Trial 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

Installing the Trial Version of Security Manager 23

Chapter 3

Exploring the User Interfaces 45

Chapter 4

Exploring Security Manager 65

About This Book and the Library

The trial guide provides information to help you install the trial version and explore the NetIQ Security Manager product (Security Manager).

Intended Audience

This book provides information for individuals responsible for understanding Security Manager concepts and evaluating the product for use in a production environment.

Other Information in the Library

The product library provides the following additional information resources:

Installation Guide
Provides detailed planning and installation information.

User Guide
Provides concepts and tasks to help user understand and use the product.

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

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

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

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

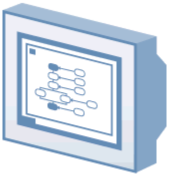
Security Manager includes a number of software components that you can distribute and install as needed to meet your security management objectives and environment.

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.

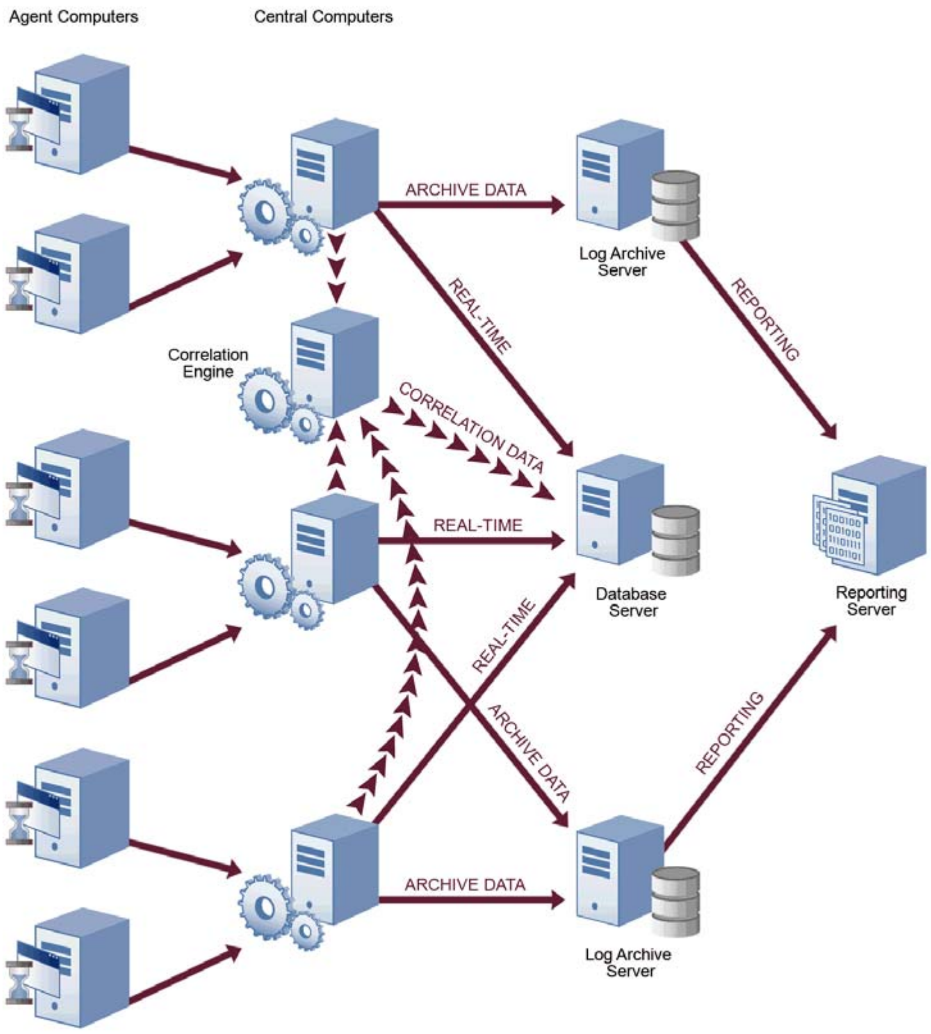
A choice of configuration options is especially important in large distributed enterprises or when communicating over slower network links, such as WANs. In some environments, you may want to optimize load balancing and performance by installing multiple configuration groups.

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:

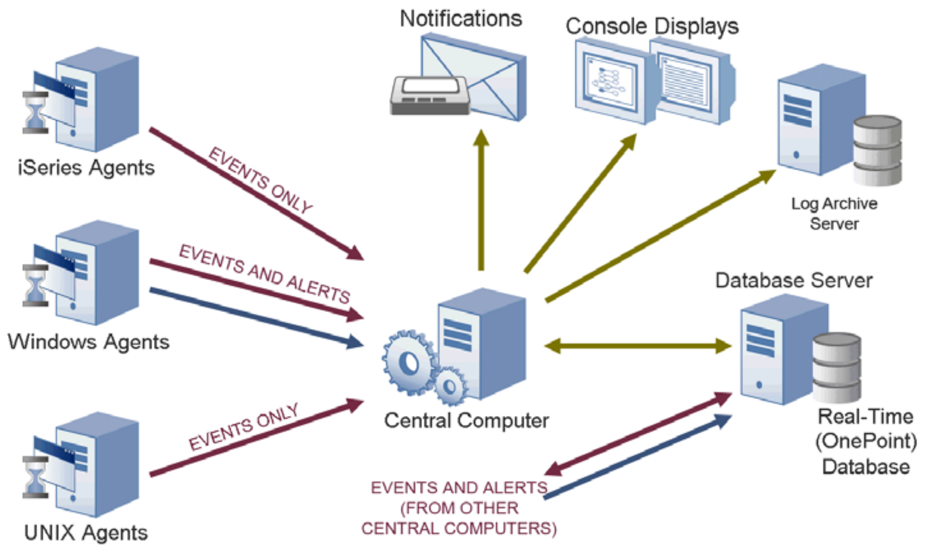
- Inform you about the current state of security (real-time alerts and events)
- Identify events indicating complex threats (correlated real-time events)
- Research significant historical security incidents (log data)
- Understand current security and trends (reporting data)

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.

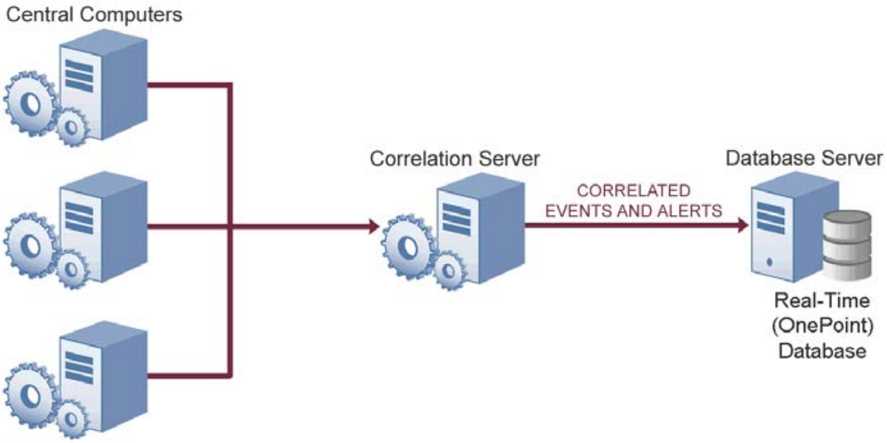
The central computers also send alert and event data to the log archive server for storage in the log archive. You can manage the automatic grooming settings for the log archive from the Log Archive Configuration utility.

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.

