Assigning an Alert" on page 114.

4. Change the resolution state of the alert to track the resolution process. For more information about changing alert resolution states, see "Changing Alert Resolution States" on page 115.

5. ***If you want to add comments to the alert resolution history detailing the efforts for this specific alert***, modify the alert resolution history. For more information about the alert resolution history, see "Modifying the Resolution History of an Alert" on page 116.

6. ***If you want to add information that others can use to resolve similar conditions in the future***, modify the knowledge base. For more information about adding to the knowledge base, see "Modifying the Knowledge Base for an Alert" on page 117.

Assigning an Alert

You can use the Control Center to assign an Owner to an alert. The Owner is typically the person responsible for tracking and resolving the indicated problem. You can assign an Owner when you create a rule that generates an alert, or you can assign an Owner when the alert occurs. Alerts can also contain the source of the alert and an alert description. By default, alert views display Owner names for each alert.

To assign an alert:

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 "Understanding Requirements and Permissions" on page 24.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

3. Display the alert. For more information about viewing alerts, see "Viewing Alerts" on page 109.

4. In the Results window, click the alert.

5. On the Tasks menu, click **Alert Tasks > Update Alert**.

6. Next to the **Alert Assigned To Owner** field, click **Browse**.

7. Select the appropriate owner and click **OK**. For more information about fields on a window, see the Help.

8. Click **OK**.

Changing Alert Resolution States

When viewing alerts using the Control Center you can change resolution states to indicate that the alert has been acknowledged, is in the process of being resolved, or is resolved. Security Manager immediately removes resolved alerts from a view so you only see alerts that require attention.

You can use the Control Center to change the resolution state for an alert.

To change a resolution state:

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 "Understanding Requirements and Permissions" on page 24.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

3. Display the alert. For more information about viewing alerts, see "Viewing Alerts" on page 109.

4. In the Results window, click the alert.

5. On the Tasks menu, click **Alert Tasks > Update Alert**.

6. Select the appropriate resolution state in the **State of Alert** field. For more information about the fields on a window, see the Help.

7. Click **OK**.

Creating Alert Knowledge

You can add information to the company knowledge base when you resolve an alert. 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. If you want to add information that others can use to resolve similar conditions in the future, modify the knowledge base. For more information about adding to the knowledge base, see "Modifying the Knowledge Base for an Alert" on page 117.

Security Manager automatically tracks alert resolution history. The history indicates whether any responses were carried out for this alert, and records all changes made to alert fields. You cannot edit the alert resolution history, but you can add your own resolution comments that are appended to the history. If you want to add comments to the alert resolution history detailing the efforts for this specific alert, modify the alert resolution history. For more information about modifying the resolution history, see "Modifying the Resolution History of an Alert" on page 116.

Modifying the Resolution History of an Alert

Security Manager automatically tracks and records all changes to alert properties. You cannot edit this information, but you can add your own comments using the Control Center.

To add comments to the resolution history of an alert:

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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Display the alert. For more information about viewing alerts, see "Viewing Alerts" on page 109.
4. In the Results window, click the alert.

5. On the Tasks menu, click **Alert Tasks > Update Alert**.
6. Type your comments in the **Comments to be appended to Alert History** text area. For more information about the fields on a window, see the Help.
7. Click **OK**.

Modifying the Knowledge Base for an Alert

You can add information to the company knowledge base for an alert to save comments about its resolution. Your comments are added to the rule that generated the alert, and are included in any alerts later generated by the rule.

You can use the Control Center to append information to the company knowledge base. To modify existing information in the company knowledge base, your user account must be a member of the OnePointOp Operators group. For more information about OnePointOp groups, see “Understanding Requirements and Permissions” on page 24.

To modify the alert knowledge base:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Display the alert. For more information about viewing alerts, see “Viewing Alerts” on page 109.
4. In the Results window, click the alert.
5. On the Tasks menu, click **Alert Tasks > Update Knowledge**.
6. Type your comments in the text area. For more information about the fields on a window, see the Help.
7. Click **OK**.

Understanding Incident Packages

Incident packages are containers for information you can use to investigate and resolve an incident. Incident packages can contain the following items:

- Alerts
- Events
- File attachments
- Completed Forensic Analysis reports
- Web links

Incident packages allow you to gather and organize your research about an incident, store it in a single container, and share it with other people. You can use an incident package for many purposes, including the following:

- Saving incident research for examination at a later time and in a different location
- Packaging crucial security evidence for use in litigation
- Sharing incident research with coworkers

Security Manager saves incident packages in the SecurityManagerCommon database. You can keep an incident package and its contents indefinitely. Security Manager does not automatically groom alerts and events stored in an incident package. If you delete all incident packages containing an alert or event, Security Manager grooms the alert or event at the next scheduled grooming cycle.

Both incident packages and incident package folders can be public or private. Only the creator of a private incident package or folder can view the private object, while all users can view public incident packages or folders.

Creating an Incident Package

You can create incident packages to gather events, alerts, and other related data in a single container while investigating an issue or to share with other people. The following procedure guides you through the process of creating an empty incident package in the specified incident package folder. After you create an incident package, you can add objects to it.

To create a new incident package:

1. Log on to the Control Center computer as a member of the OnePointOp Users group or OnePointOp Reporting group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Incident Packages**.
4. Click the folder in which you want to store the incident package.
5. On the Tasks menu, click **Folder Tasks > New Incident Package**.
6. Complete the fields in the window. For more information about the fields on a window, see the Help.
7. Click **OK**.

Note
An incident package name can contain letters, numbers, and special characters. Ensure the incident package you create within, or move to, an incident package folder has a unique name.

Adding Objects to an Incident Package

You can add objects to incident packages. Incident packages can contain the following items:

- Alerts
- Events

- File attachments
- Completed Forensic Analysis reports
- Web links

To add objects to an incident package:

1. Log on to the Control Center computer as a member of the appropriate OnePointOp group for the object you want to add. To add alerts or events your account must be a member of the OnePointOp Users group. To add Forensic Analysis reports, your account must be a member of the OnePointOp Reporting group. To add Web links or attachments, your account must be a member of either the OnePointOp Users group or OnePointOp Reporting group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. ***If you want to add a Web link,*** complete the following steps:
   a. In the Navigation pane, click **Incident Packages**.
   b. Expand the incident package folders and click the incident package to which you want to add a Web link.
   c. On the Tasks menu, click **Incident Package Tasks > Add Web Link**.
   d. Specify the name and the URL of the Web link.
   e. Click **OK**.
4. ***If you want to add a file attachment,*** complete the following steps:
   a. In the Navigation pane, click **Incident Packages**.
   b. Expand the incident package folders and click the incident package to which you want to add a file.
   c. On the Tasks menu, click **Incident Package Tasks > Add Attachments**.

   d. Navigate to the file you want to add, and then select it.

   e. Click **Open**.

5. ***If you want to add an alert,*** complete the following steps:

   a. In the Navigation pane, click **Alert Views**.

   b. Expand the views and click the view containing the alert you want to add to the incident package.

   c. In the Results window, click the alert.

   d. ***If you have more than one incident package,*** on the Tasks menu, click **Incident Package** and select the incident package to which you want to add the selected alert.

   e. On the Tasks menu, click **Alert Tasks > Add to Incident Package**. You can also drag the alert to the **Incident Package Drop Box**.

6. ***If you want to add an event,*** complete the following steps:

   a. In the Navigation pane, click **Event Views**.

   b. Expand the views and click the view containing the event you want to add to the incident package.

   c. In the Results window, click the event.

   d. ***If you have more than one incident package,*** on the Tasks menu, click **Incident Package** and select the incident package to which you want to add the selected event.

   e. On the Tasks menu, click **Event Tasks > Add to Incident Package**. You can also drag the event to the **Incident Package Drop Box**.

7. ***If you want to add a completed Forensic Analysis report,*** complete the following steps:

   a. In the Navigation pane, click **Forensic Analysis**.

   b. Expand **Forensic Analysis > Completed Reports**.

   c. In the Results window, click the completed report.

d. ***If you have more than one incident package,*** on the Tasks menu, click **Incident Package** and select the incident package to which you want to add the selected report.

e. On the Tasks menu, click **Forensic Analysis Report Tasks > Add to Incident Package**. You can also drag the report to the **Incident Package Drop Box**.

8. In the Navigation pane, click **Incident Packages**.

9. Expand the incident package folders and click the incident package you want to view.

The Control Center displays the contents of the incident package in the Results window.

Exporting Incident Packages

The following procedure allows you to export a consolidated view of the objects stored in an incident package to any of several preset formats. You can export an incident package view in `PDF`, `HTML`, `TXT`, `CSV`, `XLS`, `BMP`, `GIF`, `JPEG`, `PNG`, `TIFF`, `EMF`, or `WMF` format.

Exporting a consolidated view of an incident package allows you to keep a record listing all the files contained in the incident package.

Note
An incident package consolidated view is a list of all of the objects stored in the incident package. You cannot view the data contained within those objects using this view.

To export a consolidated view of an incident package:

1. Log on to the Control Center computer as a member of the OnePointOp Users group or OnePointOp Reporting group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

3. In the Navigation pane, click **Incident Packages**.

4. Expand the incident package folders to the folder containing the incident package you want to view.

5. Click the incident package you want to view.

6. On the Tasks menu, click **Consolidated View Tasks > Print\Export**. This opens the Preview window.

7. Click **File > Export To** and select the format in which you want to export the incident package view.

8. Specify a name for the exported file and click **Save**.

9. Close the Preview window.

Chapter 5

Managing and Analyzing Logs

Security-conscious companies need to manage security logs. Attempting to manage logs is a problematic task for several reasons:

- Manually gathering and archiving information from various logs on numerous computers or devices is time consuming.
- Analyzing critical events requires time, effort, and security expertise, which is difficult to accomplish with distributed logs and an inexperienced staff.
- Meeting government regulations to ensure the privacy of information or other audit requirements involves accurately documenting and reporting on security events.

Security Manager provides you with an easy method of gathering logs, analyzing critical security events, and meeting audit requirements. Security Manager can help you resolve these issues through log management.

What Is Log Management?

Log management means gathering data from various logs across your enterprise network and storing this data in a secure repository, and creating reports for auditing and analysis.

Log Collection

Security Manager provides you with the ability to meet legal and business log-retention requirements. Security Manager provides a powerful yet simple-to-use, out-of-the-box solution that enables data collection from multiple platforms into secure log archives.

Security Manager collects raw log data from various sources and stores log data in the log archives, located on the log archive server, for archival and reporting.

You can view collected log data using the Control Center, which provides a useful interface to create, examine, and print reports of all collected log data. Log archives provide data for Forensic Analysis, Trend Analysis, and Summary reports.

You can configure Security Manager to collect almost any log data. Security Manager collects logs using agents and settings you specify using the Configuration Wizard. Ensure you have installed and configured agents and then configured Security Manager using the Configuration Wizard and the Log Archive Configuration utility.

Also ensure you have configured logging or auditing for some platforms. For more information about log collection, see the module documentation for products you want to monitor.

Log Archival

The log archive server stores collected log data in log archives. A **log archive** is a folder on the log archive server that contains a set of subfolders called partitions, as well as statistical information on all data stored in the log archive.

A **log archive partition** is a storage folder on the server used to store log data collected each day. Security Manager uses the date in local time on the log archive server (*`YYYYMMDD`*) for the names of daily log archive partitions, as in the following example:

```
NetIQSMLogArchive\20100322
```

Security Manager agents collect log data and build the collected events into compressed record blocks, then sends those compressed blocks to the central computer. The central computer then sends the record blocks to the log archive server, which temporarily stores the received data in the `netiq.sm.logarchival` Microsoft Message Queue (MSMQ).

When the central computer sends data to the log archive server, the log archive server appends the blocks of data to the most recent log archive file. A **log archive file** is a collection of record blocks, each consisting of event data collected from logs.

Each daily log archive partition contains one or more log archive files, depending on the amount of data collected that day. Security Manager names each log archive file sequentially, as in the following example:

```
00000001.NDS
```

By default, each log archive file contains up to 400 record blocks. Once Security Manager appends the maximum number of record blocks to a log archive file or the `NetIQ Security Manager Log Archive` service restarts, Security Manager closes the current log archive file and creates a new file.

When a log archive reaches the maximum size configured either during installation or using the Log Archive Configuration utility, Security Manager stops storing data in the current log archive and starts storing data in the next available log archive on the server computer. If all log archives on the server are full, Security Manager stops collecting new event data and logs an Error event in the event log.

Notes

- You can use the Log Archive Configuration utility to create multiple log archives on a log archive server. However, a log archive server can store collected data in only a single log archive at any given time. By default, Security Manager stores archival data in the initial log archive created during installation.

- After you install Security Manager, NetIQ recommends downloading and installing the **Log Archive Resource Kit** on your log archive server computer. The Log Archive Resource Kit is a set of tools that allow advanced users to directly view, query, export, reindex, migrate, and repair log archive data.

  You can download the Log Archive Resource Kit from the NetIQ Support site for Security Manager at `www.netiq.com/support/sm/extended/utilities.asp`.

Log Archive Statistics

Each log archive also contains a `VolumeInfo.xml` file, which Security Manager uses to track statistical information about the log archive as a whole. The `VolumeInfo.xml` file includes the following data:

- Total number of records currently in the log archive
- Total number of records groomed out of the log archive
- Compressed size of the log archive (in bytes)
- Uncompressed size of the log archive (in bytes)
- List of all log archive partitions in the log archive, with statistical data for each

Each log archive partition contains a similar file, `PartitionInfo.xml`, which includes statistical information about that particular partition.

When a user runs a Forensic Analysis query, Security Manager uses the `PartitionInfo.xml` files to query only log archive partitions within the time range of the query. Security Manager does not query log archive partitions that do not fall within the query time range.

You can view log archive and partition statistics using the Log Archive Configuration utility or by viewing the `.xml` files directly. For more information about viewing log archive statistics, see "Viewing Log Archive Statistics" on page 136.

Log Archive Indexing

Security Manager uses Forensic Analysis queries to retrieve records from a log archive based on specific query criteria. To enable log archive querying, Security Manager indexes all data collected and stored in the log archive.

Security Manager automatically formats all collected records so the log archive server can index the data. After the log archive server appends a record block to a log archive file, the server uncompresses the record block and stores part of the block in a `.indexing` file in the `index_data` subfolder of the main log archive folder.

The log archive server uses one or more indexing processes to index collected log data. By default, the number of indexing processes on a log archive server is equal to the number of processor cores on the log archive server computer.

Each log archive indexing process takes a `.indexing` file out of the `index_data` subfolder and adds the data from the file to the index files for the current log archive partition. The process then deletes the `.indexing` file from the `index_data` subfolder.

Once the log archive server indexes a partition, the partition contains an `index` folder with one or more numbered subfolders, each of which contains a set of `.ix` files that the log archive server uses to store index information.

Note
Due to the nature of the information needed for indexing, files in the `index` subfolders of your log archive partitions can be very large. A log archive index file may be as much as five to ten times the size of the data indexed.

Log Archive Retention

Security Manager retains log archive partitions for 90 days, by default. After 90 days, Security Manager permanently deletes the old log archive partitions and all log archive data contained in those partitions from the volume to make room for new log archive partitions and data.

If you want to store the log archive partitions for a longer period of time, you can modify the retention setting. For more information about log retention settings and grooming, see “Grooming the Log Archives” on page 142.

NetIQ recommends backing up log archive data on a regular basis. For more information about backing up log archives, see “Backing Up Log Archives” on page 139.

Log Archive Data Signing

Security Manager provides data signing of log archive data as an option to ensure the integrity of your data. Digital signatures created using public key cryptography allow you to detect any alterations to the data and provide assurance of when and where the data originated for non-repudiation purposes.

You can choose to digitally sign log data from some or all of your central computers by specifying settings and digital certificates on the log archive server and central computers. Security Manager computes and adds a digital signature to each message block from the configured central computers. The log archive server adds a second level of protection by signing each completed log archive file.

You can obtain the necessary signing certificates, with corresponding private and public keys, from a certification authority (CA). Security Manager uses the private key to encrypt a digest of the data. This secure digest of the actual data, together with information about the signing certificate, comprise the digital signature. The certificate contains the information needed to verify the digital signature, including the public key for decryption and the algorithm used for creating the digest.

Note

When you configure data signing on the log archive server, ensure the service account used to run the NetIQ Security Manager Log Archive service has Read and Write access on the certificate you want to use to sign data.

Review the access control list (ACL) of the key container file to ensure the service user has Read and Write permissions, at minimum. For more information about key containers, see the following article on the Microsoft support site:

`http://msdn.microsoft.com/en-us/library/bb204778(VS.85).aspx`

If you want to sign log archive data, you must specifically enable and configure data signing after installing Security Manager. You may also want to minimize the possibility of data alteration by setting restrictive file system permissions on the log archives. For more information about configuring data signing or using file system security, see the *Installation Guide for NetIQ Security Manager.*

After data signing is enabled, you can verify signed log archive data at any time, using the **Log Archive Analyzer** utility. The Log Archive Analyzer utility allows you to verify digitally signed log archive data by detecting and reporting any alterations of the stored data. Information in the signature is used to compare the current data with the original data stored in an encrypted digest form in the signature. If they match, the data is intact and was signed by the owner of the certificate. If they do not match, the data was altered.

You can verify a single log archive file, a daily partition, or an entire log archive. The utility provides a list of log archive files that fail signature verification and also generates error events for the failures. Signed data in a log archive file that has been moved to a different volume or server can still be verified. The move does not affect the comparison. For more information about verifying log archive data, see “Verifying Signed Log Archive Data” on page 136.

You can also use the Log Archive Analyzer to repair corrupted log archive partition files (`.nds` files) and sign repaired log archive files, whether the repaired files were previously signed. You cannot use the tool to re-sign files that are already signed and do not need to be repaired. For more information about repairing and re-signing log archive files, see “Repairing Log Archive Data” on page 137.

Trend Analysis

Analyzing trends allows you to compare data over a period of time to identify ongoing security issues occurring on network nodes through your enterprise. You can analyze trends using the following Trend Analysis reports:

Severity Analysis
Allows you to examine the number of log events by severity per network node.

User Analysis
Allows you to examine the number of log events by user account per network node.

Resource Analysis
Allows you to examine the number of log events caused by a source IP address per network node.

Protocol Analysis
Allows you to examine the number of log events by communication protocol per network node. The network node can provide the communication protocol by acronym, such as TCP, or by the IP protocol number. For more information about the numbers certain network nodes assign to certain protocols, see the documentation for that network node.

Trend Analysis reports are highly interactive views. Each report contains a graph and a table that you can manipulate to change the data displayed. You can modify the data in the graph and table using table controls. You can also rotate the graph to change perspective.

Trend Analysis reports display interrelated, summarized data contained in a multi-dimensional databases called the online analytical processing (OLAP) cube. Each cube contains data collected from all network nodes throughout the day.

Summarization is a process used to compact data stored in the reporting cube. The reporting server processes uploaded log archive data for Trend Analysis reports and custom Summary reports every 3 hours by default.

Trend Analysis reports allow you to navigate data collected previously so you can examine an overall trend rather than up-to-the-moment information.

For example, you can answer the following types of questions using Trend Analysis reports:

- How do the number of high-severity security events for the past quarter compare to the number for the same quarter last year?
- Which production servers in my network were the most frequently targeted for attacks during the past six months?
- How many times were the ports of a specific Web server scanned in the past week?

Trend Analysis reports display dates and times using the local time zone of the agent computer providing the data. For more information about modifying time properties, see the *Installation Guide for NetIQ Security Manager*.

For more information about working with Trend Analysis reports, see “Working with Trend Analysis Reports” on page 143.

Forensic Analysis

Forensic Analysis reports provide a consolidated view of the raw data for all collected logs using the coordinated universal time standard or in the local time of the Control Center computer. **Coordinated universal time (UTC)** is the international time standard based on International Atomic Time (TAI). UTC is equivalent to local time for countries located on the prime meridian, similar to Greenwich Mean Time (GMT), and is expressed using 24-hour time. For more information about UTC, see "Converting UTC Time" on page 175.

You can use Forensic Analysis reports to research an issue. For example, if you receive a real-time alert, you can examine all events within a specific date range to learn more about the alert in context. You can also use Forensic Analysis reports to provide proof of events written to single or multiple logs.

Forensic Analysis reports represent data stored in the log archives on all available log archive servers in the current configuration group. Security Manager retains log archive partitions for 90 days, by default. If you want to retain log archive partitions for a longer period of time, you can modify the grooming settings using the Log Archive Configuration utility. For more information about log retention, see "Grooming the Log Archives" on page 142.

Security Manager stores completed Forensic Analysis reports in the OnePoint database for 180 days, by default. You can use the Development Console to modify the grooming settings for completed reports. For more information about grooming completed reports, see "Modifying Database Grooming Settings" on page 263.

If your log archive is groomed and your company has established a backup procedure to permanently archive this data, you may need to restore the backed up log archive partitions to see reports. For more information about restoring groomed log archive partitions, see "Restoring Log Archives" on page 143.

For more information about working with Forensic Analysis reports, see "Working with Forensic Analysis Queries and Reports" on page 154.

Summary Reports

In addition to viewing Forensic and Trend Analysis reports using the Control Center, you can also access custom Summary reports using a Web browser. Summary reports are custom SQL Server Reporting Services reports created using SQL Server Business Intelligence Development Studio and published to a selected Web server. Summary reports retrieve summarized data directly from the reporting cube and can be configured to display data for a variety of purposes.

You can access Summary reports from the Configuration Groups view in the Control Center or through the Web Console. For more information about creating and viewing Summary reports using reporting cube data, see “Working with Summary Reports” on page 166.

Archival Event Severity Levels

Archival events use severity levels that are different from real-time alert severity levels. Archival events are assigned a severity level of high, medium, or low. These logged event severity levels display in Forensic Analysis reports.

The following table defines the relationship between alert severity values and logged event severity values.

Logged Event Severity	Alert Severity
High	Service Unavailable
	Security Breach
	Critical Error
	Error
Medium	Warning
Low	Information

For more information about alert severity levels, see “Alert Severity” on page 87.

Managing Log Archives

Security Manager provides several internal processes and utilities for managing log archives and the log collection process.

You can modify UNIX or iSeries log collection schedules with the Configuration Wizard, view log archive statistics with the Log Archive Configuration utility, verify signed log archive data with the Log Archive Analyzer utility, and use the Control Center to monitor log management status in real time. You can use these tools to aid in the diagnosis of problems with your Security Manager deployment.

You can also configure grooming settings for your log archives and establish a backup procedure to store log archives for auditing purposes or to restore at a later time.

Modifying Log Collection Schedules for UNIX and iSeries

Security Manager uses a schedule to specify how often to retrieve log data from UNIX computers and iSeries servers. You can modify these settings using the Configuration Wizard. For more information about using the Configuration Wizard, see “Using the Configuration Wizard” on page 232.

You do not need to modify schedules for Windows computers, antivirus applications, firewalls, IDS devices, routers, or switches. Security Manager receives log data from these sources in real time and then processes the data in the same manner as it processes the UNIX or iSeries data collected on a schedule.

Monitoring Security Manager Log Management

Security Manager provides views and reports to monitor log collection, report generation, and other configuration and service problems. You can also examine the All Open Alerts view in the Control Center to monitor log collection and report processing status, among other items.

Viewing Log Archive Statistics

You can view statistics about all existing log archives on your log archive server using the Log Archive Configuration utility. You can use the Log Archive Configuration utility to quickly see how many events are captured in your log archives.

You can use the utility to view the total number of events stored in each log archive, log archive partition, or log archive file. You can also compare the number of events collected on one day with the number collected on previous days by examining specific log archive partitions. In addition, log archive statistics can be useful for troubleshooting problems with the log archive server.

To view log archive statistics:

1. Log on to the log archive server using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start **Log Archive Configuration** in the NetIQ Security Manager > Configuration program group.
3. Click **Log Archive Statistics**.
4. Review statistics for all log archive partitions in each log archive.
5. ***If you want to refresh the displayed log archive statistics,*** click **Refresh**.
6. Click **Close**.

Verifying Signed Log Archive Data

If you choose to enable data signing on your log archive server, you can verify the integrity of the stored data using the Log Archive Analyzer utility. You can verify a single log archive file, a daily partition, or an entire log archive. The utility provides a list of log archive files that fail signature verification and also generates error events for the failures.

To verify signed log archive data:

1. Log on to the log archive server using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. At a command prompt, type the following commands:

   ```
   cd installation folder\NetIQ Security Manager\NetIQ Log Archive
   ```

   where *installation folder* is the location where you installed Security Manager.

   ```
   LogArchiveAnalyzer.exe logarchivepath
   ```

   where *logarchivepath* is the path to the log archive file or directory you want to verify. For example:

   ```
   LogArchiveAnalyzer.exe
   C:\NetIQSMLogArchive\20070507\00000001.NDS
   ```

   ```
   LogArchiveAnalyzer.exe C:\NetIQSMLogArchive\20070507
   ```
3. Click **Enter**.

For more information about configuring log archive data signing, see the *Installation Guide for NetIQ Security Manager.*

Repairing Log Archive Data

You can also repair corrupted log archive files using the Log Archive Analyzer utility and re-sign the repaired files if necessary. You can repair a single log archive file, a daily partition, or an entire log archive. The Log Archive Analyzer can sign repaired `.nds` files, whether or not the files were signed previously.

Note

You cannot use the tool to re-sign files that are already signed and do not need to be repaired.

To repair log archive data:

1. Log on to the log archive server using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.

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

   ```
   cd installation folder\NetIQ Security Manager\NetIQ Log Archive
   ```

   where *installation folder* is the location where you installed Security Manager.

3. ***If you want to repair log archive data without re-signing the data,*** type the following command:

   ```
   LogArchiveAnalyzer.exe -r logarchivepath
   ```

   where *logarchivepath* is the path to the log archive file or directory you want to repair. For example:

   ```
   LogArchiveAnalyzer.exe -r
   C:\NetIQSMLogArchive\20070507\00000001.NDS
   ```

   ```
   LogArchiveAnalyzer.exe -r C:\NetIQSMLogArchive\20070507
   ```

4. ***If you want to repair and re-sign log archive data,*** type the following command:

   ```
   LogArchiveAnalyzer.exe -r -cnCertificateSubjectName -
   csCertificateStoreName logarchivepath
   ```

   where *CertificateSubjectName* is the value specified for the Data Signing Certificate Subject Name in the Log Archive Configuration utility, *CertificateStoreName* is the value specified for the Data Signing Certificate Store in the Log Archive Configuration utility, and *logarchivepath* is the path to the log archive file or directory you want to repair and sign. For example:

   ```
   LogArchiveAnalyzer.exe -r -cnLogArchive-DataSigning -
   csCurrentUser C:\NetIQSMLogArchive\20070507\00000001.NDS
   ```

```
LogArchiveAnalyzer.exe -r -cnLogArchive-DataSigning -
csCurrentUser C:\NetIQSMLogArchive\20070507
```

Note
If the certificate subject name includes spaces, you must enclose the entire option, including the `-cn` flag, in quotation marks.

5. Click **Enter**.

For more information about configuring log archive data signing, see the *Installation Guide for NetIQ Security Manager*.

Backing Up Log Archives

NetIQ recommends that you regularly back up log archives. You can establish a backup procedure to store log archives in another location and restore log archives as necessary for disaster recovery or auditing purposes.

Because log archive files are compressed binary files that are located outside of a physical database, you do not need to use an external tool to back up log archive partitions. If you have an automated file backup system in place, you can configure your system to automatically back up log archive files like the system would back up any other file.

When you back up a log archive, you can choose one of two options:

- Back up only the necessary data files
- Back up the data files and all index files

If you back up only log archive data and then decide to restore your backed-up partitions, you must use the Log Archive Reindexer tool included in the Log Archive Resource Kit to reindex the restored partitions. For more information about reindexing log archive data, see the *NetIQ Security Manager Log Archive Resource Kit Technical Reference*.

Reindexing a large amount of data can require a significant amount of time, particularly on a log archive server that also needs to index newly received data.

If you choose to back up both log archive data and log archive index files, you do not need to reindex your data when you restore one or more partitions. However, index files can be very large, particularly in environments where the log archive server receives a high volume of log data. You may need a significant amount of additional storage space to regularly back up log archive index files.

Notes

- Ensure you back up the log archives before the log archive partitions are groomed. After the log archive partitions are groomed, you cannot retrieve groomed data. Security Manager permanently deletes groomed log archive data. For more information about log archive grooming, see “Grooming the Log Archives” on page 142.
- If you want to restore log archive partitions for reports, ensure backed-up log archives retain their internal file structure. If you modify the log archive file structure prior to or during the backup procedure and then restore the log archive, Security Manager cannot open the restored log archive. For more information about the log archive file structure, see “Log Archival” on page 126.

Backing Up Log Archive Data Only

If you choose to back up only log archive data and need to restore the backed-up log archive at a later date, you need to reindex the log archive data to be able to run Forensic Analysis queries on the restored data.

To back up log archive data only:

1. Log on to the log archive server using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Configure your file backup system to include only the following types of files:
   - `.nds` (data files)
   - `.xml` (main `VolumeInfo.xml` file and all `PartitionInfo.xml` files)
3. Run your file backup process on the log archive partitions you want to back up.

Backing Up Log Archive Data and Index Information

You can also back up both log archive data and the associated index files. However, because log archive index files are generally very large, the backup process can take much longer than if you only back up log archive data.

If you back up index files along with log archive data, you do not need to reindex the backed-up data when you restore the log archive. When you configure your backup system, include the `index_data` subfolder in the main log archive folder and all closed `index` files within the log archive partitions you want to back up.

Notes

- You should only back up closed `index` files. If you attempt to back up the files in an open `index` folder while the log archive server is in the process of indexing data, the `index` files may be unusable, forcing you to reindex when you restore the backed-up partition.
- Not all backup applications can exclude specific files from the backup process. Confirm that your application has this capability before attempting to back up log archive data.

To back up log archive data and index information:

1. Log on to the log archive server using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Configure your file backup system to exclude open `index` files for the current log archive partition and the `CubeExport` folder in the main log archive folder.
3. Use the Services Administrative Tool to stop the `NetIQ Security Manager Log Archive` service.
4. Run your file backup process on the log archive partitions and index information files you want to back up.
5. In the Services Administrative Tool, restart the `NetIQ Security Manager Log Archive` service.
6. Close the Services Administrative Tool.

Grooming the Log Archives

Security Manager removes log archive partitions that are older than the value specified in the Log Archive Configuration utility, which is 90 days by default. Because Security Manager creates log archive partitions daily, Security Manager grooms data from the log archives by deleting log archive partitions that have expired. Security Manager checks every 2 hours by default whether it needs to remove expired log archives.

You can modify the number of days before log archive partitions are groomed using the Log Archive Configuration utility.

To change the number of days before log archive partitions are groomed:

1. Log on to the log archive server using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start **Log Archive Configuration** in the NetIQ Security Manager > Configuration program group.
3. Click **Log Archive Server Settings**.
4. Type the number of days you want to retain log archive partitions before grooming in the **Number of Days before Grooming** field.
5. Click **Apply**.
6. Click **Yes**.
7. Click **Close**.
8. Click **Yes** on the confirmation message to restart the `NetIQ Security Manager Log Archive` service.

   Note
   If you modify any log archive setting, you must restart the log archive server for the change to take effect.

Restoring Log Archives

If you want to access data contained in groomed log archive partitions and have previously backed up your log archive, you can restore the groomed log archive partitions.

To restore groomed log archive partitions:

1. Log on to the log archive server using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Use your file backup system to restore the groomed or deleted log archive partitions you want to access.
3. Restart the `NetIQ Security Manager Log Archive` service.

Notes

- Once you restore a groomed log archive partition, Security Manager does not groom the partition a second time. If you want to remove a restored partition, you must remove the partition manually.
- If you backed up a log archive partition and not the corresponding log archive index files, after you restore the partition, reindex your log archive data using the Log Archive Reindexer tool included in the Log Archive Resource Kit. For more information about reindexing log archive data, see the *NetIQ Security Manager Log Archive Resource Kit Technical Reference*.

Working with Trend Analysis Reports

The following sections provide information about working with Trend Analysis reports. Before working with Trend Analysis reports, ensure you have configured Security Manager and turned on auditing or logging. For more information about turning on auditing or logging, see the Configuration Wizard and the module documentation for products you want to monitor.

In order to access Trend Analysis reports, use the Log Archive Configuration utility to configure the log archive server to upload data to the reporting server. For more information about configuring reporting, see “Modifying Log Archive Settings” on page 280.

The reporting server processes uploaded log archive data every 3 hours by default. After installation, wait 3 hours before viewing Trend Analysis reports in the Control Center. For more information about modifying the processing job settings, see “Modifying the Reporting Cube Processing Job” on page 273.

For more information about Trend Analysis reports, see “Trend Analysis” on page 131.

Viewing Trend Analysis Reports

A Trend Analysis report is an interactive display of summarized data from the reporting cube. A Trend Analysis report contains a three-dimensional bar graph and a table control. The report represents the **measure** and **dimensions** from the OLAP cube. The measure is the event count. A dimension is a category, such as network nodes, source user accounts, or Security Manager time periods. Some categories contain objects or subcategories you can expand to reveal detail in the graph and table.

The graph has three axes. The y axis represents the event count. The z axis, by default, represents the platform, agent computers, and monitored network nodes.

The x axis is different for each default report. For example, the x axis in the User Analysis report is the **Source User** axis, representing user accounts that caused an event.

All event dates use the local time zone of the agent computer. The Time Period dimension uses the local time zone of the central computer. For more information about modifying time properties, see the *Installation Guide for NetIQ Security Manager.*

To view Trend Analysis reports:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Reporting group and that has access to the SQL Server Analysis Services computer. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.

3. In the Navigation pane, click **Trend Analysis**.

4. ***If the report is a custom report***, expand **Saved Reports**.

5. In the Navigation pane, click the report you want to view. The Control Center displays the report in the Trend Analysis Reports window.

Note

You cannot view custom Trend Analysis reports created by other Control Center users. Security Manager saves each user's custom reports in a user-specific `Trend.config` file in the following folder on the Control Center computer:

```
C:\Documents and Settings\UserName\Local
Settings\Application Data\NetIQ\Security Manager\Trend
Analysis
```

where *`UserName`* is the name of a particular user account.

6. ***If you want to change the data in the report***, modify the data. For more information about changing report data, see "Modifying Graphed Data" on page 146.

7. ***If the data in the graph is difficult to see***, on the Tasks menu, click **Trend Analysis Report Tasks > Rotate Graph**. For more information about rotating graphs, see "Modifying Graphed Data" on page 146.

8. ***If you want to restore the report to the default view or refresh the data in the report***, on the Tasks menu, click **Trend Analysis Report Tasks > Restore Report**.

9. ***If you want to save the report as a custom report***, on the Tasks menu, click **Trend Analysis Report Tasks > Save Report As**. For more information about creating custom reports, see "Creating Custom Trend Analysis Reports" on page 149.

10. ***If you want to rename a saved report,*** complete the following steps:

    a. In the Navigation pane, expand **Saved Reports**.

    b. Right-click the report you want to rename and select **Rename**.

    c. Specify a new name for the report and press **Enter**.

11. In the Navigation pane, click **Trend Analysis Reports**.

Modifying Graphed Data

Trend Analysis reports provide an interactive table control you can use to modify the data displayed in the table and graph. Because the reports are based on OLAP technology, you can immediately see the results of your modifications. You can modify the data in order to perform the following tasks:

- View all the data in a cube. For example, you can view event counts for all security-related events collected by Security Manager that occurred on all your computers, firewalls, devices, routers, and switches for every year.
- Compare large amounts of data. For example, you can compare detailed data for all security events for a given month to all security events for the same month from a previous year.

The Control Center does not save modifications you make to default reports. If you want to save modifications, save the report. For more information about saving Trend Analysis reports, see “Creating Custom Trend Analysis Reports” on page 149.

The date you modify is based on the local time zone of the agent computer from which the event was collected.

Understanding the Table Control Window

The table control window contains a dimension bar and a table. The dimension bar lists the standard dimensions you can use in the graph for the x and z axes. You cannot modify the y axis because the event count is the only measure available for trend analysis.

You can modify the data in the following ways:

- You can filter the data in the graph and table using the dimension bar. For more information about filtering Trend Analysis data, see “Filtering Graphed Data” on page 147.
- You can reveal detail in the graph and table by expanding categories. For more information about expanding categories, see “Displaying Subcategories and Objects” on page 148.
- You can also add detail to the graph and table by adding a dimension to the x or z axis. For more information about adding dimensions, see “Adding Dimensions” on page 149.

You can drag a dimension to a row or column heading to immediately change the data reflected by both the table and the graph. The row heading corresponds to the x axis and the column heading corresponds to the z axis. The following sections describe how to modify graphed data using the table control.

Note

The unlicensed version of the Microsoft Office 2003 Web Component allows you to perform the tasks described in this section and is a prerequisite for installing and using Security Manager.

The licensed version of the Microsoft Office 2003 Web Component offers additional right-click menu options. However, the licensed version is not necessary to perform the tasks in this section.

Filtering Graphed Data

You can filter the data for the table and graph. For example, you can filter the Time Period dimension to view events that occurred during a specified time frame, such as lunch hours.

To filter data:

1. Select the report containing the data you want to filter. For more information about viewing Trend Analysis reports, see "Viewing Trend Analysis Reports" on page 144.
2. In the Trend Analysis report window, using the dimension bar in the table control, click the arrow next to the dimension containing the filters you want to specify.
   - To include data in the report, select the check box for the data you want to include.
   - To filter data from the report, clear the check box for the data you want to exclude.
3. Click **OK**.

Displaying Subcategories and Objects

Some columns are expandable and contain subcategories or specific objects that you can select to display summarized data for that subcategory or object. Displaying subcategories or objects reveals hidden data. For example, you can expand the Platform column to view the number of events by platform or by individual network nodes.

To view data for subcategories or individual objects:

1. Select the report. For more information about viewing Trend Analysis reports, see "Viewing Trend Analysis Reports" on page 144.
2. In the Trend Analysis report window, in the table control select the column or row containing the subcategory or object.
3. Expand the category and subcategories until you display the subcategory or object you want to see in the table and graph.

Adding Dimensions

Trend Analysis reports can display data from multiple dimensions. You can add a dimension to an axis to add detail to a report. For example, the User Analysis report displays users and network nodes. You can drag the Time Period dimension to see the number of events caused by a specific user account on a specific agent within a certain time frame.

To add dimensions:

1. Select the report. For more information about viewing Trend Analysis reports, see “Viewing Trend Analysis Reports” on page 144.
2. ***If you want to add a standard dimension from the dimension bar,*** drag the dimension in the table control to the column or row containing the dimension where you want add detail.
3. ***If you want to add a new dimension from the field list,*** complete the following steps:
   a. Right-click inside the table and select **Field List**.
   b. Drag the dimension in the Pivot Table Field List to the column or row containing the dimension where you want to add detail.
4. Add the dimension to the right of the row or column heading.
5. Expand the categories to see the subcategories for the dimension you just added. The categories at the higher levels are for the parent dimension, which is the dimension to the left in the column or row heading. You can continue expanding the subcategories to reveal addition details for the dimension you added.

Creating Custom Trend Analysis Reports

You can create custom Trend Analysis reports based on the default Trend Analysis reports provided by Security Manager. Creating custom Trend Analysis reports allows you to save the filters and dimensions you used in a default report. Once created, you can restore the custom report or restart the Control Center each day to see new data.

The Control Center saves the Trend Analysis report in the Saved Reports folder.

To create custom Trend Analysis reports:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Reporting group and that has access to the SQL Server Analysis Services computer. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.
3. In the Navigation pane, click **Trend Analysis**.
4. In the Navigation pane, click the report you want to customize. The Control Center displays the report in the Trend Analysis Reports window.
5. Make the appropriate modifications. For more information about modifying Trend Analysis reports, see "Modifying Graphed Data" on page 146.
6. On the Tasks menu, click **Trend Analysis Report Tasks > Save Report As**.
7. Specify a report name and click **Save**.

Note
You must specify a report name with a maximum of 80 characters.

Deleting Custom Trend Analysis Reports

You can also delete existing custom Trend Analysis reports stored in the Saved Reports folder in the Control Center.

Note
You cannot delete any of the default Trend Analysis reports.

To delete custom Trend Analysis reports:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Reporting group and that has access to the SQL Server Analysis Services computer. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.
3. In the Navigation pane, click **Trend Analysis > Saved Reports**.
4. In the results window, select the report you want to delete.
5. On the Tasks menu, click **Grid Tasks > Delete**.
6. Click **Yes** to confirm.

Exporting Trend Analysis Report Data

You can export a Trend Analysis report as a Microsoft Excel PivotTable (`.xls`). Exporting a Trend Analysis report allows you to share the report with people who do not have access to the Control Center. You can also manipulate the data in Microsoft Excel PivotTable format or provide a **snapshot** of the data to be used in a Microsoft Excel PivotTable or PivotChart report. A snapshot is offline data that is not refreshed.

Exporting Trend Analysis Reports

You can export Trend Analysis reports to make the data available for online or offline viewing. Online viewing allows you to see the latest data, which is updated each morning, in Microsoft Excel PivotTable format. You must open the report on a computer with access to the reporting server.

Offline viewing allows you to look at a snapshot of the data from an offline cube (`.cub`) file. You can create an offline cube file that you can share with people who do not have access or permissions to look at the report.

To export Trend Analysis reports:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Reporting group and that has access to the SQL Server Analysis Services computer. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.
3. In the Navigation pane, click **Trend Analysis**.
4. ***If the report is a custom report***, expand **Saved Reports**.
5. In the Navigation pane, click the report you want to export. The Control Center displays the report in the Trend Analysis Reports window.
6. On the Tasks menu, click **Trend Analysis Report Tasks > Export Report Data**.
7. Specify the file name and location where you want to save the file, and then click **Save**.
8. ***If you want to make the data available to offline viewers***, create an offline cube `(.cub)` file by completing the following steps:
   a. Open the file you just created in Microsoft Excel.
   b. Click either **Enable automatic refresh** or **Disable automatic refresh**. The option you select does not affect the `.cub` file.
   c. ***If the PivotTable toolbar is not available***, on the View menu, click **Toolbars > PivotTable**.
   d. On the PivotTable menu, click **Offline OLAP**.
   e. Click **Create offline data file**.
   f. Complete the steps in the wizard to create and save the offline cube `(.cub)` file.
9. Close the Control Center.

Viewing Data in an Offline Cube File

You do not need access to the reporting server or to be a member of the OnePointOp Reporting group to view the data in an offline cube file.

To open an offline cube (`.cub`) file:

1. Open Microsoft Excel.
2. ***If the PivotTable toolbar is not available***, on the View menu, click **Toolbars > PivotTable**.
3. On the PivotTable menu, click **PivotTable Wizard**.
4. Select **External data source**.
5. Select the appropriate report type:
   - To view the data as a table, click **PivotTable**.
   - To view the data as a chart, click **PivotChart**.
6. Click **Next**.
7. Click **Get Data**.
8. On the OLAP Cubes tab, click **New Data Source**.
9. Click **OK**.
10. Type a name for the data source in field **1**.
11. Select **Microsoft OLE DB Provider for OLAP Services** in field **2**.
12. Click **Connect**.
13. Select **Cube File**, browse and select the `.cub` file you want to use as a data source, and then click **Open**.
14. Click **Finish**.
15. Click **OK**.
16. Click **OK**.

17. Click **Next**, and then click **Finish**.

18. Drag and drop the measure and categories in the appropriate places in the chart or table. Count is the only data measure available.

Working with Forensic Analysis Queries and Reports

The following sections provide information about working with Forensic Analysis queries and reports using the Security Manager Control Center. Before working with Forensic Analysis reports, ensure you have configured Security Manager and turned on auditing or logging.

For more information about turning on auditing or logging, see the Configuration Wizard and the module documentation for products you want to monitor. For more information about Forensic Analysis reports, see “Forensic Analysis” on page 133.

Creating Forensic Analysis Queries

You can create **Forensic Analysis queries** to view raw log data for specific platforms on certain computers, devices, firewalls, routers, or switches. You can specify search criteria based on the UTC time standard or in the local time of the Control Center computer. For more information about UTC, see “Converting UTC Time” on page 175.

Notes

- Ensure you have data for the date range you specify in the query. You cannot query data that has been groomed, which happens at 90 days by default. If you need to query data that has been groomed, you need to restore the data first. For more information about restoring groomed log archive data, see “Restoring Log Archives” on page 143.
- Security Manager queries all log archive servers in the configuration group and returns data from all ungroomed log archive partitions, as well as the current partition open when the query runs.
- Security Manager queries log archive partitions sequentially, starting with the oldest events in a particular log archive.
- You can configure a query to return a maximum of 99,999 events per data source. For example, if you have three log archives on a log archive server and specify that a query returns 100 events, Security Manager returns a maximum of 100 events from each log archive, for a maximum total of 300 events.
- You can only query log archive servers that are currently running and connected to the configuration group. Security Manager automatically ignores any disconnected log archive servers.
- You must specify a minimum five-minute interval when configuring a scheduled Forensic Analysis query.
- Security Manager stores Forensic Analysis schedules and completed Forensic Analysis reports in the OnePoint database on the database server.
- You can query a log archive server located in an untrusted domain only if you configure a central computer in the configuration group to communicate with the log archive server in the untrusted domain. For more information about changing log archive servers, “Changing the Log Archive Server or Port” on page 281.

Security Manager automatically displays queries you create in the My Queries folder in the Control Center on the local computer. Members of the OnePointOp Reporting group can see any query you create on the computer on which you saved the query.

Security Manager saves custom Forensic Analysis queries you create to the following location on your central computer by default:

installation folder\NetIQ Security Manager\OnePoint\VSOC\config\forensicqueries

where *installation folder* is the location where you installed Security Manager.

When you create a new unscheduled query, Security Manager automatically runs the query immediately. When you create a new scheduled query, Security Manager automatically runs the query according to the schedule you specify.

To create Forensic Analysis queries:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Reporting group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.
3. In the Navigation pane, click **Forensic Analysis**.
4. ***If you want to create a query in a specific My Queries subfolder***, expand **My Queries** and select the appropriate subfolder in the Navigation pane. Otherwise, the query is created in the main My Queries folder.
5. On the Tasks menu, click **Forensic Analysis Tasks > Create New Forensic Analysis Query**.
6. Follow the instructions in the wizard to create a Forensic Analysis query. When you finish creating the query, Security Manager runs the query, temporarily saves the query status in the Pending Reports folder, and then saves the results in the Completed Reports folder. Security Manager saves the query itself in the My Queries folder. For more information about fields on a window, see the Help.

Modifying Forensic Analysis Queries

You can modify the search criteria used in a query, and then run the query again to change the results displayed in a Forensic Analysis report. You can specify search criteria based on the UTC time standard or the local time of the Control Center computer. For more information about UTC, see “Converting UTC Time” on page 175.

You can modify your existing queries to run automatically according to a schedule you specify.

To modify a Forensic Analysis query:

1. Log on to the Control Center computer where you saved the query with a user account that is a member of the OnePointOp Reporting group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.
3. In the Navigation pane, click **Forensic Analysis**.
4. Click **My Queries**.
5. Expand lower-level folders as necessary.
6. In the Results window, click the query you want to modify.
7. On the Tasks menu, click **Forensic Analysis Query Tasks > Edit Query**.
8. Make the appropriate modifications and click **OK**. For more information about fields on a window, see the Help.
9. ***If you want to see changes you made reflected in a completed report***, click the query, and then on the Tasks menu, click **Run Query > Over *DateRange***, where ***DateRange*** is one of the possible date range options. For more information about running Forensic Analysis queries, see “Running Saved Forensic Analysis Queries” on page 158.

Modifying Scheduled Forensic Analysis Queries

Using the Control Center, you can modify when an existing scheduled Forensic Analysis query runs.

To modify a Forensic Analysis query schedule:

1. Log on to the Control Center computer where you saved the query with a user account that is a member of the OnePointOp Reporting group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.
3. In the Navigation pane, click **Forensic Analysis > Scheduled Queries**.
4. In the Results window, click the query you want to modify.
5. On the Tasks menu, click **Forensic Analysis Query Tasks > Edit Query Schedule**.
6. Modify the schedule and click **OK**. For more information about fields on a window, see the Help.

Running Saved Forensic Analysis Queries

Saved Forensic Analysis queries are located in the My Queries folder. You can run saved queries to create a new report with refreshed data.

To run saved Forensic Analysis queries:

1. Log on to the Control Center computer where you saved the query with a user account that is a member of the OnePointOp Reporting group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.
3. In the Navigation pane, click **Forensic Analysis**.

4. Click **My Queries**.
5. Expand lower-level folders as necessary.
6. In the Results window, click the query you want to run.
7. ***If you want to run the query on data from the default date range of the query,*** click **Run Query > Over Default Date Range** on the Tasks menu. The Control Center runs the query and saves the results in the **Completed Reports** folder.
8. ***If you want to run the query on data from the last 24 hours,*** click **Run Query > Over Last 24 Hours** on the Tasks menu. The Control Center runs the query and saves the results in the **Completed Reports** folder.
9. ***If you want to run the query on data from the last 7 days,*** click **Run Query > Over Last 7 Days** on the Tasks menu. The Control Center runs the query and saves the results in the **Completed Reports** folder.
10. ***If you want to run the query on data from the last 30 days,*** click **Run Query > Over Last 30 Days** on the Tasks menu. The Control Center runs the query and saves the results in the **Completed Reports** folder.

Canceling Pending Queries

Pending queries appear in the Pending Reports view. If you do not want a pending query to run, you can initiate a request to cancel it.

Note
The Cancel task sends a *request* to cancel the selected pending query. If Security Manager runs the query before receiving the Cancel request, the Control Center displays the resulting report in the Completed Reports view.

To request cancellation of a pending query:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Reporting group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.

3. In the Navigation pane, click **Forensic Analysis**.
4. Click **Pending Reports**.
5. In the Results window, click the query you want to cancel.
6. In the Tasks pane, click **Cancel Pending Query**.
7. Click **Yes**.
8. Click **OK**.
9. In the Navigation pane, click **Completed Reports** and check the Results pane to determine the status of the query.

The Results pane displays the following possible status messages:

Failed

The log archive server received the cancellation request and canceled the pending query.

Success

The pending query completed successfully.

Partial Success

The Partial Success status can occur if you have two log archive servers. In this case, the query completed successfully on one server, but the other server canceled the query as requested. Highlight the report name and check the Report Properties pane to determine which log archive server completed the query and which canceled the query.

Viewing Forensic Analysis Reports

When you run a query, Security Manager creates a report of the completed results for all network nodes specified in the query criteria. Security Manager saves the results on the database server. Members of the OnePointOp Reporting group can review the completed results in the Completed Reports folder of any Control Center in a connected configuration group. The results contain data matching the query or information about why the query failed.

Security Manager also creates a report for each log archive that contains the results for only those network nodes managed by that central computer.

Note

You can only view report data for computers that belong to computer groups to which you have access. For more information about security filtering, see the *Installation Guide for NetIQ Security Manager*.

The data displayed in the completed report is based on the UTC time standard or the local time of the Control Center computer. For more information about UTC, see “Converting UTC Time” on page 175.

To view Forensic Analysis reports:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Reporting group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.
3. In the Navigation pane, click **Forensic Analysis**.
4. Click **Completed Reports**.
5. ***If you want to view report results for a different configuration group,*** click **Configuration Group** and select the appropriate configuration group name. For more information about monitoring multiple configuration groups, see “Monitoring Multiple Configuration Groups” on page 256.
6. In the Results window, select the report you want to view.
7. ***If you want to review report results for only the network nodes specified in the query criteria that are managed by a certain central computer***, in the bottom pane, select the central computer that manages the network nodes.

8. On the Tasks menu, click **Forensic Analysis Report Tasks > Show Report** to launch the report in a new window. You can then perform various tasks on the report:

   - To sort the report, click the heading of the column by which you want to sort. To sort a group of columns, press the **Shift** key while clicking the column headings. To deselect a column, press the **Ctrl** key while clicking the column heading.
   - To filter the report, click the arrow button in the column heading by which you want to filter the report. For more information about filtering reports, see “Filtering Forensic Analysis Reports” on page 163.
   - To group the report, drag and drop a column heading by which you want to group the report over the **Drag a column header here to group by that column** text.
   - To export the report, on the Options menu, click **Export**. For more information about exporting reports, see “Exporting Forensic Analysis Data to a File” on page 165.
   - To print the report, on the Options menu, click **Print**. For more information about printing reports, see “Printing Forensic Analysis Reports” on page 164.
   - To add, remove, or rearrange columns, on the Options menu, click **Customize**. For more information about customizing columns, see the Help.
   - To find text in the report, on the Options menu, click **Find**. Type your search criteria in the **Find what** window and click **Find Next**.

9. After you have finished viewing the report, click **Close**. For more information about the fields on a window, see the Help.

10. ***If you want to view the properties of the query that created the report,*** on the Tasks menu, click **Forensic Analysis Report Tasks > View Query**.

11. ***If you want to delete a report, on the Tasks menu,*** click **Forensic Analysis Report Tasks > Delete Report**.

12. ***If you want to mark a report as read without viewing it,*** on the Tasks menu, click **Forensic Analysis Report Tasks > Mark as Read**.

13. ***If you want to mark an already-viewed report as unread,*** on the Tasks menu, click **Forensic Analysis Report Tasks > Mark as Unread**.

14. ***If you want to run the query again to create a new report with refreshed data***, on the Tasks menu, click **Forensic Analysis Report Tasks > Run Query**.

Filtering Forensic Analysis Reports

Filtering Forensic Analysis reports allows you to limit the amount of data you want to see or make available in printed and exported formats.