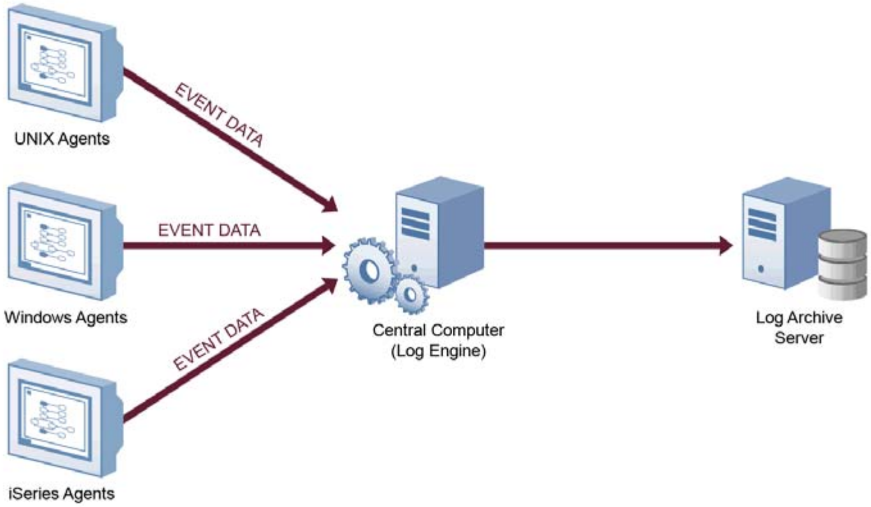


A **correlation rule** is a set of criteria that configures Security Manager to detect a pattern of real-time events and respond accordingly. The Correlation server evaluates collected alerts and events against the correlation rules as data arrives. When a rule match occurs, the Correlation server responds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



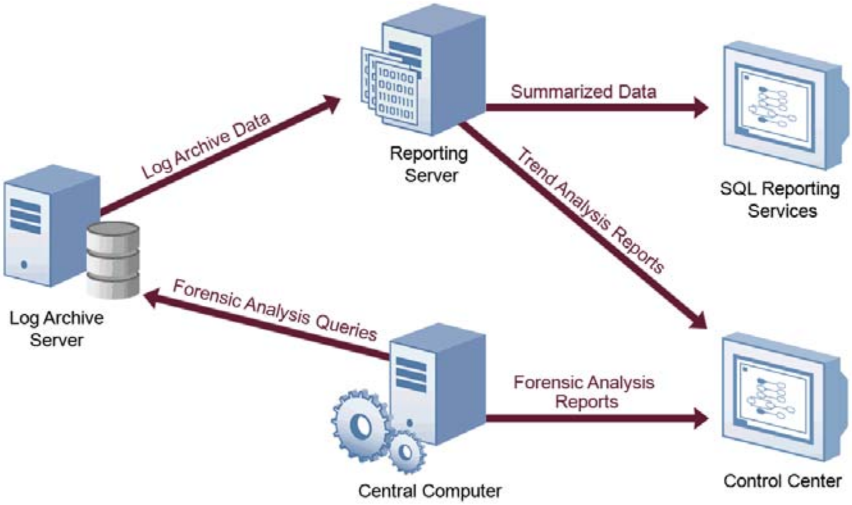
The Log Engine receives the event data and sends it to a log archive for storage. Each central computer receives only a portion of the log data, so the Log Engine on each central computer transfers its portion to a log archive on a dedicated log archive server.

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

Installing the Trial Version of Security Manager

The following sections guide you through a trial installation of Security Manager so you can explore the features and benefits of using the product to monitor Windows computers. Even though Security Manager supports other versions of Microsoft Windows Server and Microsoft SQL Server, this guide illustrates using the product only for computers using Windows Server 2003 and Microsoft SQL Server 2005.

Why You Should Evaluate Security Manager

The trial version of Security Manager lets you quickly install and run the fully functional product, monitoring up to 10 computers and devices for 30 days. When you complete the evaluation process, you should understand the basics of how to use Security Manager to meet your security event management needs. You should also be familiar with many of the significant benefits Security Manager offers you, your staff, and your organization.

If you have additional questions during or after your evaluation or if you need to evaluate the product for a longer period to conduct a pilot study, contact your NetIQ sales or support representatives.

The trial guide does not provide a tour of the product using UNIX computers or iSeries servers, but the trial version of the product does allow you to evaluate support for these platforms.

For more information about installing Security Manager with UNIX computers or iSeries servers, see the NetIQ UNIX Agent documentation and NetIQ Security Solutions for iSeries documentation, respectively.

The remaining chapters in this book guide you through installing and evaluating Security Manager. By following the steps in this book, you can quickly install the product and immediately begin seeing the benefits of using the product. The guided tour can help you explore many important product features.

Selecting an Evaluation Computer

Security Manager can be installed in various configurations. A production setting typically includes at least one central computer, one database server, one log archive server, and one reporting server. To make it easier to evaluate the product, the trial installation places all product components on one Windows computer, referred to as the **evaluation computer**.

The evaluation computer serves as a central computer, database server, log archive server, reporting server, and monitored computer. For more information about installing Security Manager in a production environment, see the *Installation Guide for NetIQ Security Manager.*

Because the evaluation computer plays several roles during evaluation, select a computer with adequate resources to act as central computer, database server, log archive server, reporting server, and monitored computer. Before you begin installing Security Manager, review the “Trial Installation Checklist” on page 25. Complete the steps in order for best results.

Trial Installation Checklist

Complete each of the following tasks to select an evaluation computer, install prerequisite software, install the product, and prepare for the guided tours.

The following checklist helps you track each task as you complete it and provides a reference to the detailed steps for each task.

☑	**Preparation Checklist**
□	**1.** Verify your computers meet the requirements for the trial installation and evaluation tours. For more information about computer requirements, see "Verifying Computer Requirements" on page 26.
□	**2.** Create the administrator and service accounts Security Manager needs to operate and create an email account to send email alert notifications. For more information about creating accounts, see "Creating User, Service, and Email Accounts" on page 31.
□	**3.** Install the software Security Manager requires on the evaluation computer. For more information about installing prerequisites, see "Installing Prerequisite Software" on page 33.
□	**4.** Install Security Manager on the evaluation computer. For more information about installing Security Manager, see "Installing and Starting Security Manager" on page 34.
□	**5.** Deploy Windows agents for Security Manager to monitor during the evaluation. For more information about deploying agents, see "Deploying Security Manager Agents" on page 36.
□	**6.** Install NetIQ Change Guardian for Windows on the evaluation computer. Change Guardian for Windows allows you to actively generate events and alerts in Security Manager by simulating unauthorized changes. For more information about installing Change Guardian for Windows, see "Installing Change Guardian for Windows" on page 37.
□	**7.** Prepare for the guided tour by performing configuration steps. For more information about configuration options, see "Configuring Security Manager" on page 38.

Verifying Computer Requirements

The following sections identify the requirements for the evaluation computer and computers you plan to monitor.

Evaluation Computer System Requirements

Security Manager operates in a Windows domain environment and must have access to a domain controller. If you are installing Security Manager in a test environment, ensure the domain is properly configured before you begin installing the product. The following table lists the suggested system requirements for the Windows evaluation computer.

Category	Requirement
Operating System	Microsoft Windows Server 2003 Service Pack 2 (including 64-bit version).
Processor	2.0 GHz Intel Pentium 4 minimum, 3.0 GHz or faster recommended.
Disk Space	20 GB or more free space (2 GB minimum for databases).
Memory	2 GB minimum, 4 GB recommended.
Display	1024 x 768 resolution or higher.
Access to Domain Controller	Access to a domain controller (DC) in the domain.

Evaluation Computer Software Requirements

If prerequisite software is not already installed on the evaluation computer, the setup program can automatically install some software when you install Security Manager. If you install the software before running the Security Manager setup program, you may be able to avoid the interruption of a system restart.

Security Manager requires you to have the following software installed on the evaluation computer before you run the setup program:

Software	Comments
Microsoft SQL Server 2005 with Service Pack 3, Standard or Enterprise Edition	Because the computer also acts as the database server and reporting server during evaluation, install Microsoft SQL Server on the evaluation computer before installing Security Manager. The trial version requires you to install Security Manager using the default instance of Microsoft SQL Server. For production, you can install Security Manager to a named instance of Microsoft SQL Server.
Microsoft SQL Server 2005 Analysis Services with Service Pack 3	Analysis Services is a component of Microsoft SQL Server Enterprise, Standard, Developer, Personal, and Enterprise Evaluation Editions. Install Analysis Services components when you install Microsoft SQL Server. Analysis Services is required by the Security Manager reporting server component. **Note:** When installing Analysis Services on the reporting server, select the **Decision support objects** option and specify the same service account for Analysis Services as the service account used by the reporting server. You specify the reporting server service account in the Security Manager setup program.
Microsoft SQL Server 2005 Database Services	Integration Services is a component of Microsoft SQL Server. Install Database Services components when you install Microsoft SQL Server. Database Services is required by the Security Manager database and reporting servers.
Microsoft SQL Server 2005 Analysis Services with Service Pack 3	Analysis Services is a component of Microsoft SQL Server. Install Analysis Services components when you install Microsoft SQL Server. Analysis Services is required by the Security Manager reporting server.
Microsoft SQL Server 2005 Integration Services (SSIS)	Integration Services is a component of Microsoft SQL Server. Install Integration Services components when you install Microsoft SQL Server. Integration Services is required by the Security Manager reporting server.