To filter Forensic Analysis reports:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Reporting group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.

3. In the Navigation pane, click **Forensic Analysis**.

4. Click **Completed Reports**.

5. In the Results window, select the report you want to filter.

6. ***If you want to display report results for only the network nodes specified in the query criteria that are managed by a certain central computer***, in the bottom pane, select the central computer that manages the network nodes.

7. On the Tasks menu, click **Forensic Analysis Report Tasks > Show Report** to launch the report in a new window.

8. Click the arrow button in the column heading by which you want to filter the report.

9. Select the appropriate filter:

    - To remove a column filter to show all results, select **All**.
    - To specify a custom filter, select **Custom**.

- To show only rows with empty cells in the filtered column, select **Empty**.
- To omit rows with empty cells in the filtered column, select **Not Empty**.
- To show only rows with a specific value in all cells in the filtered column, select the value.

10. After you have finished viewing the report, click **Close**.

Printing Forensic Analysis Reports

Printing Forensic Analysis reports allows you to archive or distribute a hard copy of the report, to be used as a physical record of relevant log archive data. For example, you could use a printed report to provide legal proof of events.

To print Forensic Analysis reports:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Reporting group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.
3. In the Navigation pane, click **Forensic Analysis**.
4. Click **Completed Reports**.
5. In the Results window, select the report you want to print.
6. ***If you want to print report results for only the network nodes specified in the query criteria that are managed by a certain central computer***, in the bottom pane, select the central computer that manages the network nodes.
7. On the Tasks menu, click **Forensic Analysis Report Tasks > Show Report** to launch the report in a new window.

8. On the Options menu, click **Print**. On the Preview window, print to a specified printer by completing one of the following tasks:
   - To select the printer and print from the Print window, click the **Print** button, select the printer, and then click **OK**.
   - To bypass the Print window and immediately print the report to the default printer, click the **Print Direct** button.
9. When finished, close the Preview window.
10. Click **Close** to close the report.

Exporting Forensic Analysis Data to a File

You can export report data in `HTML`, `XLS`, `TXT`, or `XML` format. Exporting Forensic Analysis data allows you to use this data in other applications or share the data with other people who may not have access to the Control Center.

To export Forensic Analysis reports to a file:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Reporting group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.
3. In the Navigation pane, click **Forensic Analysis**.
4. Click **Completed Reports**.
5. In the Results window, select the report you want to print.
6. ***If you want to export report results for only the network nodes specified in the query criteria that are managed by a certain central computer***, in the bottom pane, select the central computer that manages the network nodes.
7. On the Tasks menu, click **Forensic Analysis Report Tasks > Show Report** to launch the report in a new window.
8. On the Options menu, click **Export** and select the file type.

9. Specify the file name and location where you want to save the file and click **Save**.
10. Click **OK**.
11. Click **Close** to close the report.

Working with Summary Reports

The following sections provide information about accessing summarized log archive data using SQL Server Reporting Services. Before creating or viewing Summary reports, ensure you have configured Security Manager, turned on auditing or logging, and configured SQL Server permissions.

In addition, ensure you have configured the Web address for the SQL Server Report Server Virtual Directory before creating or viewing reports. Users access Summary reports online using either the SQL Server Report Server or SQL Server Report Manager Virtual Directories.

For more information about configuring the SQL Server Report Server Web address, see “Configuring Web Addresses” on page 294.

Note
If you do not configure the Reports Web address in the Development Console Global Settings, the Control Center does not display the Launch Summary Reports task.

For more information about turning on auditing or logging, see the Configuration Wizard and the module documentation for products you want to monitor. For more information about configuring SQL Server permissions, see the Microsoft SQL Server Management Studio Help.

Adding a Data Source

Before uploading or viewing Summary reports using the Report Manager or Report Server Web interfaces, specify the reporting cube as the data source from which Summary reports will pull summarized log data.

To add a data source:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Reporting group and that has the appropriate SQL Server permissions to view reports. For more information about Security Manager groups and permissions, see “Understanding Requirements and Permissions” on page 24. For more information about SQL Server permissions, see the Microsoft SQL Server Help.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.
3. In the Navigation pane, click **Configuration Groups**.
4. On the Tasks menu, click **Configuration Group Tasks > Launch Summary Reports**. The Control Center launches the Report Manager Website in an Internet Explorer window.
5. Click **New Data Source**.
6. Specify a name and description for the data source.
7. Under Connection Type, select **Microsoft SQL Server Analysis Services**.
8. In the Connection String text box, type `Data Source=`*`ReportingServerName[\InstanceName]`*`;Initial Catalog=SMReporting`, where *`ReportingServerName`* is the Security Manager reporting server and *`InstanceName`* is the SQL Server instance on which the reporting cube is installed, if applicable.
9. Select **Windows integrated security**, unless your security policy specifies that you use another method to connect. For more information about fields on a window, see the Report Manager Help.
10. Click **OK**.
11. Click **Home**.

Uploading Summary Reports

Security Manager provides several preconfigured Summary reports for common, useful views of summarized log data in the installation kit. In addition, users can download new and updated reports from the Summary Reports section of the NetIQ Support site for Security Manager at `www.netiq.com/support/sm/`. After uploading into SQL Server Report Manager, users can view downloaded reports using the Report Manager or Report Server Websites.

Users can upload report files (`.rdl`) into the Report Manager Website, configure the reports to use a specific data source, and then view the reports. For more information about viewing uploaded Summary reports, see "Viewing Summary Reports" on page 169.

To upload a preconfigured Summary report to the Report Manager Website:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Reporting group and that has the appropriate SQL Server permissions to view reports. For more information about Security Manager groups and permissions, see "Understanding Requirements and Permissions" on page 24. For more information about SQL Server permissions, see the Microsoft SQL Server Help.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.
3. In the Navigation pane, click **Configuration Groups**.
4. On the Tasks menu, click **Configuration Group Tasks > Launch Summary Reports**. The Control Center launches the Report Manager Website in an Internet Explorer window.
5. Click **Upload File**.
6. Browse to the `.rdl` file you want to upload.
7. Specify a name for the report, if necessary.
8. Click **OK**.
9. Click **Show Details**.

10. On the uploaded report row, click **Edit**.

11. Click **Data Sources**.

12. Click **Browse**.

13. Select the appropriate data source.

14. Click **OK**.

15. Click **Apply**.

16. Click **Home** to view all Summary reports.

Viewing Summary Reports

Any user with the appropriate SQL Server permissions can view uploaded or deployed Summary reports online through the Report Manager Website, including both preconfigured Summary reports provided with Security Manager and custom Summary reports deployed on the reporting server.

Before viewing Summary reports, configure the Web address for the Report Manager Website. For more information about configuring the Report Manager Website address, see “Configuring Web Addresses” on page 294.

To view published Summary reports:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Reporting group and that has the appropriate SQL Server permissions to view reports. For more information about Security Manager groups and permissions, see “Understanding Requirements and Permissions” on page 24. For more information about SQL Server permissions, see the Microsoft SQL Server Help.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.

3. In the Navigation pane, click **Configuration Groups**.

4. On the Tasks menu, click **Configuration Group Tasks > Launch Summary Reports**. The Control Center launches the Report Manager Website in an Internet Explorer window.

5. ***If Internet Explorer prompts you for your user account and password,*** specify the user account and password for the domain in which the Report Manager Website is located and click **OK**.

6. ***If you want to view a report within a specific project,*** click the project folder.

7. Click the name of the Summary report you want to view.

8. When finished, close Internet Explorer.

Note

In addition to accessing Summary reports through the Report Manager Website, you can view Summary reports on the Report Server Website.

The default Report Server Website address is ***`ReportingServerName$InstanceName/`***`ReportServer`, where ***`ReportingServerName`*** is the Security Manager reporting server and ***`InstanceName`*** is the SQL Server instance on which the reporting cube is installed, if applicable.

This interface allows you to only view reports and not modify or create reports.

For more information about SQL Server Reporting Services, see the Report Manager Help.

Creating Basic Summary Reports

Using the Report Builder component of the Report Manager Web interface, you can create basic Summary reports as desired from the summarized log data stored in the reporting cube. Before creating basic Summary reports, generate a new Report Server model to use for all reports.

To create more in-depth, advanced Summary reports, use the SQL Server Business Intelligence Development Studio tool. For more information about creating advanced Summary reports, see “Creating Advanced Summary Reports” on page 172.

To generate a Report Server model and create a basic Summary report:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp Reporting group and that has the appropriate SQL Server permissions to view and create reports. For more information about Security Manager groups and permissions, see "Understanding Requirements and Permissions" on page 24. For more information about SQL Server permissions, see the Microsoft SQL Server Help.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.
3. In the Navigation pane, click **Configuration Groups**.
4. On the Tasks menu, click **Configuration Group Tasks > Launch Summary Reports**. The Control Center launches the Report Manager Website in an Internet Explorer window.
5. To generate a Report Server model, complete the following steps:
    a. Click the data source you want to use for the report.

    b. Click **Generate Model**.

    c. Specify a name and description for the model.

    d. Click **OK**.

    e. Click **Home**.
6. To create a new report, complete the following steps:
    a. Click **Report Builder**.

    b. ***If Microsoft Report Builder displays a confirmation message,*** click **Yes**.

    c. Specify the name of the Report Manager site where you want to publish the report.

    d. Select a model and data source for the report.

    e. Select a report layout.

    f. Click **OK**.

   g. Drag and drop column fields to the Report Layout pane to create a report. For more information about creating reports using Microsoft Report Builder, see the Microsoft Report Builder Help.

   h. When you finish creating the report, click **File > Save**.

   i. Specify a name for the report and click **Save** to save the `.rdl` file to the Report Manager Website.

   j. Repeat Steps **a** through **i** for each report you want to create.

   k. Close Microsoft Report Builder.

7. Click **Home**.

8. Click the name of the Summary report.

9. When finished, close Internet Explorer.

Creating Advanced Summary Reports

Using the SQL Server Business Intelligence Development Studio tool installed with SQL Server Analysis Services, you can create more detailed, in-depth custom Summary reports of the summarized log data stored in the reporting cube. The SQL Server Business Intelligence Development Studio tool is much more powerful than the Report Builder used through the Report Manager Web interface and is primarily used by experts and developers who need more advanced capabilities in a report-generation application.

To create a Summary report using SQL Server Business Intelligence Development Studio, you need to create a Report Server project and specify a data source to use for the report. After creating a Report Server project, you can create as many Summary reports as you need.

For more information about creating custom Summary reports, see the SQL Server Management Studio and SQL Server Business Intelligence Development Studio Help.

To create a custom Report Server project and advanced Summary report:

1. Log on to the reporting server computer using an account that has SQL Administrator privileges. For more information about SQL Server permissions, see the Microsoft SQL Server Help.
2. Start the **SQL Server Business Intelligence Development Studio** in either the Microsoft SQL Server 2005 or Microsoft SQL Server 2008 program group.
3. To create a new Report Server project, complete the following steps:
   - **a.** On the **File** menu, click **New > Project**.
   - **b.** In the right pane, click **Report Server Project**.
   - **c.** Under **Create an Empty Report Server Project**, specify a name and other appropriate values.
   - **d.** Click **OK**.
4. To add a data source, complete the following steps:
   - **a.** In the Solution Explorer, right-click **Shared Data Sources** and click **Add New Data Source**.
   - **b.** On the General tab, type the name of the new data source and select **Microsoft SQL Server Analysis Services** as the type.
   - **c.** Click **Edit**.
   - **d.** Type the name of your SQL Server Analysis Services server. In many cases, this is the name of the reporting server. You can also specify a particular instance of SQL Server Analysis Services to use as the data source.
   - **e.** In the **Connect to a database** list, select **SMReporting**.
   - **f.** Click **Test Connection** to verify that the name of the Analysis Services instance is correct and click **OK**.
   - **g.** Click **OK**, and then click **OK** again to exit the Shared Data Source window.

5. To add a new report template, complete the following steps:

   a. In the Solution Explorer, right-click **Reports** and click **Add New Report**.

   b. Follow the instructions in the Report Wizard to create a new report template. For more information about fields on a window, see the Help.

   When you finish creating the report template, SQL Server Business Intelligence Design Studio opens the report in the center pane. You can view the report data, use the Layout tab to customize the appearance of the report, or preview the published report. For more information about customizing reports, see the Report Wizard Help.

6. To publish all project reports to the Report Server, complete the following steps:

   a. In the Solution Explorer, select the new project.

   b. On the Project menu, click **Properties**.

   c. In the **TargetServerURL** field, specify the name of the reporting server where you want to publish the report. The reporting server name should use the `http://`*`ReportingServerName$InstanceName/`*`ReportServer` format. If you have more than one SQL instance installed, make sure to include the name of the SQL instance where you created the report. For the default instance, only use the reporting server name.

   d. Click **OK**.

   e. In the Solution Explorer, right-click the project and select **Deploy**.

7. Close SQL Server Business Intelligence Studio.

After you create and deploy a new Summary report, the report template is saved in the Reports folder of the project you created. For more information about viewing deployed reports, see “Viewing Summary Reports” on page 169.

Converting UTC Time

All Forensic Analysis reports display data using the **coordinated universal time (UTC)** standard. UTC is the international time standard based on International Atomic Time (TAI). Optionally, you can run Forensic Analysis queries and view completed Forensic Analysis reports in the local time of the Control Center computer.

When specifying report parameters or examining report results, you may need to convert the date and time from UTC to your time zone to understand the data represented in the report. UTC, like Greenwich mean time (GMT), uses the zero longitude as a reference point in a 24-hour format. You convert from UTC in the same way you convert from GMT, by subtracting or adding hours as necessary. For example, if you live in the central time zone and Daylight Saving Time is off, subtract 6 hours from the UTC value to obtain the value for your time zone.

However, UTC also affects the *date*. For example, if the UTC time is 0500 on May 2nd and you are in the central time zone with Daylight Saving Time off, then the local time is 11:00 PM on May 1st.

The following table describes the UTC time zones.

City or Location	Time Zone
Eniwetok	UTC-12
Samoa	UTC-11
Hawaii	UTC-10
Alaska	UTC-9
Pacific US Standard (PST)	UTC-8
Pacific US Daylight Saving (PDT)	UTC-7
Mountain US Standard (MST)	UTC-7
Mountain US Daylight Saving (MDT)	UTC-6
Central US Standard (CST)	UTC-6

City or Location	Time Zone
Central US Daylight Saving (CDT)	UTC-5
Eastern US Standard (EST)	UTC-5
Eastern US Daylight Saving (EDT)	UTC-4
Atlantic, Canada	UTC-4
Brazil, Buenos Aries	UTC-3
Mid-Atlantic	UTC-2
Cape Verdes	UTC-1
Greenwich Mean Time, Dublin	UTC
Berlin, Rome	UTC+1
Israel, Cairo	UTC+2
Moscow, Kuwait	UTC+3
Abu Dhabi, Muscat	UTC+4
Islamabad, Karachi	UTC+5
Almaty, Dhaka	UTC+6
Bangkok, Jakarta	UTC+7
Hong Kong, Beijing	UTC+8
Tokyo, Osaka	UTC+9
Sydney, Melbourne, Guam	UTC+10
Magadan, Soloman Is.	UTC+11
Fiji, Wellington, Auckland	UTC+12

Chapter 6

Monitoring Your Environment

Security Manager enables you to monitor various platforms in your enterprise with modules. Modules can contain processing rules and embedded expertise, as well as other information, to configure Security Manager products to monitor certain platforms. Security Manager allows you to monitor these platforms with views and reports in the Control Center.

Periodically, new or updated modules are available and you can download and install new or updated modules using the Security Manager Module Installer. The **Module Installer** queries the NetIQ AutoSync Server to determine whether an update is available, and then allows you to install modules. The **AutoSync Server** is a Web server from which the Module Installer can download new and updated modules.

NetIQ publishes all new or updated module releases to a special RSS feed on the NetIQ Web site. Using a feed reader, you can subscribe to the following Security Manager RSS feed and view the latest module-related information available:

```
http://products.netiq.com/SM/SecurityManager.xml
```

Monitoring Antivirus Applications

Security Manager for Antivirus allows you to monitor the availability, currency, and installation of antivirus applications on monitored computers with a centralized console. Security Manager for Antivirus allows you to monitor viruses detected by antivirus applications across your network in real-time views.

Security Manager collects antivirus event information from the Application log. Security Manager also collects Security Manager script-generated events used to provide additional critical information, such as if computers have the application installed or how long ago the application performed an update.

For more information about monitoring antivirus applications, see the module documentation for products you want to monitor, located on the user interfaces computer in the Documentation folder of the NetIQ Security Manager program group.

However, if you updated the module, the updated module documentation for the module might not be in this folder. To obtain updated documentation, synchronize your existing documentation with the content stored in the database. For more information about synchronizing documentation, see "Obtaining the Latest Documentation" on page 189.

Monitoring Databases

Security Manager for Databases enables Security Manager to monitor database user privileges and the actions users perform on database tables. Security Manager for Databases collects events from logs and stores them in secure repositories so you can archive this data, create reports for management or auditing purposes, and analyze critical events to research issues.

For more information about monitoring databases, see the module documentation for products you want to monitor, located on the user interfaces computer in the Documentation folder of the NetIQ Security Manager program group.

However, if you updated the module, the updated module documentation for the module might not be in this folder. To obtain updated documentation, synchronize your existing documentation with the content stored in the database. For more information about synchronizing documentation, see “Obtaining the Latest Documentation” on page 189.

Monitoring Firewalls

Security Manager for Firewalls monitors various firewall products to identify suspicious activity occurring on or detected by firewalls, and monitor firewall health and configuration.

Security Manager collects syslog messages, firewall logs, audit logs, and accounting logs.

For more information about monitoring firewalls, see the module documentation for products you want to monitor, located on the user interfaces computer in the Documentation folder of the NetIQ Security Manager program group.

However, if you updated the module, the updated module documentation for the module might not be in this folder. To obtain updated documentation, synchronize your existing documentation with the content stored in the database. For more information about synchronizing documentation, see “Obtaining the Latest Documentation” on page 189.

Monitoring Intrusion Detection Systems

Security Manager for IDS provides a way to easily monitor intrusion detection system (IDS) product operations and policy settings, and monitor suspicious activity detected by IDS products.

Security Manager collects log data on intrusion and attack attempts and configuration and state changes.

For more information about monitoring IDS products, see the module documentation for products you want to monitor, located on the user interfaces computer in the Documentation folder of the NetIQ Security Manager program group.

However, if you updated the module, the updated module documentation for the module might not be in this folder. To obtain updated documentation, synchronize your existing documentation with the content stored in the database. For more information about synchronizing documentation, see "Obtaining the Latest Documentation" on page 189.

Monitoring Operating Systems

Security Manager can collect events from logs or syslog messages from Windows, UNIX, and iSeries computers.

For more information about monitoring operating systems, see the module documentation for products you want to monitor, located on the user interfaces computer in the Documentation folder of the NetIQ Security Manager program group.

However, if you updated the module, the updated module documentation for the module might not be in this folder. To obtain updated documentation, synchronize your existing documentation with the content stored in the database. For more information about synchronizing documentation, see "Obtaining the Latest Documentation" on page 189.

Monitoring Routers and Switches

Security Manager for Routers and Switches can monitor events on routers and switches. Security Manager can collect data from routers and switches.

For more information about monitoring routers and switches, see the module documentation for products you want to monitor, located on the user interfaces computer in the Documentation folder of the NetIQ Security Manager program group.

However, if you updated the module, the updated module documentation for the module might not be in this folder. To obtain updated documentation, synchronize your existing documentation with the content stored in the database. For more information about synchronizing documentation, see “Obtaining the Latest Documentation” on page 189.

Monitoring Workstations

Security Manager can monitor Windows server and Windows workstation computers, collecting data from both. Because many environments can include many workstation computers, Security Manager uses a scalability multiplier to enable central computers to monitor large numbers of agents installed on workstations.

Agents deployed on workstation computers may send relatively few events to the central computer. However, while an agent may need to send event data to the central computer infrequently, the agent must heartbeat within the configured heartbeat interval in order to remain active. Continually receiving heartbeats from multiple computers, even without event data, can affect the performance of the central computer.

If you want to enable a central computer to monitor a large number of low-volume workstation computers without becoming overburdened, you can configure the workstation scalability multiplier to increase the interval between agent communications. The agent then multiplies the default heartbeat interval and other agent communication settings by the multiplier value for all workstation computers.

For example, when a central computer uses the default multiplier value of `36` for all workstations, all workstation computers heartbeat every 3 hours instead of the default 300 seconds. The delay reduces the performance load on the central computer, allowing one central computer to monitor a large number of workstation computers.

If no computers belong to the Windows Workstations computer group, changes to the workstation scalability multiplier setting do not affect your agent computers.

Note

When you deploy an agent to a workstation computer, the workstation uses the server agent heartbeat setting until the central computer sends initial configuration information to the workstation agent. After receiving configuration information, the workstation agent uses the scalability multiplier when heartbeating.

Using the Development Console, you can modify the default scalability multiplier setting. For more information about modifying global agent settings in the Development Console, see "Configuring General Agent Settings" on page 292.

Updating Security Manager with the Latest Modules

You typically install modules when you install Security Manager. Modules for Security Manager contain processing rules, reports, and embedded expertise that enable you to configure Security Manager products to monitor various platforms and applications in your environment.

Understanding AutoSync

Periodically, new modules and updates to existing modules are provided between major releases of Security Manager. The latest modules are provided on the NetIQ AutoSync Server.

You can use the Module Installer to check the NetIQ AutoSync Server for new or updated modules. If a new or updated module is available, you can download and install it with the Module Installer. The Module Installer contains the URL to the NetIQ AutoSync Server.

Enabling Secure AutoSync Connections

You can connect to the NetIQ AutoSync Server using a TCP/IP connection or a connection that uses secure HTTP (HTTPS).

Note
If using Security Manager in a firewall environment, you must ensure HTTP port 80 is open to enable Security Manager to access the NetIQ AutoSync Server. For more information about configuring ports for Security Manager, see the *Installation Guide for NetIQ Security Manager*.

To enable a secure connection to the NetIQ AutoSync Server:

1. Log on to a Control Center computer as a member of the OnePointOp Operators group.

   Note
   You can run the Module Installer on a central computer or on a user interface computer. However, if you run the Module Installer from the installation kit, you must be on a central computer.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.
4. On the Tasks menu, click **Global Tasks > Launch Module Installer**.
5. In the Module Installer, click **Settings**. For more information about the fields on a window, see the Help.
6. In the **NetIQ AutoSync Server URL** text box, change `http:` to `https:`.
7. Click **OK**.

Installing New or Updated Modules

You can download and install new or updated modules with the Module Installer, which you access using the Control Center.

If you create custom modules, use the Development Console to install them. For more information about custom modules, see the *Programming Guide for NetIQ Security Manager*.

When you install an update to an existing module, the Module Installer merges the new module data with any existing customizations you may have made to rules or to the knowledge base. If you want to overwrite some or all of you customizations with the new module data, see the *Programming Guide for NetIQ Security Manager*.

Consider running the Module Installer at regular intervals, such as once per month, to ensure you are aware of the latest available updates.

Install a module only once for a configuration group. Once installed, the module knowledge is available to all computers in the configuration group.

Installing Modules on a Computer with Internet Access

You can install modules on a computer with Internet access by using AutoSync to update the computer with the most recent versions of the modules.

To install modules on a computer with Internet access:

1. Log on to a Control Center computer as a member of the OnePointOp Operators group.

   Note
   You can run the Module Installer on a central computer or on a user interface computer. However, if you run the Module Installer from the installation kit, you must be on a central computer.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.
4. On the Tasks menu, click **Global Tasks > Launch Module Installer**.
5. ***If you want to install new or updated modules from the NetIQ AutoSync server,*** select **NetIQ AutoSync Server**.

6. ***If you want to install a module from a folder or share,*** complete the following steps:

   a. Select **Local Network** and then click **Browse**.

   b. Select the folder where you saved the modules, and then click **OK**.

   c. Click **Go**.

7. ***If you want to determine whether an update is available for a module,*** find the row for the appropriate module. If an update is available, the Module Installer displays the value, **Update Available**, in the **Status** column.

   Note
   When both **Local Network** and **NetIQ AutoSync Server** are selected and the Module Installer finds the same module in both places, it displays the module with the most current version.

8. ***If you want to apply a license,*** complete the following steps:

   a. Click **Settings**.

   b. Click **Add License**.

   c. Select the license you want to apply, and click **Open**.

   d. Click **OK**.

9. Select the modules you want to update or install.

10. Click **Install**.

11. Click **Continue**.

12. Click **Finish**, then click **Close**.

Installing Modules on a Computer with No Internet Access

You can also manually download and transfer modules to install to computers with no Internet access.

To install modules on a computer with no Internet access:

1. Log on to a computer that has Internet access.
2. Open a browser and navigate to `http://products.netiq.com/sm/securitymanager.xml` (use `https://products.netiq.com/sm/securitymanager.xml` for a secure connection).
3. Click the name of appropriate module to download.
4. Save the file to a network location that is accessible by the Module Installer.
5. Log on to the Control Center computer as a member of the OnePointOp Operators group.
6. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
7. In the Navigation pane, click **All Folders**.
8. On the Tasks menu, click **Global Tasks > Launch Module Installer**.
9. In the Module Installer, select **Local Network** and then click **Browse**.
10. Select the folder where you saved the modules, and then click **OK**.
11. Click **Go**.
12. ***If you want to apply a license,*** complete the following steps:
    a. Click **Settings**.
    b. Click **Add License**.
    c. Select the license you want to apply, and click **Open**.
    d. Click **OK**.
13. Select the modules you want to update or install.
14. Click **Install**.
15. Click **Continue**.
16. Click **Finish**, then click **Close**.

Upgrading Providers

When you update modules using the Module Installer, you may also need to upgrade the providers for those modules installed on your agent computers. If an updated module includes an updated provider, the Module Installer displays a message notifying you that you should upgrade.

The following modules or products include providers that may require upgrading:

- Event Manager for Check Point
- Log Manager for Check Point
- NetIQ Change Guardian for Group Policy
- NetIQ Change Guardian for Windows
- Security Manager Self-monitoring

You can scan managed computers using the Development Console to upgrade the provider on your managed agents. You must manually upgrade the provider on unmanaged agents.

Note

You need to upgrade providers only if you use the provider functionality in your environment. For example, if you do not monitor Windows computers using proxy agents, you do not need to upgrade the Windows Proxy Provider included in the Security Manager Self-monitoring module.

For more information about providers, see the *Programming Guide for NetIQ Security Manager.*

To upgrade providers on your Security Manager agents:

1. Log on to a central computer as a member of the OnePointOp ConfgAdms group.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration**.
4. In the left pane, click **Central Computers**.

5. In the right pane, select the central computer that manages the agents you want to upgrade.

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

7. Click **OK**.

Note

Ensure the Remote Registry Service is started on the managed agent and central computer before attempting to scan agents. You can review services using the Component Services Administrative Tool, located in the Control Panel.

---

8. In the left pane, expand **Pending Agents > Installation** to see the results of the managed computer scan.

9. ***If you want to upgrade providers on an unmanaged agent,*** complete the following steps:

   a. In Windows Explorer, navigate to the following location on the central computer:

      ```
      installation folder\NetIQ Security
      Manager\OnePoint\InstallMcsApps\ProgrammableProvider
      ```

      where *`installation folder`* is the location where you installed Security Manager.

   b. Log on to the unmanaged agent computer from the central computer.

   c. Copy all `.cab` files from the `ProgrammableProvider` folder on the central computer to the following location on the agent computer:

      ```
      installation folder\NetIQ Security
      Manager\OnePoint\Providers\configgroup\IncomingPrgProviders
      ```

where *`installation folder`* is the location where you installed Security Manager and *`configgroup`* is the name of your configuration group.

Notes

- Do not copy files from the `ProgrammableProvider` folder on the central computer into the `IncomingPrgProviders` folder on the central computer.
- You do not need to restart any Security Manager services on the agent or the central computer after copying the `.cab` files to the agent computer.

d. Log off of the unmanaged agent computer.

10. Close the Development Console.

Obtaining the Latest Documentation

An updated module includes an updated version of the module documentation.

Each time you open the Control Center, Security Manager automatically copies the latest version of the documentation to the following location on the local computer:

`installation folder``\NetIQ Security Manager\OnePoint\Documentation`

where *`installation folder`* is the location where you installed Security Manager.

To update and view the documentation:

1. Log on to the Control Center computer as a member of the OnePointOp Operators group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Click **Documentation** in the NetIQ Security Manager program group.

Chapter 7

Administering Agents

Security Manager monitors computers using host-based agents and proxy agents. An agent is a service that runs on a monitored computer to collect events and execute automatic responses. A **proxy agent** allows you to monitor firewall and IDS devices without installing the agent directly on the device. A proxy agent also allows you to remotely monitor Windows computers.

Understanding Managed and Unmanaged Windows Agents

A **managed agent** is an agent the central computer can install and upgrade remotely. An **unmanaged agent** is an agent you manually install and update. The central computer cannot upgrade unmanaged agents.

Use an unmanaged agent in circumstances where a managed agent is not supported. Security Manager cannot deploy managed Windows agents to remote Windows computers that are located outside a firewall. Consider installing an unmanaged agent to access the network over a WAN or a slow connection.

Note

NetIQ Corporation does not support managed agents separated from the central computer by a firewall or other device or configuration that can impede RPC or NetBIOS functionality.

When monitoring computers behind a firewall, NetIQ Corporation recommends installing unmanaged agents on your remote computers.

For more information about installing agents in a firewall environment, see the *Installation Guide for NetIQ Security Manager.*

When you deploy a managed agent or install an unmanaged agent you assign that agent to a central computer.

For a managed agent, a central computer performs the following functions:

- Installs and upgrades the managed agent
- Scans the managed agent
- Sends rules and configuration information to the managed agent
- Receives events from the managed agent

For an unmanaged computer, a central computer performs the following functions:

- Sends rules and configuration information to the unmanaged agent
- Receives events from the unmanaged agent

The central computer cannot install, upgrade, or scan an unmanaged agent.

All managed agents are authorized by the central computer by default. You can use either the Agent Administrator utility or Security Manager Control Center to specifically authorize each unmanaged agent.

It is recommended that you monitor both the log archive server and reporting server using agents. Monitoring the log archive and reporting servers using agents enables you to more easily monitor the performance and status of Security Manager as a whole.

Understanding Discovery and Managed Windows Agent Deployment

Security Manager can automatically deploy agents on computers that you identify. You can use the Agent Administrator to select these computers individually, or you can select multiple computers based on common characteristics using discovery rules.

Discovery rules are rules that identify computers. Security Manager deploys a managed agent to a discovered computer and monitors it. Security Manager evaluates discovery rules during a managed computer scan. Managed computer scans occur daily at 2:05 AM. You can manually run a managed computer scan.

Use discovery rules to identify multiple computers with similar characteristics. The central computer periodically scans all managed Windows computers assigned to it and uses computer grouping rules to determine whether to place a computer in a computer group. Central computers then install or update managed agents on computers as necessary.

Central computers install managed agents only when a computer matches the criteria for inclusion in a computer group. You can configure central computers to automatically install agents or to wait for your approval.

To deploy managed agents, the service account used to run Security Manager must be a member of the local Administrators group on the central computer and all agent computers that the central computer will manage in the domain. If you want the service account to have rights to install agents in other trusted domains, the service account must be a member of the local Administrators group on all agent computers that the central computer will manage in the trusted domain.

Notes

- Security Manager uses NetBIOS to identify computers. Any computer on which you want to install a Windows agent must have a NetBIOS-compliant name.
- When you deploy a managed agent to a new computer, Security Manager does not immediately display the new computer in the Infrastructure Components > Agents view. The agent first sends a heartbeat to the central computer and receives configuration data from Security Manager. At the next agent heartbeat, the agent sends configuration information back to the central computer. Security Manager then assigns the new agent computer to all applicable computer groups and displays the agent in the Agents view.

  For more information about configuring the heartbeat interval for agents, see “Configuring General Agent Settings” on page 292.

Security Manager cannot deploy managed agents on computers outside a firewall or on a non-Windows platform. For more information about manually installing unmanaged Windows agents, see “Understanding Unmanaged Windows Agent Installation” on page 199.

When assigning agents to computers, ensure that you assign no more agents to the central computer than it can handle. If you want to rebalance the distribution of agents across central computers, use the Agent Administrator to assign an agent to a different central computer.

Deploying a Managed Windows Agent

Use this procedure to deploy managed agents on Windows computers you want to monitor.

After the central computer installs a managed agent, you may need to restart the computer before the managed agent will start. If the central computer logs an event with an event ID of `21116`, `21118`, or `21169`, you need to restart the computer.

To immediately deploy a managed Windows agent:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Configuration Groups**.
4. Select the appropriate configuration group in the Results window.
5. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.
6. In the Agent Administrator window, click the Managed Agents tab.
7. In the right pane, click **Deploy Agents**.
8. Click **Add**.
9. Specify a computer you want to monitor, and then click **OK**.
10. Repeat Steps 7 through 9 for each computer you want to monitor.
11. ***If you want to deploy the managed agents at the next scan,*** click **Finish**.

12. ***If you want to deploy the managed agents immediately or add them to the Pending Agents Installation list,*** complete the following steps:

    a. In the Deploy Action column, click the row corresponding to an agent.

    b. Select one of the following options:

    - To deploy the managed agent immediately, select **Deploy now**.
    - To add the computer to the Pending Agents Installation list, select **Add to pending list**. Depending on your settings, Security Manager either approves and deploys agents during the next managed computer scan, or places them in the list pending your approval.

13. Click **Finish**.

For more information about deploying an agent at the next scan, see “Scanning Managed Computers” on page 203.

For more information about deploying agents added to the Pending Agents Installation list, see “Handling Pending Installations” on page 210.

Deploying Multiple Managed Windows Agents

You can create discovery rules to define which Windows agent computers you want to discover. Security Manager applies the discovery rules every time it runs the daily managed computer scan.

You can use string matching or Active Directory Light Directory Access Protocol (LDAP) queries to discover multiple computers with common attributes. Because Security Manager runs the discovery rules at every scan, Security Manager discovers any new computers you have added to your network that fit the rule criteria.

Depending on your settings, Security Manager installs managed agents on discovered computers, or adds them to the pending Agents Installation list to be approved or installed at the next managed computer scan. For more information about pending installations, see “Handling Pending Installations” on page 210.

Note

Security Manager does not automatically deploy agents on UNIX computers. To deploy an agent to a UNIX computer, you must use the UNIX Agent Manager.

For more information about deploying UNIX agents, see the NetIQ UNIX Agent documentation.

After the central computer installs an agent on a Windows computer, you might need to restart the computer before the managed agent will start. If the central computer logs an event with an event ID of `21116`, `21118`, or `21169`, you need to restart the computer.

To discover and deploy Windows agents:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Configuration Groups**.
4. Select the appropriate configuration group in the Results window.
5. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.
6. In the Agent Administrator window, click the Managed Agents tab.
7. In the right pane, click **Configure Agent Discovery Rules**.
8. Click **Add**.
9. Select **Include Computers**, and then click **Next**.
10. Complete the rules creation wizard, specifying parameters that select the computers you want to discover. For more information about fields on a window, see the Help.

11. Select the check box and row corresponding to the rule you created.

12. Click **Next**.

    - To discover computers at the next managed computer scan, click **No**.
    - To immediately discover computers, click **Yes**.

13. ***If you clicked Yes,*** select the central computers that will manage the computers you discover.

14. Click **Next**.

15. ***If you want to deploy agents immediately,*** click **Yes**.

16. ***If you want to add agents to the list of computers pending deployment,*** click **No**.

17. Click **Next**.

18. ***If you want to approve deployment,*** select **Approved** for each discovered computer to which you want to deploy a managed agent, and then click **Next**.

19. ***If you do not want to approve deployment at this time,*** clear **Approved** for each discovered computer you want to place in the Pending Agent Installation list, and then click **Next**.

    Note
    If you do not approve deployment to a computer, Security Manager places the computer in the Pending Agent Installations list until you approve deployment.

20. Specify whether to immediately deploy agents to approved computers or to deploy the agents at the next managed computer scan.

21. Click **Finish**.

Note
If you discover agents using a discovery rule, modify an existing rule or create a new discovery rule, and run the modified or new discovery rule, the Agent Administrator may display previously-discovered computers in both the Discovered Computers list and Agent Summary View.

If you want to only display computers discovered by a modified or new discovery rule, remove any previously-discovered computers from both the Manage Pending Actions list and Agent Summary View before using the discovery rule.

For more information about deploying an agent at the next managed computer scan, see "Scanning Managed Computers" on page 203.

Understanding Unmanaged Windows Agent Installation

The unmanaged Windows agent setup program, `manualagent.msi`, installs an unmanaged agent on the local Windows computer and guides you through Windows agent configuration. You can also use a transform file to specify setup options and silently run the setup program. Additionally, you can specify that multiple configuration groups monitor the unmanaged agent. For more information about unmanaged agent installation, see the *Installation Guide for NetIQ Security Manager*.

Understanding Agentless Monitoring and Proxy Agents

If you do not want to install an agent on a computer, you can monitor the computer by using a proxy agent. A proxy agent is a Windows agent that you specify to remotely monitor and collect events from an **agentless monitored computer**, a computer that does not have a Security Manager agent.

A proxy agent can also be used to monitor non-agent endpoints, including non-Windows computers, devices, database instances, applications, or custom providers.

A proxy agent for Windows can monitor the following Windows event logs on multiple Windows computers:

- Application
- System
- Security
- DNS
- File Replication
- Directory Service

Note

Proxy agents must use the same Windows operating system as any monitored agentless computers, including the same application software associated with the role of the computer. For example, if you are monitoring a Windows Server 2008 domain controller, the proxy agent must also be a Windows Server 2008 domain controller.

Proxy Agent Responses

No responses are supported on the agentless monitored computer. Proxy agents do not support script responses. However, the following responses are supported and run on the proxy agent computer:

- Send a notification to a notification group
- Send an email
- Send a page
- Send an external command notification
- Execute a command or batch file
- Send an SNMP trap
- Change state variables

Configuring Agentless Windows Monitoring

Using the Agent Administrator, you can configure a Windows agent to monitor another Windows computer with no agent. Agentless monitoring allows you to collect Windows event logs and monitor security applications for computers on which you cannot install an agent.

To configure agentless monitored computers:

1. Ensure you have a Windows agent installed that you want to use as a proxy agent. For more information about installing agents, see “Understanding Discovery and Managed Windows Agent Deployment” on page 193 and “Understanding Unmanaged Windows Agent Installation” on page 199. For more information about proxy agent requirements, see the *Installation Guide for NetIQ Security Manager.*
2. Log on to the Control Center computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
3. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

4. In the Navigation pane, click **Configuration Groups**.
5. Select the appropriate configuration group in the Results window.
6. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.
7. In the Agent Administrator window, click the Agentless Monitored Computers tab.
8. In the right pane, click **Configure Agentless Windows Monitoring**.
9. Complete the Configure Agentless Windows Monitoring wizard to select proxy agents, proxy agent credentials, and agentless monitored computers. For more information about fields on a window, see the Help.

Excluding Computers from Discovery

You can exclude a Windows computer from discovery to prevent the central computer from installing an agent on the computer. Consider excluding computers for the following reasons:

- You configured discovery rules to find a large group of computers, but would like to prevent Security Manager from installing an agent on certain computers within the group. For example, you might want to discover computers in a domain, but exclude certain computers in the domain.
- You are uninstalling an agent and deleting the computer from the Security Manager database. However, you are still running the discovery rule that initially found this computer and others with similar characteristics. You do not want to accidentally rediscover and deploy an agent to the computer.

Excluding a computer with an agent does not prevent Security Manager from monitoring the computer or cause Security Manager to uninstall the agent. For more information about uninstalling agents, see “Uninstalling Windows Agents” on page 223.

You can exclude a Windows computer using the Agent Administrator. When you exclude a computer, Security Manager runs the rule at the next managed computer scan.

To exclude a computer from discovery:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Configuration Groups**.
4. Select the appropriate configuration group in the Results window.
5. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.
6. In the Agent Administrator window, click the Managed Agents tab.
7. In the right pane, click **Configure Agent Discovery Rules**.
8. Click **Add**.
9. Select **Exclude Computers**, and then click **Next**.
10. Complete the wizard, specifying parameters that identify the computers you want to exclude from discovery. For more information about fields on a window, see the Help.

Scanning Managed Computers

Security Manager does not immediately install agents on remote computers. The central computer periodically scans computers assigned to it. The first time it scans, the central computer identifies computers on which to install agents. If you approve the computers the central computer identifies, the central computer installs agents the next time it performs a managed computer scan. By default, the central computer scans every day at 2:05 AM.

You can also scan on demand. Scanning finds computers that match the discovery rules, collects computer attributes older than 24 hours, places computers in or removes computers from computer groups, and identifies computers requiring an agent installation or upgrade. By default, Security Manager lists these computers in the Pending Agents Installation window of the Configuration snap-in, where you can choose to approve or disapprove pending installations.

To scan managed computers:

1. 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 "Understanding Requirements and Permissions" on page 24.

   Note
   The Security Manager service account must be a member of the local Administrators group on the managed agent computer and must be in a trusted domain or in the same domain as the database server.

2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration**.
4. In the left pane, click **Global Settings**.
5. In the right pane, click **Central Computers**.
6. On the Action menu, click **Properties**.
7. ***If you want to change the time and frequency that central computers automatically scan managed computers,*** specify the appropriate values on the Managed Computer Scan tab.
8. ***If you want the central computer to perform a managed computer scan now,*** click **Scan managed computers now** on the Managed Computer Scan tab.

9. Click **OK**.

> **Note**
> Ensure the Remote Registry Service is started on the managed agent and central computer before attempting to scan agents. You can review services using the Component Services Administrative Tool, located in the Control Panel.

10. In the left pane, expand **Pending Agents > Installation** to see the results of the managed computer scan.

Scanning a Single Managed Computer

If you change the configuration of a Windows agent computer, you can prompt the central computer to scan only that computer instead of all managed computers. Scanning only the affected computer takes less time than scanning all managed computers, and allows the central computer to update the affected computer immediately, instead of waiting until the scheduled scan.

Creating a Custom Task to Scan a Windows Computer

If you have changed the configuration of the computer, such as installed new software, you can scan the computer to allow Security Manager to collect computer attributes and update the agent. You can prompt the central computer to scan a single Windows computer by creating a custom task. For more information about creating custom tasks, see “Managing Custom Tasks” on page 240.

To create a task for scanning a single Windows computer:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.

4. On the Tasks menu, click **Global Tasks > Manage Custom Tasks**.
5. Select the appropriate user name from the **Task Available To** list.
6. Select **computer items** from the **Task Available For** list.
7. Click **Add**.
8. In the **Name** field, type *`CentralComputer`* `scan computer`, where *`CentralComputer`* is the name of the central computer that manages the agent. For more information about the fields on a window, click **Help**.
9. In the **Description** field, type `Causes the central computer to scan a Windows agent computer`.
10. In the **Command** field, type:

    ```
    CSCRIPT.EXE "$Agent Directory$\AMScanSingle.vbs"
    /a:CentralComputer /s:$Computer$
    ```

    Where *`CentralComputer`* specifies the name of the central computer that manages the agent. If you have multiple central computers, consider creating a task for each central computer.

    For example:

    ```
    CSCRIPT.EXE "$Agent Directory$\AMScanSingle.vbs" /a:NYC_AM023
    /s:$Computer$
    ```
11. Click **OK**.
12. Click **OK** to exit the Custom Tasks window.

Scanning a Single Windows Computer Using the Custom Task

You can run the custom task whenever you need to scan a single Windows computer that is managed by the central computer you specified in the custom task **Command** field.

To run the custom task to scan a Windows agent computer:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp Users group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Computers**.
4. In the Results window, click the computer you want to scan.
5. On the Tasks menu, click **Custom Tasks > *CentralComputer* scan computer**, where ***CentralComputer*** is the name of the central computer that manages the agent. For more information about the fields on a window, click **Help**.

Configuring Central Computer Properties

Using the Development Console, you can modify the properties for a central computer. For example, you can specify whether the central computer automatically installs agents, or places them into the Pending Agents Installation list to await your approval.

You can also modify the Global Settings used by all central computers to deploy agents. For more information about modifying Global Settings, see "Configuring Central Computer Settings" on page 290.

Note

If you modify settings in the Advanced tab of the central computer settings, you must right-click **Security Manager Development Console** in the left pane of the Development Console, select **Force Configuration Changes Now**, then manually restart the `NetIQ Security Manager` service on all affected central computers for the change to take effect.

To configure a central computer:

1. 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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand the **Security Manager Development Console**, and then expand **Configuration**.
4. Click **Central Computers**.
5. In the right pane, click the central computer you want to configure.
6. On the Action menu, click **Properties**.
7. Specify the appropriate values on the Properties tabs. For more information about the fields on a window, click **Help**.
8. Click **OK**.

Configuring Agent Properties

You can configure individual Windows agent properties if necessary, including buffering, service checking, event collection, communication failure handling, and response handling parameters, among others.

You can also modify the Global Settings used by all Windows agents in your configuration group. For more information about modifying Global Settings, see “Configuring General Agent Settings” on page 292.

Note

If you modify settings in the Communications, Buffering, Temporary Storage, Response Handling, or Advanced tabs, Security Manager automatically restarts the `NetIQ Security Manager` service on all affected agent computers.

To configure individual Windows agent properties:

1. 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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration**.
4. Click **Central Computers**.
5. In the right pane, click the central computer for the agent you want to configure.
6. On the Action menu, click **Properties**.
7. On the Managed Computers tab, click the computer with the agent you want to configure.
8. Click **Settings**.
9. Specify the appropriate values on the Properties tabs. For more information about the fields on a window, click **Help**.
10. Click **OK**.

Handling Pending Installations

Discovery rules and the settings you specify using the Agent Administrator and in the Configuration snap-in determine when an agent needs to be installed on a Windows computer. After a managed computer scan, the Pending Agents Installation window lists computers requiring agent installations and upgrades. You can approve or disapprove all pending installations or each individual pending installation.

Note

If a computer on the approved installation list is running the Windows Event Viewer or any Security Manager console, ensure you close the Windows Event Viewer and the console before starting the managed computer scan. If these products are running during a managed computer scan, you may need to restart the computer before the Security Manager agent will start.

Approving Pending Installations

By default, Security Manager requires you to manually approve deployment of managed agents. If you did not choose to immediately deploy managed agents or approve them for deployment at the next scan, Security Manager adds them to a Pending Agents Installation list, where the managed agents wait until you approve them for deployment either immediately or at the next scan.

Approving Pending Installations Using the Agent Administrator

You can use the Agent Administrator to approve pending installations of managed agents.

To approve pending installations using the Agent Administrator:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

3. In the Navigation pane, click **Configuration Groups**.
4. Select the appropriate configuration group in the Results window.
5. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.
6. In the Agent Administrator window, click the Managed Agents tab.
7. In the left pane, click **Managed Agents**.
8. In the right pane, click **Manage Pending Actions**.
9. Select computers to approve for installation, and then click **Next**. For more information about the fields on a window, see the Help.
10. ***If you want to install the agent immediately,*** click **Yes**.
11. ***If you want to schedule the approved agent installation for the next managed computer scan,*** click **No**.
12. Click **Finish**.

Approving Pending Installations Using the Development Console

By default, Security Manager adds Windows computers requiring agent installations or upgrades to the Pending Agents Installation list to wait for approval. You can approve all pending installations or upgrades or each individual pending installation or upgrade using the Development Console.

To approve pending installations or upgrades using the Development Console:

1. 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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration > Pending Agents > Installation**.
4. ***If you want to approve all pending installations or upgrades,*** on the Action menu, click **Approve All Pending Installations**.

5. ***If you want to approve individual pending installations or upgrades,*** complete the following steps for each computer you want to approve:

   a. In the right pane, click the computer you want to approve.

   b. On the Action menu, click **Approve**.

6. ***If you want to install all approved installations and upgrades now***, on the Action menu, click **Install All Approved Agents Now**. The time required for installation depends on your network configuration.

Disapproving Pending Installations

In some circumstances, you may not want to automatically deploy managed agents to computers that you want to monitor. If you have already approved an agent for deployment at the next scan but want to delay that deployment, you can disapprove deployment indefinitely.

Disapproving Pending Installations Using the Agent Administrator

You can use the Agent Administrator to disapprove pending installations.

To disapprove pending installations using the Agent Administrator:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

3. In the Navigation pane, click **Configuration Groups**.

4. Select the appropriate configuration group in the Results window.

5. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.

6. In the Agent Administrator window, click the Managed Agents tab.

7. In the right pane, click **Manage Pending Actions**.

8. Clear the check boxes of approved agents you want to disapprove, and then click **Next**. For more information about the fields on a window, click **Help**.
9. Click **No**.
10. Click **Finish**.

Disapproving Pending Installations Using the Development Console

By default, Security Manager adds Windows computers requiring agent installations or upgrades to the Pending Agents Installation list to wait for approval. You can disapprove all pending installations or upgrades or each individual pending installation or upgrade using the Development Console. The central computer waits for approval before installing or upgrading agents on Windows computers.

To disapprove all pending installations using the Development Console:

1. 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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console > Configuration > Pending Agents > Installation**.
4. ***If you want to disapprove all pending installations or upgrades,*** on the Action menu, click **Disapprove All Pending Installations**.
5. ***If you want to disapprove individual pending installations or upgrades,*** complete the following steps on each computer you want to disapprove:
    a. In the right pane, click the computer you want to disapprove.
    b. On the Action menu, click **Disapprove**.
6. Close the Development Console.

Verifying Windows Agent Installation

If a computer on the approved installation list is running the Windows Event Viewer or any Security Manager console, ensure you close the Windows Event Viewer and the console before starting the managed computer scan. If these products are running during a managed computer scan, you may need to restart the computer before the Security Manager agent will start.

If the central computer logs an event with an event ID of `21116`, `21118`, or `21169`, you need to restart the computer. Monitor these events in the Control Center to verify correct agent installation.

To verify that Windows agents are online:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp Users group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Infrastructure Components**.
4. In the Navigation pane, click **Agents**.
5. In the Results window, check the **Agent Status** column. If the agent is working, the status is **Running**.

Note

After you deploy one or more new agents, you may not immediately see the new agents in the Agents view. Until the new agents receive configuration information from the central computer and respond, the agent computers do not belong to any computer group. The Agents view does not display computers that do not belong to at least one computer group.

To view newly deployed agents before Security Manager configures the agent computers, click **Ungrouped Computers** in the Navigation pane, instead of Agents.

Viewing Agents in a Configuration Group

From the **Agent Summary View** in the Agent Administrator, you can view the status of agents on all computers monitored by your configuration group. From this window, you can also perform maintenance and troubleshooting tasks to keep your agent environment in good working order.

Viewing All Agents in a Configuration Group

You can view information about all agents in a configuration group. The information available from the Agent Administrator includes:

- The domain of an agent computer
- Whether a computer has a managed, unmanaged, UNIX, or iSeries agent
- Whether a computer is authorized in the database
- Whether a computer has an agent installation or upgrade pending
- Whether a computer is a proxy agent or an agentless monitored computer

The Agent Administrator displays only the central computers and agents for the configuration group from which you run it.

To view agents managed by central computers:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Configuration Groups**.
4. Select the appropriate configuration group in the Results window.
5. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.

6. In the Agent Administrator window, click the Agent Summary tab.

7. Click **Agent Summary View** to see all monitored computers, arranged by their central computers. For more information about the fields on a window, see the Help.

Viewing the Computers Assigned to a Central Computer

The central computer finds computers that match the discovery rules, collects computer attributes older than 24 hours, places computers in or removes computers from computer groups, and installs an agent as appropriate.

To view the agents assigned to a central computer:

1. 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 "Understanding Requirements and Permissions" on page 24.

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

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

4. Click **Central Computers**.

5. In the right pane, click the central computer with agents you want to view.

6. On the Action menu, click **View Managed Computers**. For more information about the fields on a window, click **Help**.

Changing which Central Computer Manages an Agent

You can change the central computer to which a managed or unmanaged agent is assigned. You can specify any central computer in the same configuration group. For more information about the relationship between an agent and a central computer, see "Understanding Managed and Unmanaged Windows Agents" on page 191.

Note
If you reassign an agent to a central computer that uses a different service account, ensure the service account is a member of the local Administrators group on all agents it will manage.

You may want to assign a new central computer to an agent in the following circumstances:

- To remove the central computer from the configuration group. When you permanently stop using a central computer, assign a new central computer to the managed and unmanaged agents managed by that computer.
- To take a central computer offline temporarily.
- To reassign agents to different central computers to balance the agent load. No central computer should manage too many agents. Monitor central computer performance to determine whether you need to rebalance the agent load.

To change the central computer to which an agent is assigned:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Configuration Groups**.
4. Select the appropriate configuration group in the Results window.
5. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.
6. In the left pane, click **Agent Summary**.

7. In the right pane, click **Agent Summary View**.
8. Select an agent you want to reassign to another central computer.
9. Click **Reassign**.
10. Select a different central computer, and then click **OK**. For more information about the fields on a window, see the Help.
11. Click **Yes** to confirm the change.
12. Click **Apply**.
13. Click **Close**.
14. Select **Apply configuration changes now**.
15. Click **OK**.
16. Verify the selected central computer and click **OK**.
17. Click **Close**.

Changing the Name or Domain of a Monitored Computer

If you change the name of the domain in which a monitored computer is located, move the computer to a different domain, or want the agent to monitor a different computer, update the agent using the Agent Administrator. If you are changing the domain of an agent computer, perform this task after you change the domain of the computer.

To change the name or domain of a monitored computer:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Configuration Groups**.
4. Select the appropriate configuration group in the Results window.

5. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.
6. In the Agent Administrator window, click the Agent Summary tab.
7. Click **Agent Summary View**.
8. Select the agent you want to associate with a different domain.
9. Click **Change**. For more information about the fields on a window, see the Help.
10. ***If you want to change which computer the agent monitors,*** complete the following steps:
    a. Select **Computer**.
    b. In the **New Computer** field, type the name of the computer you want the agent to monitor and click **OK**.
11. ***If you want to update the domain to which a monitored computer belongs,*** complete the following steps:
    a. Select **Domain**.
    b. Select the domain to which the monitored computer now belongs, and then click **OK**.
12. Click **Apply**.

Disabling Communication from Computers

Instances may occur in which you want to disable communication from an agent without uninstalling the agent software or removing the agent from the Security Manager database. For example, if an agent begins to send garbled data, you may want to prevent the agent from communicating with the central computer until you resolve the problem with the agent.

Note

If you plan to keep the agent in an unauthorized state for an extended period of time, stop the `NetIQ Security Manager` service on the agent computer. If the service is not stopped, the agent will continue evaluating rules and attempting to contact the central computer.

By default, each agent is authorized to communicate with the central computer. The following procedure suspends this authorization.

To disable communication from an agent:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Configuration Groups**.
4. Select the appropriate configuration group in the Results window.
5. In the Navigation pane, expand **Infrastructure Components > Agents**.
6. In the Results window, click the agent you want to stop monitoring.
7. On the Tasks menu, click **Agent Tasks > Unauthorize**.

Ignoring Agent Status

Agents notify the central computer of their status by sending a periodic heartbeat message to the central computer. If the agent does not send a heartbeat for any reason, the central computer begins to calculate the time the agent is out of contact. After a certain period of time has passed, as determined by a global setting in Security Manager, the agent is considered to be offline. Security Manager ignores the agent.

The following procedure determines how the central computer responds if the "lost" agent reestablishes communication.

To ignore the status of a Windows agent:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Infrastructure Components**.
4. In the Navigation pane, click **Agents**.
5. In the Results window, click the agent computer whose status you want to change.
6. ***If you want to ignore the status even if the agent reconnects,*** click **Agent Tasks > Ignore Agent Status Forever** on the Tasks menu.
7. ***If you want to ignore the status until the agent reconnects,*** click **Agent Tasks > Ignore Status until Agent Reconnects** on the Tasks menu. When the agent computer reconnects to the network, the Control Center will stop ignoring the status of the agent.
8. ***If you want to stop ignoring agent status,*** click **Agent Tasks > Stop Ignoring Agent Status** on the Tasks menu.

Viewing Hidden Computers

When you uninstall an agent from a Windows computer, Security Manager automatically hides that computer from some views. You can still view any collected events or alerts for the computer in views or Forensic Analysis reports. The events or alerts are available until Security Manager grooms them from the OnePoint and log archives.

Security Manager automatically hides the computer from the Agent Administrator and from the following views:

- Computer Group View
- Computer View
- Attribute View
- Agent Summary View in Agent Administrator

You can also show hidden computers if at a later date you want to view old agent information about them. However, showing a hidden computer does not cause Security Manager to resume monitoring that computer.

To view hidden computers:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Computer Views**.
4. On the Tasks menu, click **Computer Tasks > Show Hidden Computers**.
5. ***If you want to display specific hidden computers,*** select the hidden computer or computers you want to display and click **OK**.
6. ***If you want to display all hidden computers,*** select **Select all** and click **OK**.

7. ***If you want to hide a computer after reviewing the displayed computer information,*** complete the following steps:

    a. In the Results window, click the computer you want to hide.

    b. On the Tasks menu, click **Computer Tasks > Hide Computer**.

8. Close the Control Center.

Uninstalling Windows Agents

You may decide that an agent already installed on a computer is not required.

To uninstall agents from Windows computers, you can use one of the following procedures:

- Uninstalling Managed Windows Agents Using the Agent Administrator
- Uninstalling Managed Windows Agents Using the Control Center
- Uninstalling Unmanaged Windows Agents from All Configuration Groups

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

Notes

- A central computer cannot uninstall manually installed unmanaged Windows agents. For more information about uninstalling manually installed Windows agents, see the *Installation Guide for NetIQ Security Manager.*
- If you want to uninstall an agent, ensure you close all Microsoft Management Consoles and snap-ins, including Event Viewer, on the agent computer before uninstalling.

Uninstalling Managed Windows Agents Using the Agent Administrator

The following procedure uninstalls agent software from a managed computer.

To uninstall a Windows agent using the Agent Administrator:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Configuration Groups**.
4. Select the appropriate configuration group in the Results window.
5. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.
6. In the Agent Administrator window, click the Agent Summary tab.
7. Click **Agent Summary View**.
8. Select the row of the computer you want to uninstall.
9. Click **Uninstall**.
10. Select when you want to uninstall the managed agent:
    - To uninstall the agent immediately, click **Uninstall Now**.
    - To uninstall the agent at the next managed computer scan, click **Pending**.

Note
By default, Security Manager automatically approves pending agent uninstallation procedures. If you changed this Global setting, clicking **Pending** places the agent uninstall procedure in the Pending Agent Installations list until you approve it.

11. Click **Finish**.

12. ***If you are uninstalling a proxy agent that monitors an agentless monitored computer***, Security Manager stops monitoring the agentless monitored computer but does not hide it from views. If you want to hide it, use the Agent Summary view in the Agent Administrator. If you want to assign another proxy agent to monitor the agentless monitored computer, run the Agentless Monitored Computers wizard in the Agent Administrator.

Uninstalling Managed Windows Agents with the Control Center

You can uninstall agents using the Agents view in the Control Center. This process does not require you to know the central computer that manages the agent.

Uninstalling an agent using the Agents view places the agent in the Pending Agents Uninstallation list. The central computer waits until the next managed computer scan before uninstalling the agents unless you configure the central computer properties to wait for your approval. You can manually run a managed computer scan in the Development Console to uninstall all agents in the Pending Agents Uninstallation list.

To uninstall a Windows agent using the Control Center:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

3. In the Navigation pane, click **Infrastructure Components**.

4. In the Navigation pane, click **Agents**.

5. In the Results window, click the agent you want to uninstall.

6. On the Tasks menu, click **Agent Tasks > Uninstall Agent**.

7. Verify that you want to uninstall the listed agent and click **OK** to confirm.

8. ***If you want to uninstall the agent immediately,*** complete the following steps:

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

   b. In the left pane, expand **Security Manager Development Console > Configuration > Central Computers**.

   c. In the right pane, click the central computer for the agent you want to uninstall.

   d. On the Action menu, click **Scan Managed Computers Now**.

9. In the Control Center, click **Refresh** on the View menu.

Uninstalling Unmanaged Windows Agents from All Configuration Groups

When you no longer want to monitor an unmanaged agent computer, uninstall the unmanaged agent with the Add or Remove Programs utility.

The following procedure uninstalls an unmanaged Windows agent for all configuration groups.

Warning
If multiple configuration groups monitor an agent and you uninstall the agent, the agent will no longer be available to the other configuration groups. To keep the agent available to other configuration groups, remove the configuration group you no longer want to monitor the computer. Do not uninstall the agent software.

For more information about uninstalling agents, see the *Installation Guide for NetIQ Security Manager.*

To uninstall an unmanaged agent:

1. Log on to an unmanaged agent computer as a local administrator.
2. Close all open applications.
3. Run **Add or Remove Programs** from the Control Panel.

4. Select **NetIQ Security Manager Agent**.
5. Click **Remove**.
6. Click **Yes**.
7. Follow the instructions until the unmanaged agent is removed.
8. Close the Add or Remove Programs window.
9. Log off of the unmanaged agent computer.
10. Log on to a central computer that monitors the unmanaged agent as a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
11. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
12. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.
13. In the left pane, click **Agent Summary**.
14. In the right pane, click **Agent Summary View**.
15. Select the unmanaged agent you want to remove.
16. Click **Uninstall > Pending**.
17. Click **Yes**.
18. Click **Apply**.
19. Click **Close**.
20. Select **Apply configuration changes now**.
21. Click **OK**.
22. Verify the selected central computer and click **OK**.
23. In the left pane, click **Managed Agents**.
24. In the right pane, click **Manage Pending Actions**.

25. Select **Approved** for the unmanaged agent you want to remove.
26. Click **Finish**.
27. In the left pane, click Agent Summary.
28. In the right pane, click Agent Summary View.
29. Select Show Hidden Computers.
30. Select the removed unmanaged agent.
31. Click **Delete**.
32. Click **Yes**.
33. Click **Close**.
34. Select **Apply configuration changes now**.
35. Click **OK**.
36. Verify the selected central computer and click **OK**.
37. Click **Close**.

Configuring Agent Deployment for IDS or Firewall Devices, Routers, and Switches

Security Manager can monitor numerous platforms and devices using various agents. For more information about monitoring particular endpoints using agents, see the module documentation for products you want to monitor.

Configuring iSeries Agent Deployment

Security Manager can monitor iSeries servers using an iSeries agent and can monitor, analyze, and consolidate events from log files on monitored iSeries servers in real-time. When significant events occur, Security Manager can raise alerts in the Security Manager consoles and can email or page your staff so they can quickly respond.

Security Manager also consolidates the events to secure repositories that provide centralized access, which is critical for meeting audit requirements. For more information about installing and configuring iSeries agents, see the NetIQ Security Solutions for iSeries documentation and the Security Manager for iSeries module documentation.

Configuring UNIX Agent Deployment

Security Manager can monitor UNIX computers using a UNIX agent. For more information about deploying and configuring UNIX agents, see the NetIQ UNIX Agent documentation. For more information about configuring the UNIX agent for Security Manager, see the NetIQ UNIX Agent documentation and the Security Manager for UNIX module documentation.

Chapter 8

Configuring Security Manager

You typically deploy agents and configure Security Manager immediately after installation. However, sometimes you must reconfigure Security Manager to add or remove operators to receive notifications or to maintain or fine-tune your Security Manager implementation. This chapter covers configuration tasks and customization tasks to refine Security Manager for your environment. For more information about the initial configuration of Security Manager, see the *Installation Guide for NetIQ Security Manager*.

This chapter does not cover configuration tasks relating to agents, such as adding and deleting agents or modifying their properties. For more information about configuring agents, see “Administering Agents” on page 191.

You can also customize Security Manager by modifying existing rules or creating new rules specially suited for your environment. For more information about modifying or creating rules, see “Customizing Rules” on page 233.

Synchronizing Device Times

Security Manager provides information about detected events, including the time the event occurred. This event information is dependent on the date and time properties of the computer where the event originates.

Security Manager also correlates events based on the time the event occurred. The Correlation server rearranges queued events to process the events using the order in which they occurred, not the order in which they arrived at the Correlation server. This rearrangement allows Security Manager to correlate events in a timely fashion despite network lag. Security Manager also disregards “old” events, which are determined by Correlation settings.

To ensure Security Manager displays the correct time for detected events and correlates events in a timely fashion, periodically synchronize the time properties for all computers and devices across your network.

If you observe Daylight Saving Time, ensure you also adjust all computers and devices in the affected time zones at the appropriate time.

Using the Configuration Wizard

You can customize Security Manager using the Configuration Wizard. The Configuration Wizard is accessible from the Control Center and from the Alert Sentry in the system tray.

Typically, you use this wizard immediately after installation and agent deployment to learn important configuration information and to customize rule and script parameters. Customizing rule and script parameters enables Security Manager to process events, alerts, and responses.

You can also run the Configuration Wizard at any time to reconfigure these parameters. Using the Control Center, you can use the Configuration Wizard to configure parameters on any connected configuration group.

To start the Configuration Wizard:

1. Log on to the Control Center computer with an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

3. In the Navigation pane, click **Configuration Groups**.
4. Select the configuration group you want to configure in the Results window.
5. On the Tasks menu, click **Global Tasks > Launch Configuration Wizard**.
6. Follow the instructions in the windows until you have finished customizing Security Manager. For more information about fields on a window, see the Help.

Customizing Rules

Processing rules enable Security Manager to process events, alerts, and responses. You can review configuration information for processing rules using the Development Console.

Use the Development Console to customize processing rules that contain the word `Customize`. While you can customize any processing rule, Security Manager users frequently customize these particular rules, and you may need to customize the rules for your own use. Use the Development Console to perform a search for these rules, and then read each rule's knowledge base for configuration instructions.

To review configuration information for rules you should customize:

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 "Understanding Requirements and Permissions" on page 24.
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. On the Action menu, click **Find Processing Rules**.
5. Click **All processing rule groups**.
6. Click **Next**.

7. Select **Rule name**, select **contains substring** from the list, and then type `Customize` in the blank field. For more information about the fields on a window, click **Help**.
8. Click **Next**.
9. Click **Finish**.
10. Double-click a rule in the results window.
11. Click the Knowledge Base tab.
12. Examine the knowledge base for each rule matching the search criteria, and decide if you need to customize it for your environment.
13. Follow the instructions in the knowledge base to customize the rule as indicated.

Configuring Notification Groups

Security Manager supports SMTP for email and paging notification. Ensure you have included operators in the appropriate notification groups to receive notifications. Using the Development Console, you can add to or customize existing notification groups or create your own custom notification groups.

Built-in Notification Groups

Security Manager uses notification groups to control email and paging notification recipients. Security Manager provides built-in notification groups configured to notify operators when specific alerts occur. Add operators to these notification groups to receive notifications.

Security Manager provides the following default notification groups:

Network Administrators

Responsible for maintaining monitored networks. Security Manager notifies operators in this notification group when alerts of severity level Error or worse occur for Security Manager self-monitored components.

Security Manager Administrators

Responsible for monitoring and maintaining Security Manager itself. Security Manager notifies operators in this notification group when the Security Manager product experiences various kinds of issues that can affect the product's ability to monitor the environment. NetIQ recommends that all administrators be members of this group.

Adding Operators to a Notification Group

To enable Security Manager to notify key personnel when an alert occurs, you must first add operators to appropriate notification groups.

To add operators 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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration > Notification Groups**.
4. Click the notification group to which you would like to add operators.
5. On the Action menu, click **Properties**.
6. ***If you have not previously created the operator***, complete the following steps:

   a. Click **New Operator**.

   b. Type a name for the operator.

   c. Click **Next**.

   d. ***If you would like to notify this operator by email,*** type the operator email address and specify the schedule during which Security Manager can send messages to the operator, and then click **Next**. For more information about the fields on a window, click **Help**.

e. ***If you would like to notify this operator by page***, type the operator email address for the pager and specify the schedule during which Security Manager can send messages to the operator. For more information about the fields on a window, click **Help**.

f. ***If you would like to notify this operator using a third-party paging application***, type the operator ID and specify the schedule during which Security Manager can send messages to the operator. For more information about the fields on a window, click **Help**.

g. Click **Finish**.

7. Select the operator name from the **Available operators** list.
8. Click the right arrow to move the operator to the **Group operators** list.
9. Click **OK**.

Modifying an Operator

You can change the properties of a notification group operator, including the email, page, and command notification options. An operator can belong to more than one notification group. You can view the operators in a notification group in the Operator Name column.

To modify operator 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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration > Notification Groups**.
4. Click a notification group to which the operator belongs.
5. In the right pane, click the operator you want to modify.

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

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

Deleting an Operator From a Notification Group

You can remove an operator from only one notification group, or delete the operator record to remove the operator from all notification groups.

To delete or remove an operator:

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 “Understanding Requirements and Permissions” on page 24.

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

3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration > Notification Groups**.

4. Click the notification group from which you want to delete an operator.

5. In the right pane, click the operator you want to delete.

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

7. ***If you want to remove the operator only from the selected notification group,*** click **Remove this operator from the current notification group**. This option removes the operator from the current notification group, but does not delete the operator record.

8. ***If you want to delete the operator from all notification groups,*** click **Delete operator**. This option removes the operator from all notification groups and deletes the operator record.

9. Click **OK**.

Creating Notification Groups

When you configure Security Manager to send a notification response, you must specify a notification group to receive it. You can use built-in notification groups or create new notification groups to receive notifications. Creating new notification groups provides more options for organizing operators. Creating new notification groups also ensures new notification groups associated with new processing rules in custom Security Manager environments are not altered or lost during product upgrades.

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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration**.
4. Click **Notification Groups**.
5. On the Action menu, click **Create Notification Group**.
6. Type an appropriate name for the notification group.
7. ***If you want to add an existing operator to the group,*** complete the following steps:
    a. Select the operator name from the **Available operators** list.
    b. Click the right arrow to move the name to the **Group operators** list.
8. ***If you want to create a new operator and add the operator to the group,*** complete the following steps:
    a. Click **New Operator**.
    b. Type a name or description of the operator.
    c. Follow the instructions until you have finished creating an operator. For more information about the fields on a window, click **Help**.
    d. Click the right arrow to move the name to the **Group operators** list.

9. ***If you want to modify an operator's properties,*** complete the following steps:

    a. Select the operator name. The operator can be in the **Available operators** list or the **Group operators** list.

    b. Click Properties.

    c. Modify the operator properties as needed. For more information about the fields on a window, click **Help**.

10. Repeat Step **7** or Step **8** to add more operators to the notification group.

11. Click **Finish** on the Notification Group Properties window.

Modifying Configuration Group Passwords

Multiple central computers in a configuration group share configuration data. The configuration data is encrypted and resides in the database server. To enable computers to access the shared configuration data, each central computer must have access to a shared encryption key.

Each configuration group has a password, supplied during setup, to allow access to the shared encryption key. Each central computer in the configuration group shares the password. At any time after installing the configuration group, you can change the password.

To change the configuration group password:

1. Log on to a central computer as a member of the OnePointOp ConfgAdms group and the local Administrators group.
2. Start **Configuration Group Password** in the NetIQ Security Manager program group.
3. Click **Yes**.
4. Type the current password and the new password. For more information about the fields on a window, see the Help.

5. Click **Change Password**.

6. Repeat Steps **1** through **5** on every central computer in the configuration group.

Managing Custom Tasks

In the Control Center, you can create custom tasks to use within views. You can define custom tasks that are available only to you or are available to all users. To create a custom task only you can use, your user account must be a member of the OnePointOp Users group. To create a global task all users can access, your user account must be a member of the OnePointOp Operators group. For more information about groups, see "Understanding Requirements and Permissions" on page 24.

Custom tasks can send information about a Results window item to another application. These custom tasks can include applications, commands, or batch files. You create custom tasks for specific view objects, including events, alerts, attribute values, and computers.

Notes

- Security Manager provides several preconfigured custom tasks in the Control Center that you can use on monitored computers, including tasks to ping the specified computer, stop the Security Manager service on the specified computer, or create a remote desktop connection to the specified computer.
- You can only run a custom task for which your user account has sufficient permissions on the computer on which you want to run the task. For example, if you use an account that is a member of the OnePointOp Operators group but is not a member of the local Administrators group, you cannot run custom tasks that require Administrator access.

Creating Custom Tasks

You can create a custom task for any task that you can run from the command-line interface, using variables to include Security Manager data for specified events, alerts, computers, or attributes. For example, you can create a simple custom task that pings a selected computer by specifying the following command in the Custom Tasks window:

```
ping $Computer$
```

In this case, the `ping` command opens a command-line interface window, and `$Computer$` specifies the column in the Control Center as the single parameter of the command.

The custom task becomes available on the Tasks menu when you select a computer in a computer view. If you select the computer `TEST001` in the Results window and run this custom task, Security Manager pings that computer to test its connectivity.

You can also create more complex custom tasks, using more advanced commands. For example, you can create a task that sends alert information to a third-party problem ticket application. The custom task becomes available on the Tasks menu when you select an alert in an alert view.

You could create a task that uses the NetIQ Directory and Resource Administrator product to control a service on a computer. When you select the computer in a computer view, the task becomes available on the Tasks menu. For an example of a specific custom task created in the Control Center, see “Scanning a Single Windows Computer Using the Custom Task” on page 206.

To create a custom task:

1. ***If you want to create a custom task available to all users,*** log on to the Control Center computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. ***If you want to create a custom task available only to you,*** log on to the Control Center computer using an account that is a member of the OnePointOp Users group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
3. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
4. In the Navigation pane, click **All Folders**.
5. On the Tasks menu, click **Global Tasks > Manage Custom Tasks**.
6. ***If you want to create a custom task available to all users,*** select `all users` from the **Task available to** list.

7. ***If you want to create a custom task available only to you,*** select *`Domain`\`User`* from the **Task available to** list, where *`Domain`* is the name of the domain to which your user account belongs and *`User`* is the name of your user account.

8. ***If you want to create a custom task for an event view,*** select `event items` from the **Task available for** list.

9. ***If you want to create a custom task for an alert view,*** select `alert items` from the **Task available for** list.

10. ***If you want to create a custom task for an attribute view,*** select `attribute items` from the **Task available for** list.

11. ***If you want to create a custom task for an computer view,*** select `computer items` from the **Task available for** list.

12. Click **Add**.

13. Specify a name and description for the custom task. You can specify a custom task name with a maximum of 50 characters.

14. Specify the command you want the custom task to run, selecting variables from the **Command** list as necessary. For more information about the fields on a window, click **Help**.

15. Click **OK**.

16. Click **OK** to exit the Custom Tasks window.

Running Custom Tasks

Once you create a custom task, you can run that task on a specific Results window item in the Control Center. You can only run a task on the item type for which it was created. For example, if you create a custom task for an alert view, you cannot run that task on an item in a computer view.

If you can run a custom task in a particular view, Security Manager displays the task on the Tasks menu or in the Tasks pane under Custom Tasks. You can only run custom task that are available to all users or that you create yourself. For more information about creating custom tasks, see “Creating Custom Tasks” on page 240.

To run a custom task:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp Users group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**, and then expand the subfolders until you reach the view where you want to run the custom task.
4. Click the view.
5. In the Results window, click the appropriate item.
6. On the Tasks menu, click **Custom Tasks >** ***Task***, where ***Task*** is the name of the custom task.

Modifying or Deleting Custom Tasks

In the Control Center, you can modify or delete custom tasks you create. In addition, if your user account is a member of the OnePointOp Operators group, you can modify or delete global tasks that all users can access. For more information about groups, see "Understanding Requirements and Permissions" on page 24.

To modify or delete a custom task:

1. ***If you want to modify or delete a custom task available to all users,*** log on to the Control Center computer using an account that is a member of the OnePointOp Operators group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. ***If you want to modify or delete a custom task available only to you,*** log on to the Control Center computer using an account that is a member of the OnePointOp Users group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
3. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

4. In the Navigation pane, click **All Folders**.
5. On the Tasks menu, click **Global Tasks > Manage Custom Tasks**.
6. ***If you want to modify or delete a custom task available to all users,*** select `all users` from the **Task available to** list.
7. ***If you want to modify or delete a custom task available only to you,*** select *`Domain`*`\`*`User`* from the **Task available to** list, where *`Domain`* is the name of the domain to which your user account belongs and *`User`* is the name of your user account.
8. Select the appropriate view type from the **Task available for** list.
9. Click the task you want to modify or delete in the **Current available tasks** list.
10. ***If you want to modify a task,*** complete the following steps:
    a. Click **Modify**.
    b. Modify existing task information as necessary.
    c. Click **OK**.
11. ***If you want to delete a task,*** complete the following steps:
    a. Click **Delete**.
    b. Click **Yes** to confirm.
12. Click **OK** to close the Custom Tasks window.

Restricting Information in Security Manager

You have two options for restricting access to information in Security Manager:

- You can use Security Manager's built-in security filtering to restrict access to Windows groups.
- You can use OnePointOp groups to limit access to views, reports, and user interfaces.

Restricting Information Using Security Filtering

You can restrict information using the security filtering feature. Security filtering allows you to limit which computers a Windows group has access to see or modify. For more information about security filtering, see the *Installation Guide for NetIQ Security Manager*.

Restricting Information Using OnePointOp Groups

Security Manager uses groups to provide or restrict user access to Security Manager functionality in the Control Center. By adding a user to a group, you grant that user access to the Security Manager functionality associated with that group.

For example, you might want a user to monitor all alerts occurring in the configuration group. You do not want this user to be able to configure Security Manager. If you add this user to the OnePointOp Users group, the user can monitor and respond to alerts in the Control Center, but cannot change the Configuration Groups settings in any way. For more information about OnePointOp groups, see “Understanding Requirements and Permissions” on page 24.

Customizing the Security Manager Interfaces

You can customize the Control Center or Development Console to display or hide certain items, such as toolbars or menus. You can also customize the layout of the Control Center and configure the Control Center to connect to a different central computer.

Connecting to a Different Central Computer

When you first open the Control Center on a user interface-only computer, Security Manager prompts you to select a central computer for the configuration group you want to monitor. The Control Center uses this central computer to access alert and event information.

Using the Control Center, you can also specify a different central computer to monitor.

To connect to a different central computer:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Click **Configuration Groups**.
4. On the Tasks menu, click **Configuration Group Tasks > Connect to Central Computer**.
5. Type the name of the central computer you want to connect to in the **Central computer name** field. For more information about the fields on a window, see the Help.
6. ***If you want to connect using a different account,*** click **Log on as** and specify the appropriate account information.
7. ***If you want to connect using a different port,*** click **Options** and specify a port number.
8. ***If you want Security Manager to always prompt you for the central computer name,*** select **Always display at startup**.
9. Click **OK**.
10. Close and reopen the Control Center.

Customizing the Control Center Today Page

You can configure the content that appears on the Control Center Today Page. You can customize your Today Page to display any alert view available in the Control Center in either an Alert State Chart or Alert Severity Chart.

Changes you make to the layout of your Today Page are saved in the SecurityManagerCommon database. Your personal Today Page can then be accessed from any Control Center in the same configuration group.

Creating a Chart

You can create up to 20 charts on the page, organized in up to four rows of five charts each. However, a large number of charts on a page may make it difficult to view the data displayed.

To add a chart to an existing row:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.
4. Click **Security Manager Control Center**.
5. On the Tasks menu, click **Today Page > Configuration**.
6. Select the row to which you want to add a chart.
7. Click **Add Chart** and select the appropriate chart type.
8. In the chart list, click **View Name** and select the alert view for which you want to display data. For more information about fields on a window, see the Help.
9. Click **Finish**.

Creating a Row

You can create new rows in the Today Page layout, each displaying up to five charts. Note that a large number of rows on a page may make it difficult to view the data displayed.

To add a row to the Today Page:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.
4. Click **Security Manager Control Center**.
5. On the Tasks menu, click **Today Page > Configuration**.
6. Click **Add Row**.
7. Click **Finish**.

The new row displays below any existing rows. You can then add charts to the new row. For more information about creating charts on the Today Page, see “Creating a Chart” on page 247.

Removing a Chart

If you no longer want to view a chart on your Today Page, you can remove the chart from the layout.

Note
If you remove a chart, it is removed permanently from the Control Center.

To remove a chart from a row:

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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.