Software	Comments
Microsoft SQL Server 2005 Reporting Services (SSRS)	Reporting Services is a component of Microsoft SQL Server. Install Reporting Services components when you install Microsoft SQL Server. Reporting Services is required by the Security Manager reporting server.
Microsoft Message Queuing (MSMQ) 3.0 (at least 8 GB)	The log archive uses this component to receive event data from the central computer.
.NET Framework 4.0	The setup program requires this component to install Security Manager.
Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package	The setup program requires this component to install Security Manager.
Network COM+ access for the Application Server	The setup program requires this component to install Security Manager.
Microsoft Core XML Services (MSXML) 6.0	The central computer requires this component to parse data properly.
Microsoft Office 2003 Web Components (Office Web Components 11)	This component provides tools Security Manager uses to publish and display charts.
Microsoft SQL Server 2005 Analysis Services 9.0 OLE DB Provider	The Control Center requires this component to help display Trend Analysis reports. You can download this component from the Feature Pack for Microsoft SQL Server 2005, located at www.microsoft.com.
Microsoft ADOMD.NET	The Control Center requires this component to help display Trend Analysis reports.
Microsoft Internet Information Services (IIS) 5.0	The Security Manager Web Console requires Microsoft IIS. The Security Manager setup program automatically configures Microsoft IIS to allow Active Server Pages and Server Side Includes. In a production setting, you need to install IIS only on one central computer you designate as the Web Console server.

Software	Comments
Microsoft Server Support Tools	The log archive server requires components included in the Microsoft Server Support Tools package to enable communication with other servers.

To ensure the evaluation computer has the required software, Security Manager provides a Verify Prerequisites tool. For more information about running the Verify Prerequisites tool, see "Installing Prerequisite Software" on page 33.

Monitored Computer Requirements

The requirements for monitored computers are the same for both the trial and production installations of the product. For evaluation purposes, you can monitor up to 10 computers and devices, including the evaluation computer. If you want to monitor more than 10 computers or devices, contact your NetIQ sales representative.

The following table outlines the minimum requirements for monitored Windows computers for evaluation.

Category	Requirement
Operating System	• Windows 7 (32- or 64-bit) • Windows Server 2008 R2 • Windows Server 2008 R2 Server Core • Windows Server 2008 (32- or 64-bit) • Windows Server 2008 Server Core (32- or 64-bit) • Windows Server 2003 R2 (32- or 64-bit) • Windows Vista (32- or 64-bit) • Windows Server 2003 (32- or 64-bit) • Windows XP (32- or 64-bit) • Windows 2000
Processor	500 MHz Intel Pentium minimum.
Disk Space	100 MB disk space.

Category	Requirement
Memory	40 MB minimum. The amount of memory usage varies and depends on the modules you have installed and the products you are monitoring. For more information about memory requirements, see the module documentation.
Network Access	• All Security Manager components must be in domains that trust each other. • All Security Manager components must be installed on computers with either Internet Protocol version 4 (IPv4) installed and enabled or both IPv4 and Internet Protocol version 6 (IPv6) installed and enabled.
Additional Requirements	• Any computer on which you want to install a managed or unmanaged agent must have a NetBIOS-compliant name. • On each agent computer you scan for viruses, configure your antivirus software to exclude the `\Application Data\NetIQ` folder for each Windows user profile and all `*.dat` files in the *`installation folder`*`\NetIQ Security Manager\OnePoint` folder, where *`installation folder`* is the location where you installed the agent. • On each Windows Server 2008 agent computer you scan for viruses, configure your antivirus software to exclude the `ProgramData\NetIQ` folder and all `*.dat` files in the *`installation folder`*`\NetIQ Security Manager\OnePoint` folder, where *`installation folder`* is the location where you installed the agent. • For more information about additional module-specific requirements, see the documentation for your installed modules.

Note

NetIQ recommends installing the latest Microsoft Windows service packs and hotfixes on all computers before installing Security Manager components.

For more information about UNIX or iSeries computer requirements, see the NetIQ UNIX Agent documentation and NetIQ Security Solutions for iSeries documentation, respectively. For more information about monitoring UNIX computers, iSeries servers, firewalls, IDS systems, routers, switches, or other products, see the corresponding module documentation.

Creating User, Service, and Email Accounts

Before you start installing the product, create the accounts Security Manager requires during and after installation. Create the following user, service, and email accounts using the tools of your choice:

Administrator account

When you install Security Manager, your logon account must be a member of the local Administrators group on the evaluation computer.

Service account

Create a user account for Security Manager to use as a service account to log on to Windows. Because you must specify the account during installation, create the service account before installing Security Manager. For more information about creating a service account for Security Manager, see "Creating a Service Account" on page 31.

Email accounts

Create an email account for Security Manager to use to send notifications of important activity. Also ensure email accounts exist for any users who will receive email notifications from Security Manager. Security Manager supports both Microsoft Exchange and SMTP email notification. For more information about creating email accounts, see "Creating Email Accounts" on page 32.

Creating a Service Account

Follow these steps to create a service account for Security Manager to use to log on, operate, and monitor computers. When you install Security Manager, the setup program prompts you for the account name and password.

To create a service account for Security Manager:

1. Create a domain user account as a service account for Security Manager. For the evaluation, choose an account name such as `SMEvalAccount`. Ensure the account has a non-blank password.
2. Add the account to the local Administrators group on the evaluation computer.
3. Ensure the account is a member of the System Administrators server role. By default, all members of the local Administrators group are included in the System Administrators server role.
4. Add the account to the local Administrators group on all computers you want to monitor. For example, if you include the Domain Admins global group as a member of each local Administrators group, add the `SMEvalAccount` to the Domain Admins global group.

The Security Manager setup program adds the following user rights to your new service account:

- Act as part of the operating system
- Create a token object
- Log on as a batch job
- Log on as a service

Creating Email Accounts

You can use Microsoft Exchange or SMTP mail for email notification. For more information about creating mailboxes, see the Microsoft Exchange or SMTP documentation. Collect information for the following items:

Security Manager Notification Mailbox

Security Manager uses this dedicated mailbox to send notifications to operators. Store the mailbox on the email server so the mailbox is accessible from the central computer. For example, create a mailbox with an email address of `SMNotifier@yourcompany.com`.

Operator Email Accounts

Operators can receive notifications from Security Manager by email. For this evaluation, you can use your own email account. You can also configure additional email accounts to receive Security Manager notifications. Configure these accounts as you would for an administrator who would respond to Security Manager alert notifications.

Text Pagers

Security Manager can also send text to text-capable pagers. To configure Security Manager to send text messages to pagers, make a note of the text pager address. For example, your pager address may be similar to `securitypager123@pager.com`.

Installing Prerequisite Software

Complete all prior preparation steps before you continue. For more information about preparing to install Security Manager, see the "Trial Installation Checklist" on page 25.

Security Manager makes use of other software components. The Security Manager setup program provides a link to the Verify Prerequisites tool that can check for and help you install the required software. Before installing Security Manager, run the Verify Prerequisites tool and install any appropriate prerequisites.

To check for prerequisite software on the evaluation computer:

1. Log on to the evaluation computer with the Administrator account you established.
2. Close all open programs.
3. Run the setup program from the Security Manager product installation kit.
4. Click the Trial Setup tab.
5. Click **Verify Prerequisites**.
6. Read the Welcome page and then click **Next**.

7. Follow the instructions until you have installed all the necessary prerequisites for the desired installation type. You can install some of the required software from the Verify Prerequisites tool. If you do not install the items required for full functionality, some parts of the product may not run. Click the links to read additional information about each requirement.
8. When you finish installing prerequisites, click **Next**.
9. Click **Finish**.

Installing and Starting Security Manager

When you run the setup program, Security Manager installs all product components on one computer. You can also configure up to nine additional computers or devices to monitor.

Be sure you have completed all prior preparation steps before you continue. For more information about preparing to install Security Manager, see “Trial Installation Checklist” on page 25.

Installing Security Manager

The following task continues from the last step in “Installing Prerequisite Software” on page 33.

To install the trial version of Security Manager:

1. Log on to the evaluation computer with the Administrator account you established.
2. Close all open programs.
3. Run the setup program from the Security Manager installation kit.
4. Click **Begin Trial Setup** on the Trial Setup tab.
5. Follow the instructions in the setup program until you finish installation.

6. Review the information on the Installation Summary window.

   Note
   Depending on the processing speed of the evaluation computer, installation can take some time.

7. Click **Launch Module Importer**.
8. Follow the instructions in the module installer.
9. Click **Finish**.
10. Click **Close**.
11. Click **Finish** to exit the setup program.
12. Follow the instructions in the Reporting setup program until you finish installation.
13. Click **Finish**.
14. ***If you are prompted to restart the computer,*** click **OK**. After the computer restarts, log on to the evaluation computer with the Administrator account you established.
15. ***If the setup window is still open***, you can review the documentation and explore the other options. When you are finished, close the window.

Starting Security Manager

After you install the product, you can start the Control Center by clicking **Security Manager Control Center** in the NetIQ Security Manager program group.

You can also start the Control Center and several other user interfaces from the Alert Sentry when the Alert Sentry is active.

Deploying Security Manager Agents

For the evaluation, you can deploy agents to additional computers. The evaluation guided tour provides information for using Windows agents. For more information about monitoring UNIX or iSeries, see the *Installation Guide for NetIQ Security Manager*.

- ***If you want to monitor additional Windows computers during the evaluation,*** complete the following task by running the Agent Administrator.
- ***If you do not want to monitor computers other than the evaluation computer***, skip to "Configuring Security Manager" on page 38.

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. For more information about required service account permissions, see "Creating a Service Account" on page 31.

To deploy agents using the Agent Administrator:

1. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
2. In the Navigation pane, click **All Folders**.
3. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.
4. In the Agent Administrator window, click the Managed Agents tab.
5. Click **Deploy Agents**.
6. Click **Add > Add a Computer**.
7. Specify the domain and name of the computer you want to monitor.
8. Click **OK**.
9. Click **Approve and deploy during next scan** and select **Deploy now**.
10. Repeat Steps **6** through **9** for each computer you want to monitor.

11. Click **OK**.

12. Click **Close**.

Installing Change Guardian for Windows

After installing Security Manager, you should also install the trial version of the NetIQ Change Guardian for Windows product. Change Guardian for Windows provides real-time change monitoring for Security Manager and can detect unauthorized changes to computer settings and automatically respond.

You must use the Configuration Wizard to enable the default NetIQ filter group before Change Guardian for Windows can monitor your trial environment. For more information about enabling the NetIQ filter group, see "Configuring Change Guardian for Windows" on page 41.

For the purposes of this trial, you will use Change Guardian for Windows to trigger events and alerts in Security Manager and review the Security Manager response to those events and alerts. For more information about triggering events and alerts using Change Guardian for Windows, see "Receiving and Managing an Alert" on page 66.

For more information about Change Guardian for Windows, see the *NetIQ Change Guardian for Windows User Guide*.

To install the trial version of Change Guardian for Windows:

1. Log on to the evaluation computer with the Administrator account you established.

2. Close all open programs.

3. Download the trial version of the Change Guardian for Windows product from the NetIQ Web site at `www.netiq.com/products/cgw/default.asp`.

4. Run the setup program from the Change Guardian for Windows installation kit.

5. Click **Begin Production Setup** on the Setup tab.

6. Follow the instructions in the setup program until you finish installation. Specify the same service account you used for the main Security Manager installation.

7. Clear **Start the Change Guardian for Windows Configuration Wizard**.
8. Click **Finish**.
9. ***If the setup window is still open***, you can review the documentation. When you are finished, close the window.

Configuring Security Manager

Security Manager provides default settings for most monitoring tasks. However, to implement some features, Security Manager needs additional information. For example, to enable Security Manager to notify you of new alerts by email, you must provide the name of the recipient mailbox and your email server.

Security Manager lets you run the Configuration Wizard to enable, change, or customize many product features. For the evaluation, run the Configuration Wizard to configure the following features:

- Identify email server and Security Manager mailbox information
- Enable Windows security auditing for all Windows agent computers

In addition to the Configuration Wizard, you will use the Configuration snap-in from the Development Console to create operator names, associate each name with an email address, and add the operators to a Security Manager notification group.

Configuring Reporting

After you install the evaluation version of Security Manager, use the Log Archive Configuration utility to modify the data upload interval to receive data more frequently than the default setting of 60 minutes. Using the Log Archive Configuration utility, you can configure the log archive to send data to the cube depot every 10 minutes.

To modify the default upload interval setting:

1. Start **Log Archive Configuration** in the NetIQ Security Manager > Configuration program group.
2. In the left pane, click **Log Archive Server Settings**.
3. Under **Reporting**, select **Reporting Server Name** and type the name of the Security Manager evaluation computer.
4. Select **Summarized Data Upload Interval** and type `5`. After data is uploaded to the reporting cube and you explore the Trend Analysis reports, you can change this setting back to the default of `60`.
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**.

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

Configuring Email Settings

When you run the Configuration Wizard, start by configuring the email server and accounts in the Global Settings.

To configure an email server and email account for Security Manager:

1. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
2. In the Navigation pane, click **All Folders**.
3. On the Tasks menu, click **Global Tasks > Launch Configuration Wizard**.

4. In the left pane, click **Global Settings**.
5. In the right pane, click **Configure Global Settings**.
6. Specify the SMTP server name.
7. Specify the mailbox you set up as the Security Manager notifier mailbox, such as *`SMNotify@yourcompany.com`*. For more information about setting up an email account, see “Creating Email Accounts” on page 32.
8. Specify or confirm the SMTP port number.
9. Click **Finish**.
10. Select **Apply configuration changes now**, and then click **OK**.
11. Click **OK**.

Leave the Configuration Wizard window open for additional configuration steps.

Configuring Auditing and Log Sizes

To enable Security Manager to collect events and monitor computers, you must enable auditing on the Windows computers you want to monitor. You should also consider modifying the log size settings. The Configuration Wizard supplies instructions for performing these tasks.

In the left pane, click **Support for Operating Systems**, and then click **Configure Security Manager to archive Windows logs**. Follow the steps in the Configuration Wizard to audit events and modify the event log sizes. When finished, leave the Configuration Wizard open for additional configuration steps.

Notes

- For this evaluation, ensure you enable success and failure auditing for all policies except `Audit object access`, which can generate an excessive number of events.
- For this evaluation, ensure you configure the event logs to overwrite events as needed or increase the maximum log size.

Configuring Change Guardian for Windows

After you install Change Guardian for Windows, you must enable the NetIQ Default Filters filter group to be able to monitor important changes using Security Manager.

To enable Change Guardian monitoring:

1. In the left pane of the wizard, click **Change Guardian**.
2. In the right pane, click **Configure Change Guardian for Windows Filters**.
3. In the left pane of the Change Guardian For Windows Filter Configuration window, click **Change Guardian for Windows > Filter Groups > NetIQ Default Filters**.
4. In the right pane, select **Enable this filter group**.
5. Click **Finish**.
6. Select **Apply configuration changes now**, and then click **OK**.
7. Click **OK**.

Leave the Configuration Wizard window open for additional configuration steps.

Filtering a Specific Process in Change Guardian for Windows

To demonstrate some Security Manager features in the guided tour, create a new Change Guardian for Windows filter group to generate a Security Manager alert when a user runs the `ftp.exe` process.

To create a filter group for `ftp.exe` using the Configuration Wizard:

1. In the left pane of the wizard, click **Change Guardian**.
2. In the right pane, click **Configure Change Guardian for Windows Filters**.
3. In the right pane of the Change Guardian For Windows Filter Configuration window, click **Create a New Filter Group**.
4. On the General tab, specify a name and description for the new filter group.