4. Click **Security Manager Control Center**.

5. On the Tasks menu, click **Today Page > Configuration**.

6. Select the row from which you want to remove a chart.

7. Select the chart you want to remove.

8. Click **Remove Chart,** then click **OK** on the confirmation window.

9. Click **Finish**.

Removing a Row

If you no longer want to view a particular row on your Today Page, you can remove the row from the layout.

Note

If you remove a row from the Today Page, any charts on the row are also removed. Rows and charts are permanently removed from the Control Center.

To remove a row from the Today Page:

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 "Understanding Requirements and Permissions" on page 24.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

3. In the Navigation pane, click **All Folders**.

4. Click **Security Manager Control Center**.

5. On the Tasks menu, click **Today Page > Configuration**.

6. Select the row you want to remove.

7. Click **Remove Row,** then click **OK** on the confirmation window.

8. Click **Finish**.

Hiding the Chart Toolbar

If you do not want to be able to access the chart toolbar from the Today Page, click **Show/hide chart toolbar**. You can click the icon at any time to bring back the toolbar.

Customizing Chart Appearance

The Control Center also allows you to customize the appearance of any chart on the Today Page, using the chart toolbar available in the Today Page preview window.

To customize chart appearance using the chart toolbar:

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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.
4. Click **Security Manager Control Center**.
5. Click the Overview tab on the chart you want to customize.
6. ***If the chart toolbar does not display,*** click **Show/hide chart toolbar**.
7. Customize the chart as follows using the toolbar:
   - To change the layout, click **Select Chart Type** and select the chart layout you want to use.
   - To change the color scheme, click **Select Color Palette** and select the color scheme you want to use.
   - To turn the legend on and off, click **Toggle Chart Legend**.
   - To turn three-dimensional rendering on and off, click **Toggle 3D View**.
   - To insert an annotation into a chart, click **Add Annotation**.

8. ***If you want to expand a chart or restore a chart to its original size,*** click **Maximize/Restore this chart** on the main chart window.

9. ***If you want to switch between percentages and numerical values,*** click **Toggle Percent/Count** on the main chart window.

You can click **Properties** in the toolbar to view detailed settings for the chart. This window allows you to further customize the appearance and layout of the chart.

Customizing Columns

Security Manager allows you to customize views by adding or removing columns.

Customizing Columns in the Control Center

In the Control Center, you can show or hide columns as necessary using the column chooser, drag and drop columns to reorganize the view, and group or sort columns to filter the alert or event data displayed.

Note
You can only customize columns permanently in your own custom Control Center views. If you customize columns in a default Control Center view, the columns revert to their default layout the next time you open the Control Center.

To add or remove columns:

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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.
4. Expand the folders and select the view you want to modify.

5. ***If you want to add a column to the view,*** complete the following steps:

   a. On the view window, right-click the column headers and select **Column Chooser**.

   b. Click the column you want to add.

   c. Drag-and-drop the column on the column headers area.

6. ***If you want to remove a column from the view,*** complete the following steps:

   a. Click the column you want to remove.

   b. Drag the column away from the column headers area, until you see an X displayed under your cursor.

   c. Drop the column.

7. ***If you want to change the order in which the columns are displayed,*** complete the following steps:

   a. Click the column you want to move.

   b. Drag-and-drop the column to the location in the column headers area where you want it displayed.

8. ***If you want to group alerts or events by a particular column,*** drag-and-drop the column to the **Drag a column header here to group by that column** area.

Customizing Columns in the Development Console

You can customize the right pane display in the Development Console by adding and removing columns and changing their order. Changes you make are saved in the `.MSC` file and are available only within the console in which you made the changes.

To add or remove columns:

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 "Understanding Requirements and Permissions" on page 24.

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

3. In the left pane, expand **Security Manager Development Console** and any subfolders until you expand the folder that contains the view you want to modify.
4. In the left pane, click the view you want to modify.
5. On the View menu, click **Add/Remove Columns**.
6. ***If you want to add a column to the right pane,*** complete the following steps:
   a. Click the column name in the **Available columns** field.
   b. Click **Add**.
7. ***If you want to remove a column from the right pane,*** complete the following steps:
   a. Click the column name in the **Displayed columns** field.
   b. Click **Remove**.
8. ***If you want to change the order in which the columns are displayed,*** complete the following steps:
   a. Click a column name in the **Displayed columns** field. This column will change location in the right pane.
   b. Click **Move Up** or **Move Down**.
9. ***If you want to return the right pane to its default column settings,*** click **Restore Defaults**.
10. Click **OK**.

Creating a Favorites Folder

You collect views and reports in the My Favorites folder. You can also create favorites folders to allow you to organize collections of views and reports.

Security Manager saves favorites folders in the SecurityManagerCommon database. You can access your favorites folders each time you open the Control Center.

To create a favorites folder:

1. Log on to the Control Center computer as a member of the OnePointOp Users group.
2. Start the **Security Manager Control Center** from the NetIQ Security Manager program group.
3. In the Navigation pane, click **My Favorites**.
4. On the Tasks menu, click **Favorites Tasks > Create favorites folder**.
5. Specify a name and description for the folder. For more information about fields on a window, see the Help.
6. Click **OK**.

Adding Views and Reports to Favorites Folders

In the Control Center you can save a collection of the Security Manager views and reports you use most often. You can add the following views and reports to a favorites folder:

- Incident packages
- Alert views
- Event views
- Computer views
- Computer group views
- Attribute views
- Infrastructure Components views
- Forensic Analysis reports
- Trend Analysis reports
- Configuration Groups view

Security Manager saves these favorites in the SecurityManagerCommon database. You can access your favorites each time you open the Control Center.

To add views and reports to a favorites folder:

1. Log on to the Control Center computer as a member of the appropriate OnePointOp group for the object you want to add. To add views your account must be a member of the OnePointOp Users group. To add reports, your account must be a member of the OnePointOp Reporting group.
2. Start the **Security Manager Control Center** from the NetIQ Security Manager program group.
3. In the Navigation pane, click **My Favorites**.
4. Expand your favorites folders and select the folder to which you want to add the object.
5. On the Tasks menu, click **Favorites Tasks > Add to favorites folder**.
6. Complete the fields in the window. For more information about fields on a window, see the Help.
7. Click **OK**.

Finding Objects to Add to Favorites Folders

You can also search for specific objects to add to your favorites folders by using a combination of type, name, and description criteria. If you select more than one criteria, only objects matching all criteria are returned.

For example, if you want to find all event views in your favorites that have to do with antivirus software updates, select **Type > Event View** and type `antivirus` in the **Name Contains** field and `update` in the **Description Contains** field. Any event view containing both the word “antivirus” in its name and “update” in its description displays in the search results.

To find objects to add to your favorites folders:

1. Log on to the Control Center computer as a member of the OnePointOp Users group or OnePointOp Reporting group.
2. Start the **Security Manager Control Center** from the NetIQ Security Manager program group.
3. In the Navigation pane, click **My Favorites**.
4. On the Tasks menu, click **Favorites Tasks > Find objects to add**.
5. On the Favorites Folder Name list, select the favorites folder to which you want to add objects.
6. ***If you want to find objects by type,*** select **Type** and then select the appropriate type from the list.
7. ***If you want to find objects by name,*** select **Name Contains** and type all or part of the name you want to search for in the text box.
8. ***If you want to find objects by description,*** select **Description Contains** and type all or part of the description you want to search for in the text box.
9. ***If you want to narrow your search,*** select any combination of **Type**, **Name Contains**, and **Description Contains** and specify search criteria as directed in Steps **5** through through **7**.
10. Click **Find Now**.
11. Select the objects you want to add and click **OK**.

Monitoring Multiple Configuration Groups

The Control Center allows you to monitor real-time data for multiple configuration groups using the same view. The first time you open the Control Center, you must specify the central computer for the configuration group you want to monitor. You can also monitor additional configuration groups by adding configuration group connections to the central computer that is connected to the Control Center.

Data from additional monitored configuration groups is displayed in alert views. The Configuration Group column specifies the name of the configuration group containing the computer that generated the alert.

For reporting on additional configuration groups using the Control Center, you must select the configuration group on which you want to report. Once you select a configuration group, you can then run Forensic Analysis queries or Trend Analysis reports on that configuration group just as you would on your primary configuration group. You can also use the Configuration Wizard and Agent Administrator to configure parameters or manage agents on a connected configuration group.

To monitor an additional configuration group, the service account used to connect must be a member of the OnePointOp TrustedServiceAccounts group and the local Administrators group on the central computer in the remote configuration group.

Note
Do not add your local service account to the OnePointOp TrustedServiceAccounts group on your local central computer. Only add local service accounts to the OnePointOp TrustedServiceAccounts group on the remote central computer.

In addition, your user account must be a member of the OnePointOp ConfgAdms group on both the local and remote configuration group central computers. If the account used to connect to the configuration group does not have the required permissions, you cannot monitor data in the configuration group.

Your user account must also be a member of the same OnePointOp groups in both the local and remotely connected configuration groups to access user interface features in the remotely connected configuration group. For example, to access Forensic Analysis reports for the remote configuration group, your account must be a member of the OnePointOp Reporting group on your local central computer and on the remote configuration group central computer.

Creating a Configuration Group Connection

To use the Control Center to monitor an additional configuration group, create a connection to a central computer within the configuration group.

To connect to another configuration group:

1. Log on to the remote central computer and use the Active Directory Users and Computers Administrative Tool to add the service account to the OnePointOp TrustedServiceAccounts and Administrators groups. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. On the remote central computer, use the Access Configuration utility to add your user account to the OnePointOp ConfgAdms group and to any other appropriate OnePointOp groups.
3. Log on to your central computer connected to the Control Center with a user account that is a member of the OnePointOp ConfgAdms group.
4. Start the **Configuration Group Connections** utility in the NetIQ Security Manager > Configuration program group.
5. Click **Add**.
6. Specify the appropriate values on the Add Configuration Group Connection window. For more information about fields on a window, see the Help.
7. Click **OK**.
8. On the Configuration Group Connections window, click **OK**. Your changes take place in a few minutes.

Modifying Configuration Group Connection Settings

You can modify configuration group connection settings using the Control Center. For example, if you manage several configuration groups, you can temporarily discontinue monitoring certain configuration groups to limit alerts. You can also change your connection account settings or port number or adjust the alert refresh rate for each configuration group you monitor.

To modify configuration group settings:

1. Log on to the central computer with a user account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Configuration Group Connections** utility in the NetIQ Security Manager > Configuration program group.
3. Select the connected configuration group you want to modify.
4. Click **Modify**.
5. Specify the appropriate values on the Modify Configuration Group Settings window. For more information about fields on a window, see the Help.
6. Click **OK**.
7. On the Configuration Group Connections window, click **OK**. Your changes take place in a few minutes.

Removing Configuration Group Connections

If you no longer want to monitor a configuration group using the Control Center, you can disable or remove the connection to the other configuration group.

To remove a configuration group connection:

1. Log on to the central computer with a user account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Configuration Group Connections** utility in the NetIQ Security Manager > Configuration program group.
3. ***If you want to disable a configuration group connection,*** clear **Enabled** in the appropriate row of the Connections table.

4. ***If you want to remove a configuration group completely,*** complete the following steps:

    a. Click **Remove**.

    b. Click **OK**.

5. On the Configuration Group Connections window, click **OK**.

Viewing Configuration Group Connections Status

You can view the status of configuration group connections using the Control Center.

To view configuration group connection status:

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 “Understanding Requirements and Permissions” on page 24.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

3. In the Navigation pane, click **Configuration Groups**. The Configuration Groups window displays all connected configuration groups. You can review configuration group connection status in the Connected column.

Configuring Message Buffering

Security Manager uses persistent storage to protect against data loss, storing data locally on the agent level. Windows agents temporarily store data on the agent computer to safeguard against communication interruptions between the agent and the monitoring central computer. If a communication failure occurs, the agent stores any collected event or log data until the agent can re-establish a connection with the central computer and then sends all collected data.

Security Manager categorizes pending agent messages as normal priority, invalid, or high priority, with buffer disk space allocated for messages of each category. The following table lists the default buffer sizes for each message category:

Message Category Name	Default Buffer Size (in KB)
High Priority	10000
Normal Priority	1000000
Invalid	10000

Using the Development Console, you can configure temporary storage settings globally, for all agents, or for specific agents in a configuration group. You can increase or decrease the default message buffer sizes, as necessary.

A Windows agent that cannot communicate with a central computer stores data until one of the following events occurs:

- The agent can send the data.
- The stored data grow to the size of the configured message buffering settings.
- The stored data grow to fill the hard disk of the agent computer.

After the agent reaches either the agent's message buffering settings or the hard disk space limit of the computer, the agent stops processing collected data. Event data remains in the native event logs until the agent can begin processing again.

To configure temporary storage settings:

1. 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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration**.

4. ***If you want to configure global temporary storage settings,*** complete the following steps:

   a. Click **Global Settings**.

   b. On the Action menu, click **Edit Agent Settings**.

5. ***If you want to configure temporary storage settings for a specific agent computer,*** complete the following steps:

   a. Click **Central Computers**.

   b. In the right pane, select the central computer that monitors the agent you want to configure.

   c. On the Action menu, click **View Managed Computers**.

   d. Select the agent computer you want to configure and click **Settings**.

6. Click the Temporary Storage tab.

7. Specify the appropriate settings. For more information about the fields on a window, click **Help**.

8. Click **OK**.

Configuring Database Grooming

Security Manager provides scheduled grooming processes for the OnePoint database, LogManagerConfiguration database, and reporting cube in Microsoft SQL Server.

Grooming the OnePoint and LogManagerConfiguration Databases

The OnePoint and LogManagerConfiguration databases store real-time alerts, events, Forensic Analysis reports, and configuration data.

Security Manager provides grooming jobs to delete data from the OnePoint and LogManagerConfiguration databases. Some of the grooming jobs use the retention times and the number of records to delete specified in Global Settings in the Configuration snap-in.

Notes

- You cannot delete Forensic Analysis reports if they are part of an incident package.
- Security Manager also automatically grooms log archive data older than 90 days, by default. For more information about configuring log archive grooming settings, see "Grooming the Log Archives" on page 142.

For more information about modifying the default grooming settings, see "Modifying Database Grooming Settings" on page 263.

Modifying Database Grooming Settings

Using the Development Console, you can change the number of records deleted and the retention time for real-time events, alerts, performance data, completed Forensic Analysis reports, and some internal bookkeeping data stored in the OnePoint and LogManagerConfiguration databases. You can also set the retention time for automatic resolution of real-time alerts.

For example, if you set the retention time for `All real-time events` to `20 days` and to delete 8000 records, the `OnePoint - Groom Events` grooming job runs every hour, checking for data older than 20 days and deleting 8000 records older than 20 days.

The following table provides the default database grooming settings.

Records to Delete	Retention Time	Number of Records	Frequency
All real-time events	30 days	16000	1 hour
All sampled numeric data	90 days	4000	1 hour
Auto-resolve Critical Error alerts	30 days	N/A	N/A
Auto-resolve Error alerts	2 days	N/A	N/A

Records to Delete	Retention Time	Number of Records	Frequency
Auto-resolve Information alerts	4 hours	N/A	N/A
Auto-resolve Security Breach alerts	30 days	N/A	N/A
Auto-resolve Service Unavailable alerts	30 days	N/A	N/A
Auto-resolve Success alerts	4 hours	N/A	N/A
Auto-resolve Warning alerts	1 day	N/A	N/A
Completed Forensic Analysis reports	180 days	1000	6 hours
Groom Bookkeeping Entries on UNIX and iSeries Data Collection	30 days	100000	1 day
Real-time events without corresponding alerts	7 days	1000	1 hour
Resolved alerts	30 days	4000	1 hour

The default settings are adequate for most enterprise environments.

Notes

- You cannot groom alerts or events if they are part of an incident package.
- You can configure Security Manager to groom a maximum of `9999999` records at a time.
- You can specify a maximum of `9999` days to keep a record.
- If you specify a number of hours to keep a record, you must specify a value from `0` to `23`.
- If you specify a number of minutes to keep a record, you must specify a value from `0` to `59`.
- While Security Manager uses the grooming settings in the Development Console to groom resolved alerts out of the OnePoint database, you must configure log archive grooming separately. For more information about configuring log archive grooming settings, see “Grooming the Log Archives” on page 142.

To change database grooming settings:

1. 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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration**.
4. Click **Global Settings**.
5. In the right pane, click **Database Server Grooming**.
6. On the Action menu, click **Properties**.
7. Click a grooming setting, and click **Edit** to configure the setting parameters. For more information about the fields on a window, click **Help**.

8. Click **OK**.
9. Click **OK**.

Expanding Your OnePoint Database

If your OnePoint database needs to expand beyond the initial limits you specified for either the data file or the transaction log file, you can manually expand the database using Microsoft SQL Server Management Studio.

To expand your OnePoint database:

1. Log on to the database server using an account that has SQL Administrator privileges. For more information about SQL permissions, see the Microsoft SQL Server Help.
2. Start **SQL Server Management Studio**, located in either the Microsoft SQL Server 2005 or Microsoft SQL Server 2008 program group.
3. In the Connect to Server window, select **Database Engine** as the server type.
4. Click **Connect**.
5. Expand **Databases**.
6. Right-click **OnePoint** and select **Properties**.
7. Select the Files page.
8. Select the OnePoint database file you want to expand.
9. Enter the size of the data file, in megabytes, in the **Initial Size (MB)** field.
10. Click **OK**.
11. Close SQL Server Management Studio.

Scheduling Database Grooming Jobs

You can change scheduled times for the default grooming jobs using Microsoft SQL Server Management Studio.

To change scheduled database grooming:

1. Log on to the database server using an account that has SQL Administrator privileges. For more information about SQL permissions, see the Microsoft SQL Server Help.
2. Start **SQL Server Management Studio**, located in either the Microsoft SQL Server 2005 or Microsoft SQL Server 2008 program group.
3. In the Connect to Server window, select **Database Engine** as the server type.
4. Click **Connect**.
5. ***If the SQL Server Agent is stopped,*** right-click **SQL Server Agent** and select **Start**.
6. ***If the SQL Server Agent is started,*** expand **SQL Server Agent > Jobs**.
7. In the right pane, right-click the job you want to reschedule and click **Properties**.
8. On the Schedules tab, click **Edit**.
9. Specify the appropriate values on the Job Schedule Properties window. For more information about the fields on a window, see the Microsoft SQL Server Help.
10. Click **OK** on the Job Schedule Properties window.
11. Click **OK** on the Properties window.
12. Close SQL Server Management Studio.

Grooming the Reporting Cube

It is generally not necessary to groom the reporting cube. This database contains summarized data representing only 7% of all data collected by Security Manager. The cube retains reporting data for 365 days by default, after which SQL Server deletes the data.

If you want to retain reporting data for a time period other than 365 days, you can modify the reporting cube lifetime settings using SQL Server Management Studio.

Note

The reporting cube does not contain Forensic Analysis report data. To groom Forensic Analysis report data, use the Development Console.

For more information about OnePoint and LogManagerConfiguration database grooming, see “Grooming the OnePoint and LogManagerConfiguration Databases” on page 262.

To modify reporting cube grooming settings:

1. Log on to the reporting server using an account that has SQL Administrator privileges. For more information about SQL permissions, see the Microsoft SQL Server Help.
2. Start **SQL Server Management Studio**, located in either the Microsoft SQL Server 2005 or Microsoft SQL Server 2008 program group.
3. In the Connect to Server window, select **Analysis Services** as the server type.
4. Select the reporting server name and click **Connect**.
5. Expand **Databases > SMCubeDepot > Tables > dbo.Process_Control**.
6. In the main toolbar, click **New Query**.
7. In the new query window, type the following command, where *NewGroomingTime* is the number of days after which you want Microsoft SQL Server to groom cube data:

```
select * from dbo.Process_Control


update dbo.Process_Control set attrValue = NewGroomingTime where
attrName = 'PartitionLifeTime'


select * from dbo.Process_Control
```

8. In the SQL Editor toolbar, click **Execute**. The first table displayed shows the original value of the reporting cube grooming setting, and the second table shows the modified value.

9. Close SQL Server Management Studio.

Note

If you need to retain reporting data for a period longer than 24 months, ensure you back up your reporting cube using SQL Server Management Studio before the data is groomed.

Configuring SQL Databases

Security Manager provides preconfigured SQL Server jobs for performing various functions in the OnePoint and LogManagerConfiguration databases and reporting cube. You can modify the SQL job settings using SQL Server Management Studio.

For more information about configuring database grooming, see “Grooming the OnePoint and LogManagerConfiguration Databases” on page 262.

OnePoint Database SQL Jobs

Security Manager provides the following standard SQL jobs for the OnePoint database:

OnePoint - Check Free Data Space

Scheduled to run every 2 hours, starting daily at 12:45 AM. This job calculates the percentage of free space in the OnePoint database and sends the information to Security Manager as an event.

OnePoint - Check Integrity

Scheduled to run once a week on Saturday at 10:00 PM. This job validates the integrity of the OnePoint database. For example, it checks that the index and data pages are correctly linked and that indices are in the proper sort order.

OnePoint - Groom Alerts

Scheduled to run every hour. This job grooms resolved alerts from the OnePoint database based on the information specified in Global Settings.

OnePoint - Groom Completed Forensic Analysis Reports

Scheduled to run every six hours. This job grooms completed Forensic Analysis report data from the OnePoint database based on the information specified in Global Settings.

OnePoint - Groom Events

Scheduled to run every hour. This job grooms events from the OnePoint database based on the information specified in Global Settings.

Note

You cannot groom alerts or events if they are part of an incident package.

OnePoint - Groom Log Archive History

Scheduled to run once a day at 2:00 AM. This job grooms log archive history data older than two days from the OnePoint database. Log archive history data are used to report successful and failed attempts to collect and insert log data into the log archives.

OnePoint - Groom Sampled Numeric Data

Scheduled to run every hour. This job grooms sampled numeric data from the OnePoint database based on the information specified in Global Settings.

OnePoint - Groom Security

Scheduled to run once a day at 3:00 AM. This job grooms outdated public key data from the ComputerSecurity table in the OnePoint database.

OnePoint - Real time events without corresponding alerts

Scheduled to run every hour. This job grooms real-time events from which Security Manager has not generated an alert, based on the information specified in Global Settings.

OnePoint - Reindex

Scheduled to run once a week on Sunday at 10:00 PM. This job rebuilds the Security Manager table indices to improve performance. In order to complete successfully, the OnePoint-Reindex database job requires that the OnePoint database has approximately 40% additional free space. For example, a 10 GB database needs 14 GB total space to successfully rebuild the indices. If the jobs fail because of lack of disk space, the failure does not adversely affect your Security Manager implementation.

OnePoint - Reindex Event Tables

Scheduled to run once a day between 12:16 AM and 11:59 AM. This job rebuilds the event table indices to improve performance. The OnePoint-Reindex Event Table database job requires approximately 40% free space within the OnePoint database to complete successfully. For example, a 10 GB database needs 14 GB total space in the database to successfully rebuild the indices. If the jobs fail because of lack of disk space, the failure of the jobs does not adversely affect your Security Manager implementation.

OnePoint - TodayStatisticsUpdateComputersAndAlerts

Scheduled to run every 5 minutes. This job updates the OnePoint Security Manager Today window.

OnePoint - TodayStatisticsUpdateEvents

Scheduled to run every 30 minutes. This job updates the OnePoint Security Manager Today window.

OnePoint - TodayStatisticsUpdatePerfmonRulesKB

Scheduled to run every hour. This job updates the OnePoint Security Manager Today window.

OnePoint - Update Database

Scheduled to run every hour. This job grooms auto-resolved alerts based on the information specified in Global Settings.

OnePoint - Update Statistics

Scheduled to run once a day at 1:00 AM. This job updates information on key value distribution in the OnePoint database to improve performance.

Disabling OnePoint Database Reindexing Jobs

You can disable the OnePoint - Reindex and OnePoint - Reindex Event Tables default database jobs using SQL Server Management Studio. If you do not expand the Security Manager OnePoint database, allocating at least 40% free space, these jobs fail. For more information about expanding your database capacity, see “Expanding Your OnePoint Database” on page 266.

If you disable the reindexing jobs, you do not experience the performance benefits the jobs create. However, failure of the reindexing jobs adversely affects performance of your Security Manager implementation.

To disable the database reindexing jobs:

1. Log on to the database server using an account that has SQL Administrator privileges. For more information about SQL permissions, see the Microsoft SQL Server Help.
2. Start **SQL Server Management Studio**, located in either the Microsoft SQL Server 2005 or Microsoft SQL Server 2008 program group.
3. In the Connect to Server window, select **Database Engine** as the server type.
4. Click **Connect**.
5. ***If the SQL Server Agent is stopped,*** right-click **SQL Server Agent** and select **Start**.
6. ***If the SQL Server Agent is started,*** expand **SQL Server Agent > Jobs**.
7. Right-click **OnePoint - Reindex** and select **Disable**.
8. Right-click **OnePoint - Reindex Event Tables** and select **Disable**.
9. Close SQL Server Management Studio.

LogManagerConfiguration Database SQL Job

Security Manager provides the following SQL job for the LogManagerConfiguration database:

LogManagerConfiguration - Groom Bookkeeping Entries on UNIX and iSeries Data Collection

Scheduled to run once a day at 3:00 AM. This job grooms internal bookkeeping entries related to collection of UNIX or iSeries log data. The job grooms any data older than 30 days.

Reporting Cube SQL Job

Security Manager provides the following SQL job for the reporting cube:

NetIQ_SM_SSIS

Scheduled to run every three hours. This job runs a SQL Server Integration Services Package that uploads log archive data received by the cube depot into the reporting cube.

Modifying the Reporting Cube Processing Job

Using SQL Server Management Studio, you can change the interval at which the reporting server processes data in the cube depot and uploads the data into the reporting cube. The reporting server processes log archive data every 3 hours by default.

To modify the reporting cube processing job:

1. Log on to the database server using an account that has SQL Administrator privileges. For more information about SQL permissions, see the Microsoft SQL Server Help.
2. Start **SQL Server Management Studio**, located in either the Microsoft SQL Server 2005 or Microsoft SQL Server 2008 program group.
3. In the Connect to Server window, select **Database Engine** as the server type.
4. Click **Connect**.

5. ***If the SQL Server Agent is stopped,*** right-click **SQL Server Agent** and select **Start**.
6. ***If the SQL Server Agent is started,*** expand **SQL Server Agent > Jobs**.
7. Right-click **NetIQ_SM_SSIS** and select **Properties**.
8. Click **Schedules**.
9. Select the listed schedule and click **Edit**.
10. Specify the appropriate settings and then click **OK**.
11. Click **OK** again.
12. Close SQL Server Management Studio.

Configuring Forensic Analysis Query Settings

Using the Control Center, you can configure global settings for all Forensic Analysis queries on your central computer, including the number of minutes before a Forensic Analysis query times out.

If you modify Forensic Analysis query settings, the changes do not affect a query that is currently running. However, the next time you run the query, the modified settings take effect.