5. Click the Processes tab and click **New**.
6. Specify a filter description.
7. In the Objects field, type `ftp.exe`.
8. Select **Process Started**.
9. Select **Process Terminated**.
10. Select **Alert with severity level**.
11. In the Alert with severity level menu, select **Security Breach**.
12. Click **OK**.
13. Click **Finish**.
14. Select **Apply configuration changes now**, and then click **OK**.
15. Click **OK**.
16. Close the Configuration Wizard.

Note
To remove this process from the list after evaluation, rerun the Configuration Wizard and disable or remove the filter group containing the `ftp.exe` process filter.

Configuring Notification Groups

Security Manager can automatically notify security personnel of specified alerts by sending email, a text page, or a command. To configure Security Manager to send notifications, add one or more operators to the Network Administrators notification group.

To add operators to the Network Administrators notification group:

1. Start the Development Console in the NetIQ Security Manager program group folder.
2. In the left pane of the Development Console, expand **Security Manager Development Console > Configuration**.

3. Click **Notification Groups**.
4. In the right pane, select the **Network Administrators** notification group.
5. On the **Action** menu, click **Properties**.
6. Click **New Operator**.
7. In the **Name** field, type an operator name. For evaluation, you can use your own name.
8. Ensure that **Enabled** is selected and click **Next**
9. In the **Email Address** field, type an email address. For evaluation, you can use your own email address.
10. ***If you want to receive email only at scheduled times,*** click **Email this operator at the specified times** and specify the schedule.
11. Click **Next**.
12. Complete the wizard pages for text paging and external command notification as desired. When complete, click **Finish**.
13. In the **Available Operators** list, select an operator name.
14. Click the right arrow to add the operator to the Network Administrators notification group.
15. ***If you want to create additional operators and add them to the notification group***, repeat Steps **6** through **14**.
16. When you have finished adding operators, click **OK**.

Verifying Central Computer and Windows Agent Status

Check to ensure the central computer and Windows agents are up and running.

To verify the status of the central computer and Windows agents:

1. In the Navigation pane of the Control Center, click **All Folders** and expand **Infrastructure Components**.
2. Click **Central Computers**.
3. In the Results window, verify the central computer status is **Running**.
4. In the Navigation pane, click **Agents**.
5. In the Results window, verify the Windows agent status is **Running**.

Installing Additional User Interfaces

The Trial installation option installs all user interfaces on the evaluation computer. In production installations, Security Manager provides the option to install user interfaces on additional computers. Depending on which user interfaces you want to use, the computers may require network access to the central computer, database server, log archive server, reporting server, and Web Console server.

Security Manager user interfaces support most computers running Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, and Windows Server 2008. For more information about computer requirements and the user interface installation process, see the *Installation Guide for NetIQ Security Manager*.

Chapter 3

Exploring the User Interfaces

Security Manager provides several user interfaces that you can distribute to security personnel according to their job functions. Having this variety of user interfaces let you easily access and view the event data, alerts, rules, and product features in ways that make sense to you. The setup program installs all the following Security Manager interfaces when you select the trial installation:

- Security Manager Control Center
- Security Manager Development Console
- Security Manager Web Console

When you install Security Manager, the setup program creates security groups to control access to each interface. The trial installation process places the installer's logon account in each group automatically. In normal operations, a person administering Security Manager can provide access to a particular interface by adding user accounts to the proper Security Manager group. For more information about controlling access using Security Manager groups, see the *User Guide for NetIQ Security Manager*.

The following sections provide a brief tour of the user interfaces. For more information about using the Development Console, see the *Programming Guide for NetIQ Security Manager*. For more information about using the other user interfaces, see the *User Guide for NetIQ Security Manager* or the Help.

Exploring the Control Center

The Control Center allows you to monitor and resolve alerts about real-time events. The Control Center also allows you to create, view, and print Trend Analysis and Forensic Analysis reports of archived log data.

The Control Center is designed for security analysts who need to examine and resolve alerts for multiple configuration groups, as well as users who need to query the log archive for forensic analysis and interactively view aggregated log data in Trend Analysis graphs.

You can access different product features from the Control Center depending on your Security Manager group membership. The following table lists a sampling of the roles you can perform when you are a member of different Security Manager groups.

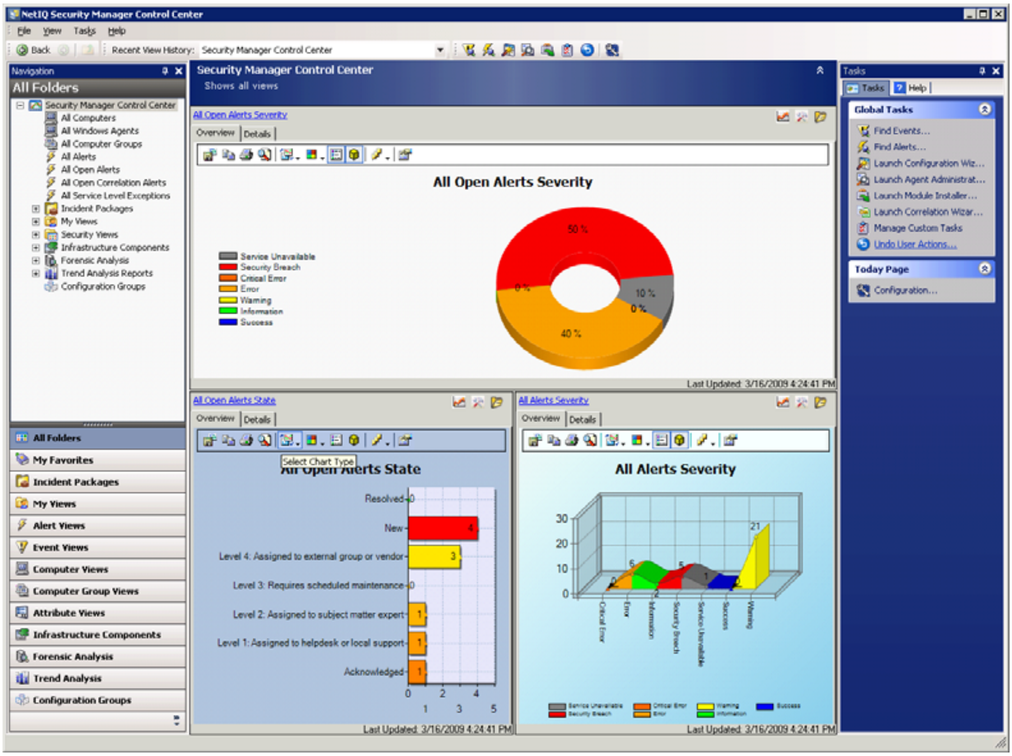
Task	Group Membership
Launching the Configuration Wizard	OnePointOp ConfgAdms
Creating a processing rule from an existing alert or event	OnePointOp Operators
Viewing the processing rule that generated a specific alert	OnePointOp Operators
Suspending an alert	OnePointOp Operators
Correlating events or 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

You can start the Control Center by clicking **Security Manager Control Center** in the NetIQ Security Manager program group.

Understanding the 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 graphs and charts are customizable and pull data directly from any alert view you specify.

The following figure illustrates the Control Center Today Page.



Understanding the Navigation Pane

The Navigation pane displays various common views and folders, such as All Alerts, Forensic Analysis, and Configuration Groups. Select or expand a folder or view to display the details of the folder or view in the Results window. At the bottom of the Navigation pane are several shortcut buttons you can use to go directly to a specific part of the Control Center. The Navigation pane can be moved anywhere within the Control Center window and then restored to its default position.

Understanding the Results Window

The Results window displays the objects contained in each folder or view, including alerts, incident packages, and reports, in list format.

On some windows or views, the lower pane of the Results window displays additional information for alerts, events, or reports. Select a tab to view details, such as Alert Description, Source Events, or Incident Package. You can also use the lower pane to save knowledge about a particular alert to your own company knowledge base. Sharing information about resolving alerts can assist others later if the alert occurs again.

The Auto Preview feature displays a brief description of each alert. Show or hide descriptions by clicking **Toggle Preview** on the Tasks menu. Hiding descriptions lets you see more alerts. Showing descriptions lets you see more detail about each alert.

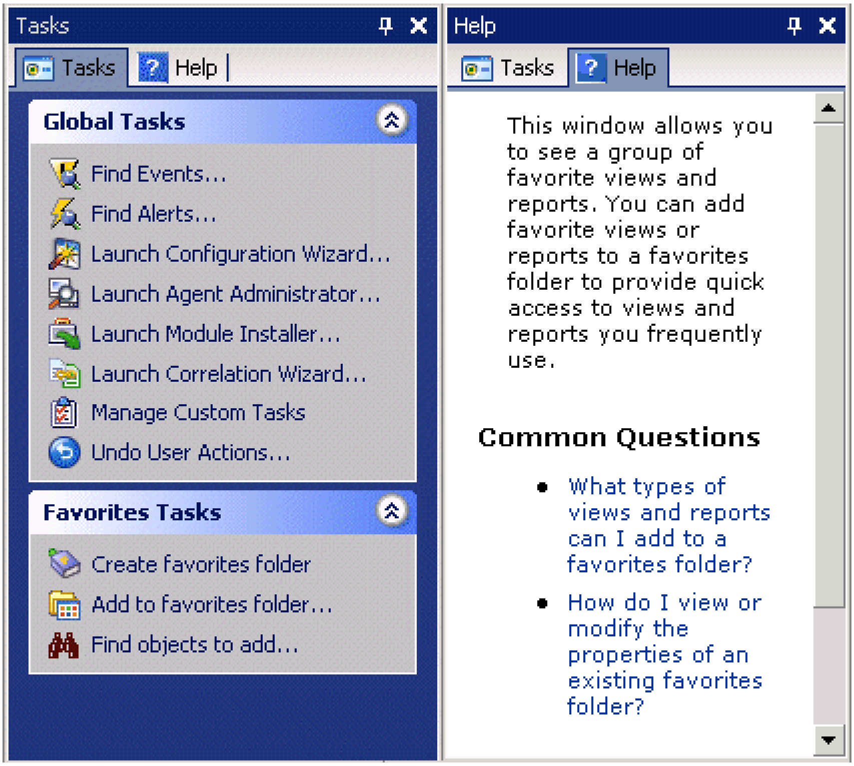
You can also show or hide columns as necessary using the column chooser, drag and drop columns to reorganize the view, and group or sort columns to filter the alert or event data displayed.

Understanding the Tasks/Help Pane

You can access tasks for each view or folder in the Tasks pane. Tasks are also included on the Tasks menu and as icons in the toolbar. To view Help for any view or window, click the Help tab in the Tasks pane. The Tasks pane can be moved anywhere within the Control Center window and then restored to its default position.

The Tasks pane contains global tasks you can access from any view in the Control Center. Global tasks include finding events or alerts, undoing user actions, and managing custom tasks. In addition, the Tasks pane includes shortcuts to wizards and utilities that can help you configure and begin using Security Manager, like the **Agent Administrator**, **Configuration Wizard**, and **Module Installer**.

The following figure illustrates the Tasks/Help pane.



This window allows you to see a group of favorite views and reports. You can add favorite views or reports to a favorites folder to provide quick access to views and reports you frequently use.

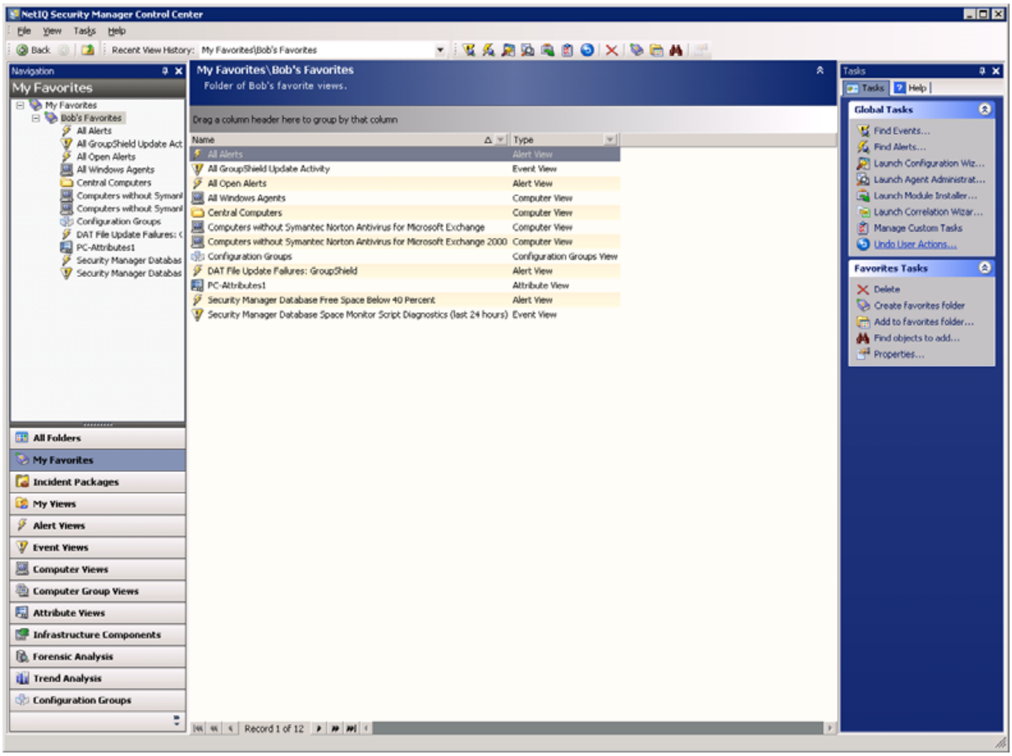
Common Questions

- What types of views and reports can I add to a favorites folder?
- How do I view or modify the properties of an existing favorites folder?

Understanding My Favorites

The My Favorites view lets you save your most frequently used Security Manager views and reports, including incident packages, alerts views, and more. This view acts as your personal, organizable work space.

The following figure illustrates the My Favorites view.

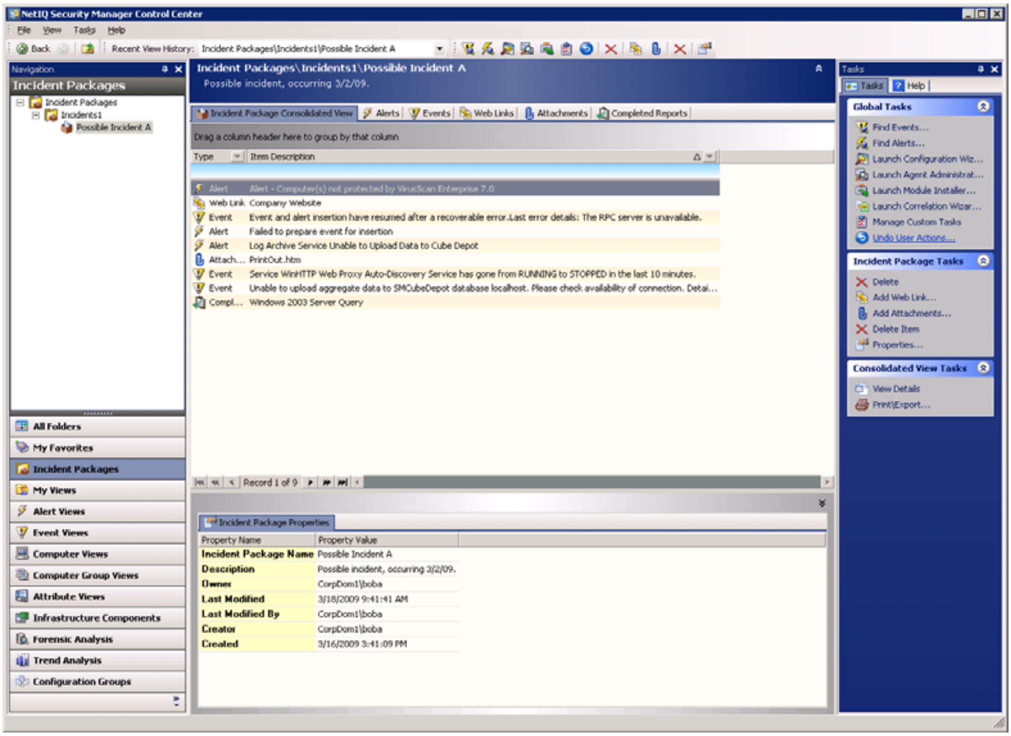


Name	Type
All Alerts	Alert View
All GroupShield Update Activity	Event View
All Open Alerts	Alert View
All Windows Agents	Computer View
Central Computers	Computer View
Computers without Symantec Norton Antivirus for Microsoft Exchange	Computer View
Computers without Symantec Norton Antivirus for Microsoft 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

Understanding Incident Packages

Incident packages are collections of all relevant information relating to a particular incident, including alerts, events, attachments, Forensic Analysis reports, and Web links. You can use incident packages to investigate possible security threats, research your overall security posture, and share information on incidents with others, storing the packages indefinitely in Security Manager. Drag and drop alerts, reports, and other items onto the Incident Package Drop Box to attach those items to an incident package.