Notes

- You cannot use the Control Center to modify completed Forensic Analysis report grooming settings. For more information about grooming completed reports, see "Modifying Database Grooming Settings" on page 263.
- In addition to the global Forensic Analysis query setting that specifies the number of minutes before a query times out on all log archives in your configuration group, you can also configure the number of minutes before a query times out on your log archive servers themselves. If a particular log archive server runs more slowly than other servers in the configuration group, you could configure that server to time out more quickly than the global setting allows. All other log archive servers would be unaffected and would use the global setting.
- If you increase the number of minutes a query can run using the Control Center, you should also increase the same setting on each log archive server in the configuration group. If the setting on your log archive server is set to the default but the global setting is larger, the query times out as specified in the smaller of the two settings. For more information about configuring log archive server settings, see "Modifying Log Archive Settings" on page 280.

To configure global Forensic Analysis query settings:

1. Log on to the central computer using an account that is a member of the OnePointOp Reporting group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Forensic Analysis**.
4. On the Tasks menu, click **Forensic Analysis Tasks > Modify Global Query Settings**.

5. Modify the default global Forensic Analysis query settings as necessary and click **OK**.

6. Click **Yes** to confirm.

Configuring Log Archives

Using the Log Archive Configuration utility, you can manage the log archives on your log archive server. You can add or create new log archives, detach existing log archives, specify settings for all log archives on the log archive server, configure data signing on your log archives, or specify a new log archive server.

You can also use the Configuration Wizard to specify a new log archive server or manually configure the number of indexing jobs the log archive server uses by modifying the `LogArchiveConfiguration.config` file.

For more information about modifying log archive grooming settings, see "Grooming the Log Archives" on page 142.

For more information about modifying log archive data signing settings, see the *Installation Guide for NetIQ Security Manager*.

Adding Log Archives

When you install Security Manager on the log archive server, the installation program creates a log archive. You can create additional log archives at any time using the Log Archive Configuration utility. Additional log archives can be useful if you want to migrate an existing log archive to another log archive server or if you want to store a log archive on a different drive.

To reduce the possibility of data alterations, you can restrict permissions on your log archives so that unauthorized users cannot access the data from the file system. When you create or add a new log archive, you can restrict permissions on the log archive.

If you choose to restrict permissions on a log archive, members of the OnePointOp ConfgAdms group and the local Administrator are granted full control. Other users have no access to the log archive directory or files. Restricting permissions on a log archive does not affect the ability of users to view log archive data in the Control Center.

To add or create a new log archive:

1. Log on to the log archive server using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start **Log Archive Configuration** in the NetIQ Security Manager > Configuration program group.
3. Click **Log Archives**.
4. Click **Add**.
5. Specify the name, path, and maximum size of the log archive. Note that if the log archive already exists, you need to make sure that you specify the correct path.
6. ***If you want to set new permissions on the log archive,*** click **Yes**.
7. ***If you want to keep the current permissions for an existing log archive,*** click **No**.
8. Click **Apply**.
9. Click **Yes**.
10. Click **Close**.
11. Click **Yes** on the confirmation message to restart the `NetIQ Security Manager Log Archive` service.
12. Click **Yes** to exit the configuration tool.

Note

If you modify any log archive setting, you must restart the log archive server for the change to take effect.

Changing Log Archives

Security Manager sends log data to one log archive at a time, even if you have installed more than one log archive on the log archive server. To redirect log data to a new log archive, create a new log archive and then disable the previous log archive using the Log Archive Configuration utility.

To change the log archive to which Security Manager sends data:

1. Log on to the log archive server using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Open the Services Administrative Tool located in the Control Panel.
3. In the Services pane, click **NetIQ Security Manager Log Archive**.
4. On the Action menu, click **Stop**.
5. Close the Services Administrative Tool.
6. Start **Log Archive Configuration** in the NetIQ Security Manager > Configuration program group.
7. Click **Log Archives**.
8. Ensure you have created a new log archive to receive log data. For more information about creating or adding new log archives, see "Adding Log Archives" on page 276.
9. Select the log archive you want to disable.
10. Select **Read-Only**. This forces Security Manager to begin sending log data to the next log archive in the list.
11. Click **Apply**.
12. Click **Yes**.
13. Click **Close**.

14. Click **Yes** on the confirmation message to restart the `NetIQ Security Manager Log Archive` service.

15. Click **Yes** to exit the configuration tool.

Note
If you modify any log archive setting, you must restart the log archive server for the change to take effect.

Detaching Log Archives

When you want to remove an existing log archive from a log archive server, you can use the Log Archive Configuration utility to detach a specified log archive.

Note
Detaching a log archive does not delete any data, but instead makes the log archive data inaccessible from Security Manager.

To detach an existing log archive:

1. Log on to the log archive server using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start **Log Archive Configuration** in the NetIQ Security Manager > Configuration program group.
3. Click **Log Archives**.
4. Select the log archive you want to detach.
5. Click **Detach**.
6. Click **Yes** on the confirmation window.
7. Click **Apply**.
8. Click **Yes**.
9. Click **Close**.

10. Click **Yes** on the confirmation message to restart the `NetIQ Security Manager Log Archive` service.

11. Click **Yes** to exit the configuration tool.

Note
If you modify any log archive setting, you must restart the log archive server for the change to take effect.

Modifying Log Archive Settings

You can modify log archive settings to configure reporting, change the number of minutes before a query times out, enable data signing, and customize other settings on the log archive server. Modified settings are applied to all log archives on the log archive server.

Notes

- If you modify global Forensic Analysis query settings in the Control Center to increase the number of minutes before a query times out, ensure you also increase the timeout setting for each log archive server in your configuration group. For more information about configuring global Forensic Analysis query settings, see "Configuring Forensic Analysis Query Settings" on page 274.
- If you enable data signing on your log archive server, you must also enable data signing on all central computers sending data to the log archive server.

To modify log archive settings:

1. Log on to the log archive server using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start **Log Archive Configuration** in the NetIQ Security Manager > Configuration program group.
3. Click **Log Archive Server Settings**.
4. Modify the fields as appropriate. For more information about fields on a window, see the Help.

5. Click **Apply**.

6. Click **Yes**.

7. Click **Close**.

8. Click **Yes** on the confirmation message to restart the `NetIQ Security Manager Log Archive` service.

9. Click **Yes** to exit the configuration tool.

Note
If you modify any log archive setting, you must restart the log archive server for the change to take effect.

Changing the Log Archive Server or Port

Using the Configuration Wizard on the central computer, you can specify a log archive server other than the server specified at installation to receive log data and Forensic Analysis queries. For example, if you specify a computer as your log archive server and then decide that the computer does not have adequate storage capacity for the amount of data received, you can redirect the agents within the configuration group to a new log archive server.

The log archive server component must be installed and configured properly on the new computer before it begins to receive data. For more information about installing the log archive server, see the *Installation Guide for NetIQ Security Manager*.

To specify a new log archive server or port:

1. Log on to the central computer with a user account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.

3. In the Navigation pane, click **All Folders**.

4. On the Tasks menu, click **Global Tasks > Launch Configuration Wizard**.

5. Click **Global Settings**.
6. Click **Log Archive Configuration**.
7. Select the existing log archive server name.
8. Click **Specify**.
9. Specify the name and port number of the new log archive server.
10. ***If you want to specify a log archive server located in an untrusted domain and use an account other than the default service account,*** complete the following steps:
    a. Click **Connect as**.

    b. Specify the name and password of the service account you want to use to connect your central computer to the log archive server in the untrusted domain.

    Notes

    - You must specify a domain account in the untrusted domain.
    - The domain account must also be a member of one of the OnePointOp groups in the untrusted domain.
    - If you specify an account that does not have the appropriate credentials for the untrusted domain, the central computer cannot connect to the specified log archive server.
11. ***If you want to specify a log archive server located in an untrusted domain and use the default service account to connect,*** select **Connect as service account**.

    Note

    You can the default Security Manager service account if that account has the appropriate credentials in the untrusted domain.
12. Click **OK**.
13. Click **Finish**.
14. Click **OK**.

15. Click **Close**.

16. Restart the `NetIQ Security Manager Core` service for your changes to take effect.

Disassociating a Log Archive Server from a Central Computer

You can also use the Configuration Wizard to disassociate an existing log archive server completely from a particular central computer. After you disassociate the log archive server from a central computer, the central computer no longer stores data in any log archive on the log archive server.

Notes

- If you disassociate a log archive server from a central computer and do not specify a new log archive server, Security Manager only stores real-time data in the OnePoint database. Any archival data remains in the log archival queue indefinitely. NetIQ recommends that only knowledgeable users modify this setting.
- In addition, if you disassociate a log archive server from a central computer, you can no longer use Security Manager to query any data stored in log archives on that log archive server.

To disassociate a log archive server from a central computer:

1. Log on to a Control Center computer using an account that is a member of the OnePointOp ConfgAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.
4. On the Tasks menu, click **Global Tasks > Launch Configuration Wizard**.
5. Click **Global Settings**.
6. Click **Log Archive Configuration**.
7. Select the central computer connected to the log archive server you want to disassociate.
8. Click **Disassociate**.

9. Click **Yes** to confirm.

10. Click **Finish**.

11. Click **OK**.

12. Click **Close**.

13. Open the Services Administrative Tool located in the Control Panel.

14. In the Services pane, click **NetIQ Security Manager Core**.

15. On the Action menu, click **Restart**.

16. Close the Services Administrative Tool.

Configuring Log Archive Server Indexing Jobs

When you install the Security Manager log archive server component, the setup program configures the log archive server to use a number of indexing jobs equal to the number of cores on the computer by default. However, if you do not use a dedicated log archive server computer, this configuration can cause the log archive server to consume a disproportionate amount of resources.

If you want to install the log archive server on a computer with other Security Manager components, NetIQ recommends reducing the number of indexing jobs to half the number of cores on the computer.

For more information about log archive indexing, see "Log Archive Indexing" on page 128.

To change the number of log archive server indexing jobs:

1. Log on to the log archive server using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.

2. ***If your log archive server uses Windows Server 2003,*** navigate to the `Documents and Settings\All Users\Application Data\NetIQ\Security Manager` folder.

3. ***If your log archive server uses Windows Server 2008,*** navigate to the `ProgramData\NetIQ\Security Manager` folder.

4. Open the `LogArchiveConfiguration.config` file using a text editor, such as Notepad.

   Note
   If your log archive server computer uses Windows Server 2008 R2 or Windows Server 2008, ensure you edit the `LogArchiveConfiguration.config` file using an account that is a member of the local Administrators group.

5. Search for the `IndexJobCount` setting.

6. Change the `IndexJobCount` setting to a value other than `default`.

7. Save and close the `LogArchiveConfiguration.config` file.

8. Restart the `NetIQ Security Manager Log Archive` service for your changes to take effect.

Configuring Global Settings

These tasks provide step-by-step guidance for configuring Global Settings, such as alert resolution states and component communications.

Configuring Alert Resolution States

Using the Development Console, you can create your own alert resolution states, as well as modify most of the default states. You can also specify the service level agreement time, which is the maximum amount of time an alert should remain in a resolution state before it becomes a service level exception.

Note
If you run the Security Manager Control Center while creating or modifying alert resolution states, you must close and restart the Control Center before you can view and use those new or modified resolution states.

To configure alert resolution states:

1. 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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration**.
4. Click **Global Settings**.
5. In the right pane, click **Alert Resolution States**.
6. On the Action menu, click **Properties**.
7. Specify the appropriate settings. For more information about the fields on a window, click **Help**.
8. Click **OK**.

Configuring Communication Ports

You can change the default TCP/IP port for communications between Windows agents and central computers in a configuration group. For more information about default ports, see the *Installation Guide for NetIQ Security Manager*.

Note
NetIQ does not recommend changing the default port after you initially configure your environment. Changing the port can cause significant interruptions in communications between central computers and agents. If you change the port and then restart the `NetIQ Security Manager` service on your central computers, your agents cannot communicate with your central computers until you restart the service on all agents, as well.

To change the TCP/IP port:

1. 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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration**.
4. Click **Global Settings**.
5. In the right pane, click **Communications**.
6. On the Action menu, click **Properties**.
7. ***If you want to modify the port for standard Windows agents,*** specify the port number you want your Windows agents to use to communicate with your central computer. For more information about the fields on a window, click **Help**.
8. ***If you want to modify the port for legacy Windows agents,*** specify the port number you want your legacy Windows agents to use to communicate with your central computer. Legacy agents are version 6.0 Service Pack 4 and earlier. For more information about the fields on a window, click **Help**.
9. Click **OK**, then click **OK** to confirm.
10. In the left pane, click **Central Computers**.
11. On the Action menu, click **Scan All Managed Computers**.
12. When the central computer finishes scanning all managed agents, stop and restart the `NetIQ Security Manager` service on all central computers in your configuration group.
13. After you restart the service on all central computers, log on to each agent computer and manually stop and restart the `NetIQ Security Manager` service.

For more information about communications for UNIX agents, see the NetIQ UNIX Agent documentation.

Configuring Email Settings

Using the Development Console, you can configure settings for all central computers to use when sending email responses to notification groups.

To configure global email settings:

1. 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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration**.
4. Click **Global Settings**.
5. In the right pane, click **Email Server**.
6. On the Action menu, click **Properties**.
7. Specify the appropriate settings. For more information about the fields on a window, click **Help**.
8. Click **OK**.

Configuring Custom Fields for Alerts

You can create fields that Security Manager displays in alerts. All alerts generated in the configuration group will contain these fields.

To configure custom alert fields:

1. 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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration**.

4. Click **Global Settings**.

5. In the right pane, click **Custom Alert Fields**.

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

7. Specify the appropriate settings. For more information about the fields on a window, click **Help**.

8. Click **OK**.

Configuring Auditing of Configuration Changes

Using the Development Console, you can audit changes to Security Manager configuration, such as changes made to processing rules. Auditing configuration changes allows you to run a Forensic Analysis query against all central computers to report on these changes. Security Manager writes configuration change events to the Security Manager Audit Log, which you can specify as the log source when creating a Forensic Analysis query. For more information about Forensic Analysis queries, see "Creating Forensic Analysis Queries" on page 155.

Note
Auditing of configuration changes is CPU-intensive.

To configure configuration auditing:

1. 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 "Understanding Requirements and Permissions" on page 24.

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

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

4. Click **Global Settings**.

5. In the right pane, click **Auditing**.

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

7. Select **Audit changes made through the central computer on *SERVERNAME***, where ***SERVERNAME*** is the name of the central computer.

   Note
   If your user account does not have read and write access to the central computer registry, this option is unavailable.

8. Click **OK**.

Configuring Central Computer Settings

Using the Development Console, you can configure settings for central computers in the configuration group, either globally or for each specific central computer. These settings specify the agent service account, the temporary data storage location, the number of responses that can run at the same time, and how often the central computer scans agents, polls for rule changes, and checks for agent heartbeats.

You can configure how central computers install and uninstall Windows agents, including whether agents are added to the Pending Agents Installation or Uninstallation list to wait for approval.

Notes

- You can only modify certain central computer settings globally, like rule change polling and temporary storage settings.
- If you modify settings in the Redundancy Policy tab of the central computer settings, Security Manager automatically restarts the `NetIQ Security Manager` service on all affected agent computers.
- If you modify settings in the Response Handling or Temporary Storage tabs of the central computer settings, you must manually restart the `NetIQ Security Manager` service on all affected central computers.
- If you modify settings in the Advanced tab of the central computer settings, you must right-click **Security Manager Development Console** in the left pane of the Development Console, select **Force Configuration Changes Now**, then manually restart the `NetIQ Security Manager` service on all affected central computers.

To configure central computer settings:

1. 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 "Understanding Requirements and Permissions" on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration**.
4. ***If you want to configure global central computer settings,*** complete the following steps:
    a. Click **Global Settings**.
    b. On the Action menu, click **Edit Central Computer Settings**.
5. ***If you want to configure settings for a specific central computer,*** complete the following steps:
    a. Click **Central Computers**.
    b. In the right pane, select the central computer you want to configure.
    c. On the Action menu, click **Properties**.
6. Specify the appropriate settings. For more information about the fields on a window, click **Help**.
7. Click **OK**.

Configuring General Agent Settings

Using the Development Console, you can configure settings for managed and unmanaged Windows agents in the configuration group, either globally or for each specific agent computer. These settings include buffering, service checking, event collection, communication failure handling, and response handling parameters, among others.

Notes

- You can only modify certain agent settings globally, like scalability and heartbeat settings.
- If you modify settings in the Communications, Scalability, Buffering, Temporary Storage, Response Handling, or Advanced tabs, Security Manager automatically restarts the `NetIQ Security Manager` service on all affected agent computers.

To configure global Windows agent settings:

1. 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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration**.
4. ***If you want to configure global agent settings,*** complete the following steps:
   a. Click **Global Settings**.
   b. On the Action menu, click **Edit Agent Settings**.
5. ***If you want to configure settings for a specific agent computer,*** complete the following steps:
   a. Click **Central Computers**.
   b. In the right pane, select the central computer that monitors the agent you want to configure.

c. On the Action menu, click **View Managed Computers**.

d. Select the agent computer you want to configure and click **Settings**.

6. Specify the appropriate settings. For more information about the fields on a window, click **Help**.
7. Click **OK**.

Configuring Licensing

Using the Development Console, you can apply a new license and read copyright and acknowledgment information. You can also view a list of applied licenses.

Note
If your Security Manager license expires, you cannot use the Development Console to apply a new license. You can use the Module Installer to apply a new license, instead.

For more information about using the Module Installer, see “Installing New or Updated Modules” on page 183.

To configure licensing:

1. 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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration**.
4. Click **Global Settings**.
5. In the right pane, click **License**. Security Manager displays a window containing the names of applied licenses.
6. On the Action menu, click **Properties**.
7. Click **Apply New License**.

8. Specify the appropriate settings. For more information about the fields on a window, click **Help**.

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.

Configuring Web Addresses

You can specify the virtual Web addresses for the Web Console and for the Microsoft SQL Server Reporting Server, if enabled.

Modifying the Web Console address allows you to point to a different computer where you installed a Web Console server. Security Manager uses the **Web Console** address to provide links in the consoles that launch the Web Console interface.

Modifying the Reports address allows you to access the SQL Server Report Manager and SQL Server Report Server Virtual Directories directly from the Web Console or Control Center. Security Manager uses the **Reports** address to provide links in the Control Center and Web Console to the Report Manager Website.

To configure Security Manager Web addresses:

1. 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 “Understanding Requirements and Permissions” on page 24.

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

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

4. Click **Global Settings**.

5. In the right pane, click **Web Addresses**.

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

7. Specify the appropriate settings. For more information about the fields on a window, click **Help**.

8. Click **OK**.

Note

If you specify the Web Console or Reports Web addresses, you must restart the `IIS Admin Service` for the change to take effect.

Configuring Primary and Backup Correlation Servers

The setup program installs a Correlation Engine on every central computer. Security Manager configures the first central computer available as the primary Correlation server. Security Manager configures additional central computers as backup Correlation servers. A primary Correlation server is the default central computer to process correlation data.

Backup Correlation servers are central computers that can process correlation data if the primary Correlation server becomes unavailable. If the primary Correlation server becomes unavailable, the Correlation server responsibility fails over to the next Correlation server listed in Global Settings. Backup Correlation servers are recommended but optional. Failover proceeds in the order that Correlation servers are listed, from top to bottom.

Using the Development Console, you can exclude central computers from acting as Correlation servers, change the identity of the primary Correlation server, and change the order in which failover occurs by modifying the Correlation server settings.

To modify Correlation server settings:

1. 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 “Understanding Requirements and Permissions” on page 24.

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

3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration > Global Settings**.

4. In the right pane, click **Correlation Server**.

5. On the Action menu, click **Properties**.
6. On the Correlation Server tab, modify the appropriate settings. The top Correlation server in the right pane is the primary Correlation server. Failover occurs in the order in which computers are listed, from top to bottom. For more information about the fields on a window, click **Help**.
7. Click **OK**.

Configuring Correlation Settings

Using the Development Console, you can specify how much time passes before failover occurs for the primary Correlation server role. You can also configure the size of the correlation queue and how long an event remains in the queue before the Correlation server submits it to the Correlation Engine for processing.

To configure correlation settings:

1. 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 “Understanding Requirements and Permissions” on page 24.
2. Start the **Development Console** in the NetIQ Security Manager program group.
3. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration**.
4. Click **Global Settings**.
5. In the right pane, click **Correlation Settings**.
6. On the Action menu, click **Properties**.
7. Specify the appropriate settings. For more information about the fields on a window, click **Help**.
8. Click **OK**.

Configuring Primary and Backup Central Computers

By default, Security Manager specifies one or more central computers the agent can contact in the event that its assigned central computer is unavailable. However, you can disable this setting and specify backup central computers for each central computer in your configuration group.

Under certain circumstances, such as maintenance or communications problems, an agent may not be able to communicate with the central computer to which it is assigned. Security Manager does not leave the agent without a central computer. Instead, Security Manager temporarily assigns the agent to another central computer, chosen from a list you specify.

When failover to another central computer occurs, the backup central computer provides many of the functions the primary central computer provided until the primary central computer is again accessible. Following failover, agents send events to the backup central computer. The backup central computer can pass rules and configuration to the agent and can scan the agent.

Each central computer can have more than one backup computer. When Security Manager initiates failover, the inaccessible central computer fails to the first designated backup central computer. If the backup central computer is also unavailable, Security Manager continues down the list until it identifies an available computer.

Note

If you are permanently removing a primary central computer from a configuration group, do not rely on failover to provide agent coverage. Instead, reassign the agent to a different central computer in the configuration group. For more information about changing the central computer to which an agent is assigned, see “Changing which Central Computer Manages an Agent” on page 217.

To manually specify central computers for failover:

1. ***If the central computers use different service accounts,*** ensure the service account used by each backup central computer is a member of the local Administrators group on all agents managed by the primary central computer and that each is also either in a trusted domain or the same domain as the database server.

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 "Understanding Requirements and Permissions" on page 24.

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

4. ***If you want to disable automatic failover,*** complete the following steps.

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

   b. In the right pane, click **Central Computers**.

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

   d. Click **Redundancy Policy**.

   e. Clear **System controlled**.

   f. Click **OK**.

5. In the left pane, click **Central Computers**.

6. In the right pane, select a central computer for which you want to specify failover computers.

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

8. Click **Redundant Central Computers**.

9. In Available Central Computers, select a computer.

10. Click **>>**.

11. Repeat Steps **9** through **10** for each central computer that you want to designate as a failover computer.

12. Click **Move Up** and **Move Down** to arrange the computers in the order that you want failover to occur.

13. Click **OK**.

Upgrading Your License

Security Manager requires a license key file. This file contains license information and is installed with the OnePoint database. When you install the product, the installation program allows you to use the default trial license key file or a customized license key file provided by NetIQ.

The license key file defines limits on key operation parameters such as an expiration date, a grace period and the number of computers that can be monitored by Security Manager. After the expiration date (during the grace period), the product logs warning messages. After the grace period, many Security Manager components will cease to function.

Using the Development Console, you can upgrade the license. Only accounts within the OnePointOp ConfgAdms group can apply new licenses.

Note

If your Security Manager license expires, you cannot use the Development Console to apply a new license. You can use the Module Installer to apply a new license, instead.

For more information about using the Module Installer, see “Installing New or Updated Modules” on page 183.

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.

To upgrade the license:

1. 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 “Understanding Requirements and Permissions” on page 24.
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, click **Apply New License**.
8. Click **Browse** in the Apply New License window.
9. Select the Security Manager `.lic` file.
10. ***If you are upgrading a trial license,*** select the trial license located in the upgrade kit.
11. ***If you are upgrading a custom license,*** select the custom license provided by NetIQ.
12. Click **Open**.
13. Read the Apply New License window and then click **OK**.
14. Click **OK** to close the Configuration Group Global Settings window.
15. Close the Development Console.

Changing Service Account Passwords

To change the password for the service account, follow the instructions in the NetIQ Technical Support Knowledge Base.

To access the NetIQ Technical Support Knowledge Base:

1. Access the Web site at `www.netiq.com/support`.
2. Click **Search the Knowledge Base**.
3. Click **Search Category** and select **Articles**.
4. Click **Select a Product** and select **NetIQ Security Manager**.
5. In **My Question is**, type `How do I change the service account password?`
6. Click **Search**.
7. Scroll down to see a list of related topics.
8. Click the title of the most appropriate topic.

Modifying Security Manager OnePointOp Group Membership

Security Manager uses OnePointOp groups and database roles to restrict access to product functionality. For more information about OnePointOp groups and database roles, see “Understanding Requirements and Permissions” on page 24.

The Access Configuration utility allows you to add global domain groups to the OnePointOp groups. The utility also creates database logins for the global domain groups, and then adds the database logins to the appropriate database roles on the database server. You can also use the Access Configuration utility to repair invalid accounts.

If you added an account with a user interface other than the Access Configuration utility, the account is invalid. For a user account to be valid it must be a member of a global domain group that you added to a OnePointOp group with the Access Configuration utility. The Access Configuration utility must also create a database login for the global domain group.

If a global domain group contains an invalid user account, you can use the Access Configuration utility to repair the user account. The Access Configuration utility repairs the user account by resetting the database login. However, the Access Configuration utility cannot make a user account valid if the account does not belong to a global domain group already a member of one or more OnePointOp groups.

To add a user account to a OnePointOp group and database role, add the user account to a global domain group that is a member of the OnePointOp group.

Note
The Access Configuration utility does not manage membership of the global domain groups. Use Active Directory Users and Computers to manage account memberships of the global domain groups.

To modify memberships in OnePointOp Groups and database roles:

1. Log on to a central computer with an account that is a member of the local Administrators group and a member of the Microsoft SQL Server sysadmin role on the database server.
2. Start **Access Configuration** in the NetIQ Security Manager > Configuration program group.
3. In the left pane, click the OnePointOp group with memberships you want to modify. Complete one of the following steps:
   - To add a member, click **Add**.
   - To remove a member, click **Remove**.
   - To repair a member, select an invalid group member, and then click **Repair**.
4. Repeat Step **3** for each OnePointOp group you want to modify.
5. Click **OK**. For more information about fields on a window, see the Help.
6. Repeat Steps **1** through **5** on each central computer in the configuration group.

Appendix A

Understanding Text String Pattern Matching

In many Security Manager fields, you can enter or select wildcard characters, regular expressions, or Boolean regular expressions. Wildcard characters and regular expressions allow you to specify or match many items using one expression or character-string formula.

Note
The Control Center and Agent Administrator do not support using regular expressions or Boolean regular expressions. Regular or Boolean regular expressions are only used in defining or finding rules in the Development Console.

You can select wildcard characters, regular expressions, or Boolean regular expressions from some drop-down menus, or you can enter them directly in the appropriate field, depending on the interface. Wildcard menu items and their associated characters are defined in tables in the following sections.

Wildcard Characters

You can use wildcard characters in some areas where you cannot use regular expressions. Wildcard pattern matching is not case-sensitive. Some fields support the following wildcard characters.