The following figure illustrates the Incident Packages view.



Incident Packages\Incidents1\Possible Incident A

Possible incident, occurring 3/2/09.

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

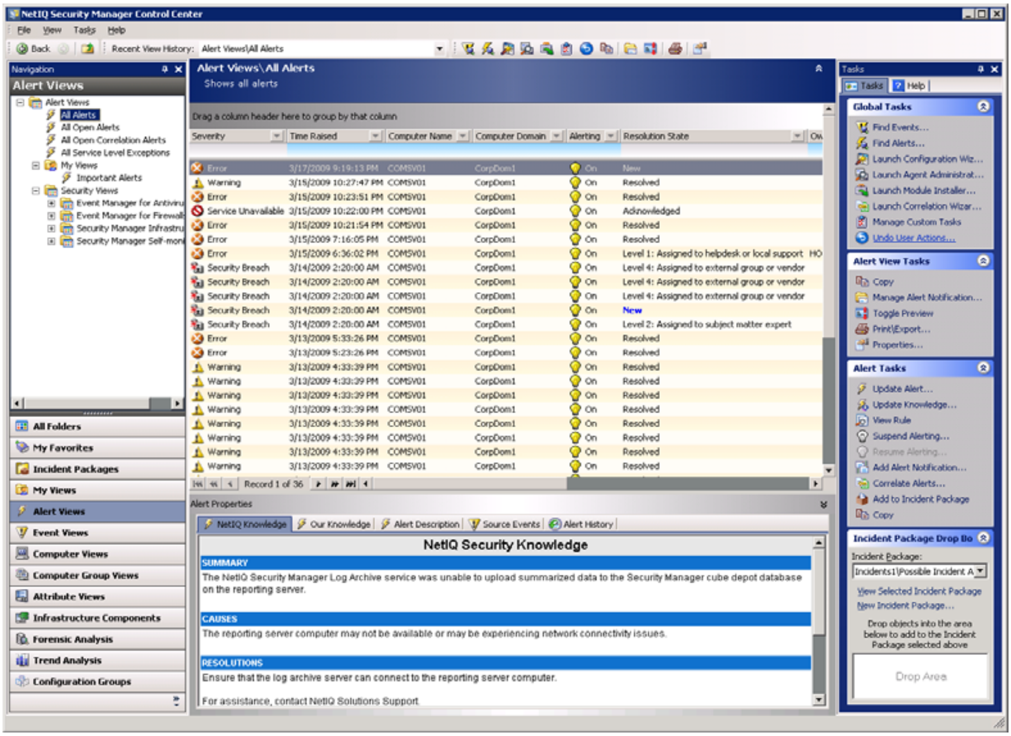
Property Name	Property Value
Incident Package Name	Possible Incident A
Description	Possible incident, occurring 3/2/09.
Owner	CorpDom1\boba
Last Modified	3/18/2009 9:41:41 AM
Last Modified By	CorpDom1\boba
Creator	CorpDom1\boba
Created	3/16/2009 3:41:09 PM

Understanding Views

The Control Center provides default views of the information in the Security Manager database. These views allow you to quickly view and resolve real-time alerts, view all central computers or agents, or examine computer groups from multiple configuration groups. You can use these views to analyze security data, monitor potential problems, and ensure that no alerts go unresolved.

You can also define custom views based on your own criteria to display specific alerts, events, computers, computer groups, or attributes in My Views.

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

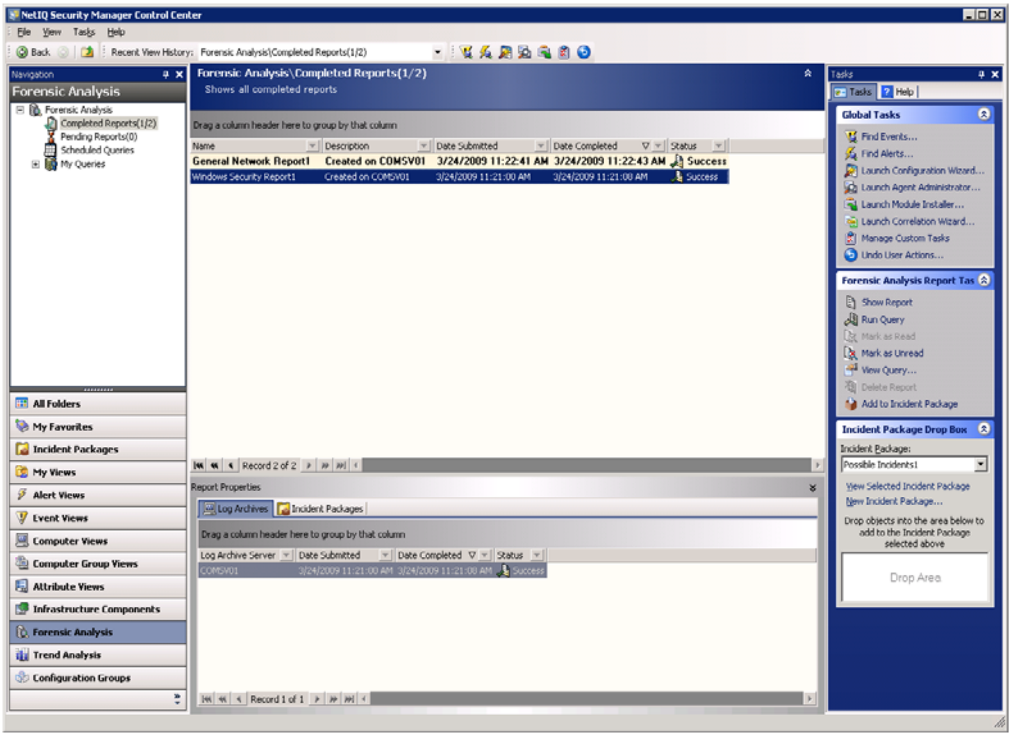
Ensure that the log archive server can connect to the reporting server computer.

For assistance, contact NetIQ Solutions Support

Understanding Forensic Analysis

Use the Forensic Analysis Wizard to query the log archives. Queries return event information that matches specific criteria you supply.

The following figure illustrates the Forensic Analysis view.