Menu Item	Character	Definition
Any Character	Question mark (?)	Matches exactly one character.
Any Digit	Number sign (#)	Matches one digit. **Note:** This wildcard is used only when defining rules or views and cannot be used for Forensic Analysis queries.
Any Character, 0 or More Matches	Asterisk (*)	Matches zero or more characters.

The following table provides examples of wildcard character specifications and example matches. The escape character (\ ) that precedes a character changes the character from a wildcard to its text meaning. For example, Security Manager reads the Any Character wildcard in `houston\?` as a question mark.

Example	Matches	Does Not Match
den???	Denton and Dennis	Denison
`el ????o`	El Campo and El Indio	El Paso
`houston\?`	Houston?	Houstons
`houston, tx #####`	Houston, TX 77024	Houston, TX USOFA
`5555 lovers ln \###`	5555 Lovers Ln #32	5555 Lovers Ln 320
`*TX`	Houston, TX and TX	Houston, TX 77024
`San *`	San Antonio and San Angelo	Santa Fe

Example	Matches	Does Not Match
`b*ville`	Brownsville and Beeville	Somerville

Regular Expressions

You can perform advanced text pattern matching using **regular expressions**. Regular expressions provide more flexibility than simple wildcard characters in defining rules or views. To match an exact regular expression character, precede the character with a backslash (\).

The following table lists regular expression operators and their definitions:

Menu Item	Character	Definition
Any Character	.	Matches any single character.
Character in Range	[ ]	Matches any single character from within the bracketed list. Within square brackets, most characters are interpreted literally.
Character Not in Range	[^]	Specifies a set of characters not to be matched.
Beginning of Line	^	Matches the beginning of a line.
End of Line	$	Matches the end of a line.
Or	|	Matches either the regular expression preceding it or the regular expression following it.
Group	( )	Groups one or more regular expressions to establish a logical regular expression consisting of sub-regular expressions. Used to override the standard precedence of specific operators.
0 or 1 Matches	?	Specifies that the preceding regular expression is matched 0 or 1 time.

Menu Item	Character	Definition
0 or More Matches	*	Specifies that the preceding regular expression is matched 0 or more times.
1 or More Matches	+	Specifies that the preceding regular expression is matched 1 or more times.
Exactly N Matches	{n}	Specifies that the preceding regular expression is matched exactly n number of times.
At Least N Matches	{n,}	Specifies that the preceding regular expression is matched n or more times.
At Most N Matches	{,n}	Specifies that the preceding regular expression is matched n or fewer times.
N to M Matches	{n,m}	Specifies that the preceding regular expression is matched a maximum of m times and a minimum of n times.
New Line Character	\n	Matches a new line.
Tab Character	\t	Matches a tab character.

The following table provides examples of regular expressions and matches.

Example	Matches	Does Not Match
`st.n`	Austin and Houston	Webster
`st[io]n`	Austin and Houston	Stanton
`st[^io]n`	Stanton	Houston or Austin
`^houston`	Houston	South Houston or Fort Sam Houston
`ston$`	Houston and Galveston	Stonewall
`dall|hart`	Dallas and Dalhart and Lockhart	Dale
`dal(l|h)art`	Dalhart	Dallas or Lockhart
`il?e$`	Etoile and Wylie	Beeville

Example	Matches	Does Not Match
`il*e$`	Etoile and Wylie and Beeville	Bellaire
`il+e$`	Etoile and Beeville	Wylie
`ad{2}`	Addison and Caddo	Adkins
`(la.*){2,}`	Highland Village and Lake Dallas	Laredo
`il{,1}e$`	Bowie and Etoile	Brownsville
`(a.*){2,3}`	Alamo Heights and La Blanca	Austin or Arkansas Pass
`not ville`	Houston and Dallas	Brownsville

Boolean Regular Expressions

Boolean regular expressions allow you to combine regular expressions using the Boolean `and`, `or`, and `not` operators.

Menu Item	Operator	Definition
Boolean And	and	Specifies that the preceding and following regular expressions must both match.
Boolean Or	or	Specifies that one of the preceding and following regular expressions must match.
Boolean Not	not	Specifies that the regular expression following the Not must not match.

Regular and Boolean regular expression operators are available from some drop-down menus, or you can enter them directly in the appropriate field. The following table shows examples of Boolean regular expressions:

Example	Matches	Does Not Match
`la and ia`	La Vernia and Lelia Lake	Lake Jackson
`ville$ or town$`	Brownsville and Baytown	Lubbock
`ille$ and not ^[n-z]`	Brownsville and Kerrville	Pflugerville

Appendix B
Configuring Authenticated Communication

Security Manager provides two types of secure communication on Windows platforms. The default is encrypted communication, used to preserve the privacy and integrity of data passed between the central computer and agents.

Additionally, you can choose to authenticate communication. Certificate-based authentication adds a level of security by enabling the central computer to verify the data it collects comes only from valid agent computers. Authentication also enables the agent computers to verify the central computer itself is valid.

Warning

Changing from encrypted communication mode to encrypted and authenticated mode is an operation that requires significant planning and consideration.

Ensure you install all appropriate certificates before enabling agent authentication or central computer authentication. If you enable authentication without correctly installing all certificates, your central computers and agents cannot communicate.

Understanding Default Security Manager Communication

Security Manager uses the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocols included in the Microsoft Secure Channel (SChannel) security package to send data from Windows agents to the central computer.

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. For more information about authenticated communication, see “Understanding Authenticated Communication” on page 310.

Agents on UNIX and iSeries computers also communicate with the central computer using the SSL protocol. UNIX and iSeries agents authenticate any central computer that requests logs for archival and reporting.

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

Understanding Authenticated Communication

Security Manager uses the self-signed certificate created during installation of the central computer to enable secure communication between the central computer and agents. By default, agent computers do not provide their own agent certificates to the central computer.

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.

To enable authenticated communication, use your PKI to deploy and install trusted certificates on the central computer, agent computers, or both, depending on your environment. You can configure authenticated communication for any of the following scenarios:

- You can enable agent authentication, so the central computer that monitors your agents communicates only with agent computers presenting valid, trusted certificates.
- You can enable central computer authentication, so monitored agents communicate only with a central computer presenting a valid, trusted certificate.
- You can enable mutual authentication, so agents communicate only with central computers presenting valid, trusted certificates, and central computers communicate only with agent computers presenting valid, authenticated certificates.

After generating and installing trusted certificates on both agent computers and the central computer, as necessary, modify the registry on all affected computers to configure Central Computer Authentication and Agent Authentication settings. For more information about modifying the registry to enable authentication, see "Enabling Agent Authentication" on page 319 and "Enabling Central Computer Authentication" on page 321.

For authentication changes to take effect, you must restart the `NetIQ Security Manager` service on the central computer and all affected agents.

If you enable authentication between a central computer and an agent but do not correctly install or configure certificates for both components, the following situations occur:

- The agent is unable to send event or alert data to the central computer. As a result, this data is not available for views and reports.
- The agent is unable to send a heartbeat to the central computer.
- The central computer is unable to update the agent configuration.

Security Manager generates an alert when an unauthenticated agent contacts the central computer.

Note

Security Manager 6.5.4 does not support authenticated communication between central computers and legacy Windows agents. Legacy agents are agents with Security Manager 5.6 or Security Manager 6.0 installed.

Implementing Authenticated Communication

You can configure authenticated communication in your Security Manager environment by completing the following checklist:

☑	Steps	See Section
□	1. ***If you want to configure authenticated communication with your agent computers,*** issue and install agent computer certificates.	“Certificate Requirements” “Issuing and Installing Agent Authentication Certificates”
□	2. ***If you want to configure authenticated communication with your central computers,*** issue and install central computer certificates.	“Certificate Requirements” “Issuing and Installing Central Computer Authentication Certificates”
□	3. ***If you want to configure authenticated communication with your agent computers,*** enable agent authentication.	“Enabling Agent Authentication”
□	4. ***If you want to configure authenticated communication with your central computers,*** enable central computer authentication.	“Enabling Central Computer Authentication”
□	5. ***If you want to customize additional authentication settings,*** modify the appropriate registry keys.	“Customizing Certificate Usage”

☑	Steps	See Section
□	**6.** Verify that authenticated agents and central computers can communicate.	“Verifying Authenticated Communication”
□	**7.** Troubleshoot any authentication-related issues.	“Troubleshooting Authentication Problems”

Notes

- You can create and deploy authentication certificates for your agents and central computers either before or after installing Security Manager.
- You can enable authentication at any time after installing Security Manager. However, ensure you issue and install all necessary certificates on agent and central computers before enabling authentication.
- Central computers forward correlation events from agents to the Correlation server. If you have enabled correlation in your environment, your Correlation server authenticates central computers in the configuration group as if the computers were agents themselves. Configure central computers that send correlation events to the Correlation server for both central computer and agent authentication.

Certificate Requirements

When you issue agent or central computer certificates for authentication, ensure all certificates meet the following requirements:

- The certificate is an X.509 certificate.
- The certificate has an Client Authentication (`1.3.6.1.5.5.7.3.2`), a Server Authentication (`1.3.6.1.5.5.7.3.1`) Enhanced Key Usage (EKU), or both.

- The certificate has a private key.
- The certificate has the EXCHANGE key specification, including a public/private key pair used to encrypt session keys so they can be safely stored and exchanged with other users.

Note
For added security, NetIQ also recommends you ensure the certificate was issued by one of the certification authorities listed in the `TrustedIssuerSubjectNames` configuration property.

Issuing and Installing Agent Authentication Certificates

If you want to configure authentication for Security Manager agent computers, each agent needs to present a trusted certificate to the central computer that monitors the agent. You must install agent certificates in the `NetIQ Security Manager` container of the `Local Computer` certificate store on each agent computer.

Agent certificates should include the Client Authentication EKU, object identifier (OID) `1.3.6.1.5.5.7.3.2`, and must be trusted by the central computer. You can establish trust by placing all issuer certificates from the certificate chain of the agent certificate in the `Trusted Root Certification Authorities` container of the `Local Computer` certificate store on the central computer.

Notes

- You can install the agent authentication certificate by logging directly into the agent computer using an account that is a member of the local Administrators group or by remotely deploying the certificate to one or more agent computers, depending on your environment and PKI.
- If you have multiple certificates with the Client Authentication EKU stored in the `NetIQ Security Manager` container in the `Local Computer` certificate store, Security Manager uses the first valid certificate and ignores any additional certificates.
- You can configure agent computers to search other certificate stores and locations for certificates, if required by your PKI. For more information about configuring certificate stores, see "Customizing Certificate Usage" on page 322.
- If the agent is configured to use an authentication certificate and is unable to access the associated private key, the agent service fails to start and the agent computer generates an event 21334 in the Application event log.

To issue and install agent authentication certificates:

1. ***If you have not configured a certificate authority for your environment,*** establish a certificate authority (CA) to issue agent authentication certificates. Ensure your certificate authority can issue agent computer certificates that meet all authentication requirements. For more information about certificate requirements, see "Certificate Requirements" on page 314.

   Notes

   - If all agents and central computers are internal to your company, NetIQ recommends you use a local CA. If any Security Manager computers are hosted externally, you should purchase a commercial certificate.

   - You can use Microsoft Certificate Services or another CA to issue certificates, as configured in your environment.

2. Use your certificate authority to issue one or more agent computer certificates.

3. Install the agent computer certificate in the `NetIQ Security Manager` container of the `Local Computer` certificate store on the agent computer.

4. ***If the issuer certificate for the agent certificate is not already installed on the agent,*** install the issuer certificate in the `Trusted Root Certification Authorities` container of the `Local Computer` certificate store.

5. Repeat Steps **3** through **4** on each agent computer where you want to configure authentication.

6. ***If the issuer certificate for the agent certificate is not already installed on the central computer that monitors the agents you want to authenticate,*** install the issuer certificate in the `Trusted Root Certification Authorities` container of the `Local Computer` certificate store of the central computer.

Issuing and Installing Central Computer Authentication Certificates

If you want to configure authentication for Security Manager central computers, each central computer needs to present a trusted certificate to all monitored agent computers. You must install central computer certificates in the `LocalMachine > NetIQ Security Manager` certificate store on each central computer.

Central computer certificates should include the Server Authentication EKU, OID `1.3.6.1.5.5.7.3.1`, and must be trusted by all monitored agent computers. You can establish trust by placing all issuer certificates from the certificate chain of the central computer certificate in the `Trusted Root Certification Authorities` container of the `Local Computer` certificate store on each monitored agent computer.

Notes

- You can install the central computer authentication certificate by logging directly into the central computer using an account that is a member of the local Administrators group or by remotely deploying the certificate to one or more central computers, depending on your environment and PKI.
- If you have multiple certificates with the Server Authentication EKU stored in the `NetIQ Security Manager` container in the `Local Computer` certificate store, Security Manager uses the first valid certificate and ignores any additional certificates.
- You can configure central computers to search other certficate stores and locations for certificates, if required by your PKI. For more information about configuring certificate stores, see "Customizing Certificate Usage" on page 322.
- If you configure central computer authentication and do not establish trust with all monitored agents, your agents cannot communicate with the untrusted central computer.
- If you have enabled correlation in your environment, include both the Server Authentication EKU, OID `1.3.6.1.5.5.7.3.1`, and the Client Authentication EKU, OID `1.3.6.1.5.5.7.3.2`, in your central computer certificates. All Correlation servers must also trust all central computer certificates.

To issue and install central computer authentication certificates:

1. ***If you have not configured a certificate authority for your environment,*** establish a certificate authority (CA) to issue central computer authentication certificates. Ensure your certificate authority can issue agent computer certificates that meet all authentication requirements. For more information about certificate requirements, see "Certificate Requirements" on page 314.

   Note
   You can use Microsoft Certificate Services or another CA to issue certificates, as configured in your environment.

2. Use your certificate issuer to issue one or more central computer certificates.
3. Install the central computer certificate in the `NetIQ Security Manager` container of the `Local Computer` certificate store on the central computer.
4. ***If the issuer certificate for the central computer certificate is not already installed on the central computer,*** install the issuer certificate in the `Trusted Root Certification Authorities` container of the `Local Computer` certificate store.
5. Repeat Steps **2** through **4** on each central computer where you want to configure authentication.
6. ***If the issuer certificate for the central computer certificate is not already installed on the agent computer you want to authenticate the central computer,*** install the issuer certificate in the `Trusted Root Certification Authorities` container of the `Local Computer` certificate store of the agent computer.
7. Repeat Step **6** on each monitored agent computer.

Enabling Agent Authentication

After creating and installing a valid certificate on your agent computers and installing the issuer certificate for the agent computer on the monitoring central computer, you can enable agent authentication on the central computer by editing the registry.

If you enable agent authentication, you restrict your central computer to only be able to communicate with agents that present valid, trusted Client Authentication certificates.

To enable agent authentication on a central computers:

1. Log on to the central computer using an account that is a member of the local Administrators group.
2. Update the following registry entry using the Registry Editor:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\Security
   Manager\Configurations\ConfigurationGroupName\Operations\Consolida
   tor\RequirePeerCerts = 1
   ```

   Where *`ConfigurationGroupName`* is the name of your configuration group.

   Warning
   Be careful when editing your Windows Registry. If there is an error in your registry, your computer may become nonfunctional. If an error occurs, you can restore the registry to its state when you last successfully started your computer. For more information about editing the registry, see the Help for the Windows Registry Editor.

3. Open the Services Administrative Tool located in the Control Panel.
4. In the Services pane, click **NetIQ Security Manager**.
5. On the Action menu, click **Restart**.
6. After the service restarts, close the Services Administrative Tool.

Note
If you want to enable agent authentication on a central computer that has a 64-bit version of Microsoft Windows installed, update the following registry key using the Registry Editor:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NetIQ\Security
Manager\Configurations\ConfigurationGroupName\Operations\Consolidator
\RequirePeerCerts = 1
```

Enabling Central Computer Authentication

After creating and installing a valid certificate on your central computer and installing the issuer certificate for the central computer on all monitored agent computers, you can enable central computer authentication on your agents by editing the registry on each agent computer.

If you enable central computer authentication, you restrict your agent computers to only be able to communicate with a central computer that presents a valid, trusted Server Authentication certificate.

Note
If you have enabled correlation in your environment, central computers forward correlation events from agents to the Correlation server. You must configure all central computers that send correlation events in the same manner as an agent for central computer authentication.

To enable central computer authentication on an agent computer:

1. Log on to the agent computer using an account that is a member of the local Administrators group.
2. Update the following registry entry using the Registry Editor:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\NETIQ\Security
   Manager\Configurations\ConfigurationGroupName\Operations\Agent\Con
   solidator\RequirePeerCerts = 1
   ```

   Where *ConfigurationGroupName* is the name of your configuration group.

   Warning
   Be careful when editing your Windows Registry. If there is an error in your registry, your computer may become nonfunctional. If an error occurs, you can restore the registry to its state when you last successfully started your computer. For more information about editing the registry, see the Help for the Windows Registry Editor.

3. Open the Services Administrative Tool located in the Control Panel.
4. In the Services pane, click **NetIQ Security Manager**.

5. On the Action menu, click **Restart**.

6. After the service restarts, close the Services Administrative Tool.

7. Repeat Steps **1** through **6** on each agent computer.

Note
If you want to enable central computer authentication on a central computer that has a 64-bit version of Microsoft Windows installed, update the following registry key using the Registry Editor:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NETIQ\Security
Manager\Configurations\ConfigurationGroupName\Operations\Agent\Consol
idator\RequirePeerCerts = 1
```

Customizing Certificate Usage

Security Manager uses several registry values to configure the default certificate store location, certificate store name, certificate name, and names of trusted issuers. You can modify the following default registry values to configure how Security Manager finds agent and central computer authentication certificates.

The agent registry values are in the following location in the registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\Security
Manager\Configurations\ConfigurationGroupName\Operations\Agent\Consol
idators
```

Where *ConfigurationGroupName* is the name of your current configuration group.

The central computer registry values are in the following location in the registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\Security
Manager\Configurations\ConfigurationGroupName\Operations\Consolidator
```

Where *ConfigurationGroupName* is the name of your current configuration group.

Warning
Be careful when editing your Windows Registry. If there is an error in your registry, your computer may become nonfunctional. If an error occurs, you can restore the registry to its state when you last successfully started your computer. For more information about editing the registry, see the Help for the Windows Registry Editor.

Registry Value	Registry Data Type	Default Value Data	Definition
`CertificateStore Location`	String	`LocalMachine`	Specifies the location of the certificate store containing the agent or central computer authentication certificate. This property determines whether Security Manager searches the local computer, current user, or service-specific store to find Security Manager certificates. Possible values are `LocalMachine`, `CurrentUser`, or `Service:`*`ServiceName`*, where *`ServiceName`* is the name of the specific service.
`CertificateStore Name`	String	`NetIQ Security Manager`	Specifies the name of the certificate store containing the agent or central computer authentication certificate. Possible values are `NetIQ Security Manager`, `My`, `Root`, or *`CustomCertificateStoreName`*, where *`CustomCertificateStoreName`* is a customized certificate store you create.

Registry Value	**Registry Data Type**	**Default Value Data**	**Definition**
`CertificateSubjectName`	String	[EMPTY]	Specifies the subject distinguished name of the specific agent or central computer authentication certificate. If empty, the agent uses the first certificate found with a Client Authentication EKU, and the central computer uses the first certificate found with Server Authentication EKU.
RequirePeerCerts	DWORD	`0`	Specifies whether or not the computer is configured to establish trust for the certificate an agent or central computer presents, depending on the computer type, when trying to connect. If the computer is not configured to trust a certificate received from another computer, the computer cannot communicate with the other computer. For more information about enabling authentication, see “Enabling Agent Authentication” on page 319 and “Enabling Central Computer Authentication” on page 321.

Registry Value	Registry Data Type	Default Value Data	Definition
`TrustedIssuerSubjectNames`		[EMPTY]	Specifies a list of issuers Security Manager trusts. Security Manager uses this list when validating certificates. If you want to restrict Security Manager to only trust certificates issued by certain issuers, you can specify a semicolon-separated list of subject distinguished names for certificate issuers you want to trust. For example, if you want to only trust certificates issued by the `Security Manager Trusted Root` certification authority, specify `CN=NetIQ Security Manager Trusted Root`.

Verifying Authenticated Communication

You can examine the **Infrastructure Components > Agents** view in the Control Center to determine if any agents in your installation are not using authentication. Security Manager identifies the agents with an `Authentication Failed` status.

An `Authentication Failed` status requires attention but does not necessarily indicate a rogue computer. If you want more information about the `Authentication Failed` status for a computer, you can examine the **Agent Authentication Failures** and **Central Computer Authentication Failures** event views.

To verify authenticated communication:

1. Log on to the Control Center computer with a user account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see "Understanding Requirements and Permissions" on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. ***If you want to examine agent status,*** in the Navigation pane, click **Infrastructure Components > Agents**.
4. ***If you want to examine agent authentication failures,*** complete the following steps:
   1. In the Navigation pane, click **Event Views**.
   2. Expand **Security Views > Security Manager Self-monitoring > Agents**.
   3. Click **Agent Authentication Failures**.
5. ***If you want to examine central computer authentication failures,*** complete the following steps:
   1. In the Navigation pane, click **Event Views**.
   2. Expand **Security Views > Security Manager Self-monitoring > Central Computers**.
   3. Click **Central Computer Authentication Failures**.
6. Close the Control Center.

Troubleshooting Authentication Problems

If one or more agents and central computers cannot communicate, you may not have configured authentication correctly. If an agent or central computer does not present a certificate, presents an invalid certificate, or presents a certificate issued by an untrusted certificate issuer, Security Manager cannot enable authenticated communication.

An authentication error is not the only possible cause of faulty communication between an agent and a central computer. Other network, software, and hardware problems can also cause the failure of communication between agents and central computers. Before you attempt to correct authentication problems, verify that the communication problem is actually caused by an authentication error.

If the error was caused because a computer was offline when a certificate was presented, the central computer and agent computer automatically attempt to present certificates to one another, as applicable depending on your configuration, at the next communication attempt.

Verifying Authentication Certificates

After ruling out network, software, and hardware problems as the cause of faulty communication between one or more agents and central computers, ensure all agent and central computer authentication certificates are valid and are installed in the `NetIQ Security Manager` container of the `Local Computer` certificate store.

To verify an authentication certificate:

1. Log on to the agent or central computer using an account that is a member of the local Administrators group.
2. Start **Microsoft Management Console**.
3. On the File menu in the Console window, click **Add/Remove Snap-in**.
4. Click **Add**.
5. Select **Certificates**.
6. Click **Add**.
7. Select **Computer account**.
8. Click **Next**.
9. Select **Local computer (the computer this console is running on)**.
10. Click **Finish**.
11. Click **Close**.

12. Click **OK**.

13. On the File menu, click **Save**.

14. Specify a location on the computer for the `.msc` file and click **Save**.

15. In the left pane of the Console window, expand **Certificates (Local Computer) > NetIQ Security Manager**.

16. In the left pane, click **Certificates**.

17. ***If the Certificates folder is missing or does not contain an authentication certificate,*** issue and install a new agent or central computer authentication certificate.

    For more information about installing agent authentication certificates, see "Issuing and Installing Agent Authentication Certificates" on page 315. For more information about installing central computer authentication certificates, see "Issuing and Installing Central Computer Authentication Certificates" on page 318.

    Note
    By default, the `NetIQ Security Manager` container of the `Local Computer` certificate store on the central computer contains the self-signed certificate `NetIQ Security Manager Server`, which Security Manager uses to enable communication between the central computer and agents. This default certificate is not a Server Authentication certificate.

18. ***If the Certificates folder contains an authentication certificate,*** complete the following steps:

    a. In the right pane, double-click the authentication certificate.

    b. On the General tab, ensure the certificate details are correct and that the certificate has a corresponding private key.

    c. Click the Certification Path tab.

d. ***If the certificate status is `This certificate is OK`,*** click **OK**.

e. ***If the certificate status is not `This certificate is OK`,*** re-issue and install a new agent or central computer authentication certificate. For more information about installing agent authentication certificates, see “Issuing and Installing Agent Authentication Certificates” on page 315. For more information about installing central computer authentication certificates, see “Issuing and Installing Central Computer Authentication Certificates” on page 318.

19. Close the Microsoft Management Console.

Verifying Trust of the Certificate Issuer

If the authentication certificate installed on your agent or central computer is valid, ensure the computer to which the agent or central computer presents a certificate trusts the certificate issuer. The issuer certificate must be installed in the `Trusted Root Certification Authorities` container of the `Local Computer` certificate store on the authenticating computer.

To verify an authenticating computer trusts a certificate issuer:

1. Log on to the authenticating agent or central computer using an account that is a member of the local Administrators group.
2. Start **Microsoft Management Console**.
3. On the File menu in the Console window, click **Add/Remove Snap-in**.
4. Click **Add**.
5. Select **Certificates**.
6. Click **Add**.
7. Select **Computer account**.
8. Click **Next**.
9. Select **Local computer (the computer this console is running on)**.
10. Click **Finish**.

11. Click **Close**.

12. Click **OK**.

13. On the File menu, click **Save**.

14. Specify a location on the computer for the `.msc` file and click **Save**.

15. In the left pane of the Console window, expand **Certificates (Local Computer) > Trusted Root Certification Authorities**.

16. In the left pane, click **Certificates**.

17. ***If the Certificates folder does not contain the issuer certificate,*** install the certificate chain for the authentication certificate issuer in the `Trusted Root Certification Authorities` container.

18. ***If the Certificates folder contains the issuer certificate,*** complete the following steps:

    a. In the right pane, double-click the issuer certificate.

    b. On the General tab, ensure the issuer certificate details are correct.

    c. Click the Certification Path tab.

    d. ***If the certificate status is `This certificate is OK`,*** click **OK**.

    e. ***If the certificate status is not `This certificate is OK`,*** re-install the certificate chain for the authentication certificate issuer in the `Trusted Root Certification Authorities container`.

19. Close the Microsoft Management Console.

Using Security Manager with FIPS-Compliant Security Algorithms Enabled

Security Manager takes advantage of the Federal Information Processing Standards (FIPS)-compliant security features available in Microsoft Windows to allow you to further secure your environment.

You can enable FIPS-compliant security algorithms only when monitoring Windows agents using Security Manager version 6.5 or later. If you enable the `System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing` local security policy on your central computer, that central computer can no longer communicate with certain components of Security Manager:

- Legacy Windows agents (version 6.0 Service Pack 4 and earlier)
- UNIX agents
- iSeries agents

Security Manager does not support communication with legacy agents because the existing legacy agent communication protocol does not meet the requirements necessary to use the FIPS 140-2 Inside logo.

After you enable this setting, your central computer can communicate with Windows agents using only Security Manager 6.5 or later.

Notes

- If you want to use FIPS-compliant security algorithms, NetIQ recommends that you enable the FIPS-compliant local security policy on all domain controllers in your environment.
- If you enable FIPS-compliant security algorithms, the policy setting overrides the `Allow Legacy Agent Communication` setting configured in the Development Console on your central computer. Although the `Allow Legacy Agent Communication` option remains selected, legacy agents cannot communicate with the central computer.