Recent View History: Forensic Analysis\Completed Reports(1/2)

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

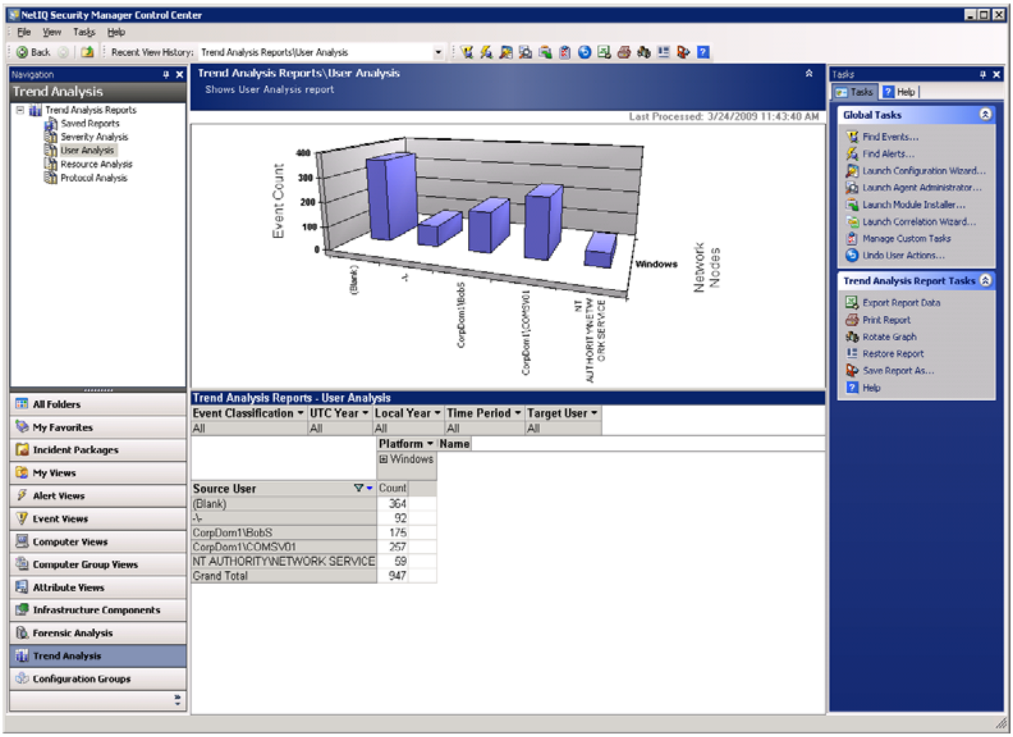
Log Archive Server	Date Submitted	Date Completed	Status
COMSV01	3/24/2009 11:21:00 AM	3/24/2009 11:21:08 AM	Success

Incident Package: Possible Incidents1

Understanding Trend Analysis

Trend Analysis reports let you analyze aggregated data displayed as interactive bar charts. The reporting server aggregates the log archive information to provide long-term trending information. These reports help answer questions such as, “How does the number of high-severity security events for this quarter compare to the number for the same quarter last year?”

The following figure illustrates the Trend Analysis view.



Trend Analysis Reports\User Analysis

Shows User Analysis report

Last Processed: 3/24/2009 11:43:40 AM

Trend Analysis Reports - User Analysis

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

Platform Name

⊞ Windows

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

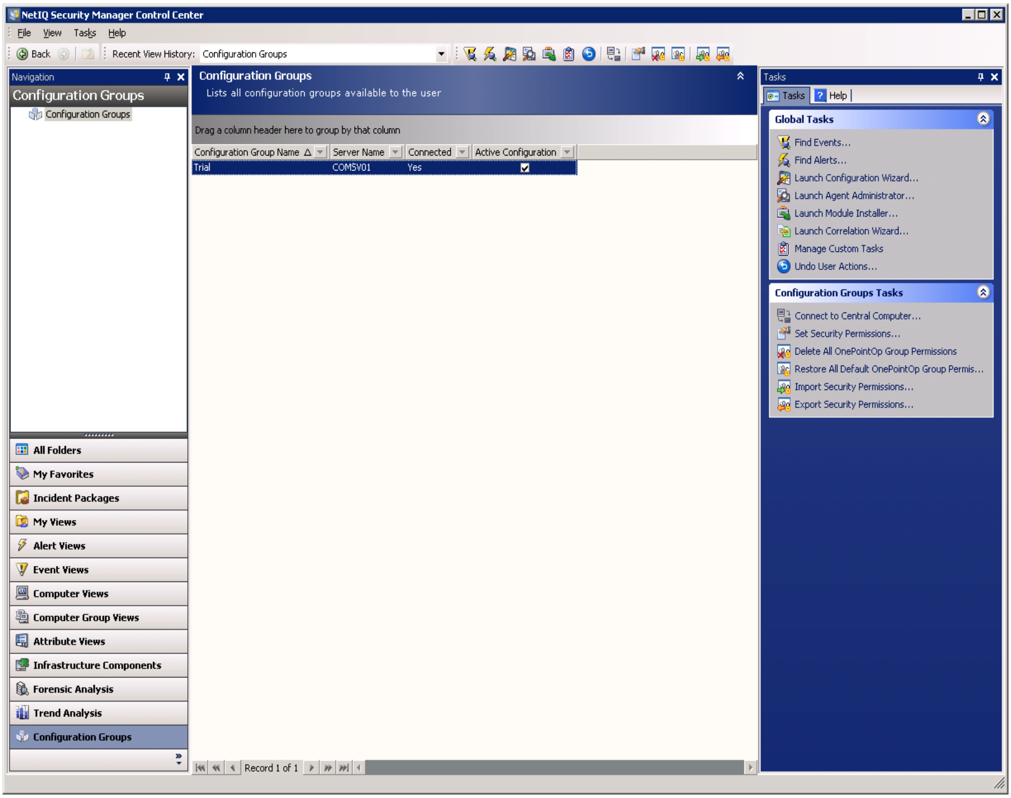
Trend Analysis reports are not available until log data is exported from the log archive and then uploaded into the reporting cube. The reporting cube receives uploaded data every three hours by default. For more information about the reporting cube processing job schedule, see “Uploading Data to the Reporting Cube” on page 75.

Understanding Configuration Groups

The Configuration Groups view indicates the status of the real-time OnePoint database for each configuration group monitored by the Control Center. If you are monitoring multiple configuration groups, those groups display in this view. 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 the *User Guide for NetIQ Security Manager*.

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 setting security permissions, see the *Installation Guide for NetIQ Security Manager*.

The following figure illustrates the Configuration Groups view.


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…

Configuration Groups

Lists all configuration groups available to the user

Drag a column header here to group by that column

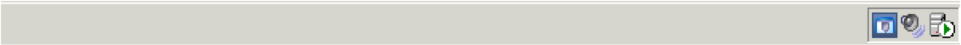
Configuration Group Name	Server Name	Connected	Active Configuration
Trial	COMSV01	Yes	☑

Record 1 of 1

Exploring the Alert Sentry

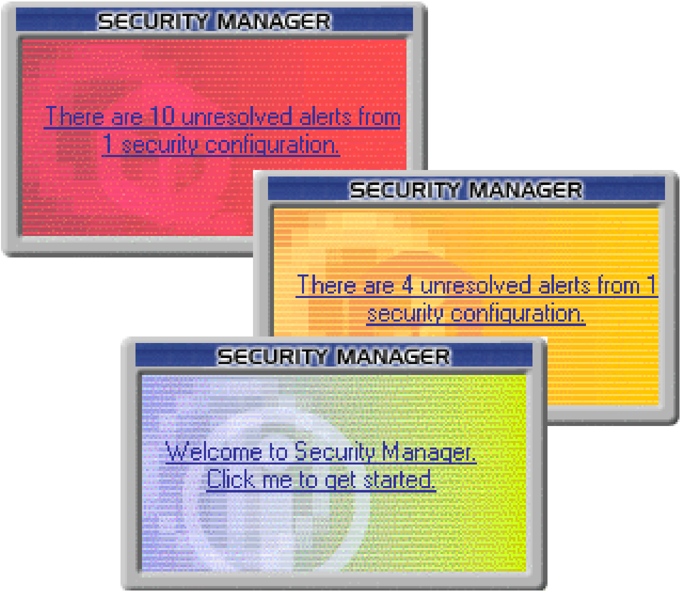
The Alert Sentry notifies you of alerts and links to the Control Center where you can resolve alerts.

The Alert Sentry is a system tray icon that displays pop-up messages to notify you of new alerts. The following figure highlights the Alert Sentry icon in the system tray.



To start the Alert Sentry, click **Alert Sentry** in the NetIQ Security Manager program group.

When an alert occurs, Alert Sentry displays a color-coded pop-up window to indicate the severity of the alert and provides a link to the Control Center.



SECURITY MANAGER

There are 10 unresolved alerts from 1 security configuration.

SECURITY MANAGER

There are 4 unresolved alerts from 1 security configuration.

SECURITY MANAGER

Welcome to Security Manager. Click me to get started.

If you click the **Welcome to Security Manager** link, Alert Sentry starts the Agent Administrator to deploy agents to monitor additional computers. If you run the Agent Administrator, run the Configuration Wizard afterwards to configure the product for your environment.

Clicking the link on other pop-up windows starts the Control Center so you can view alert details.

The alert severity colors that Alert Sentry uses 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.

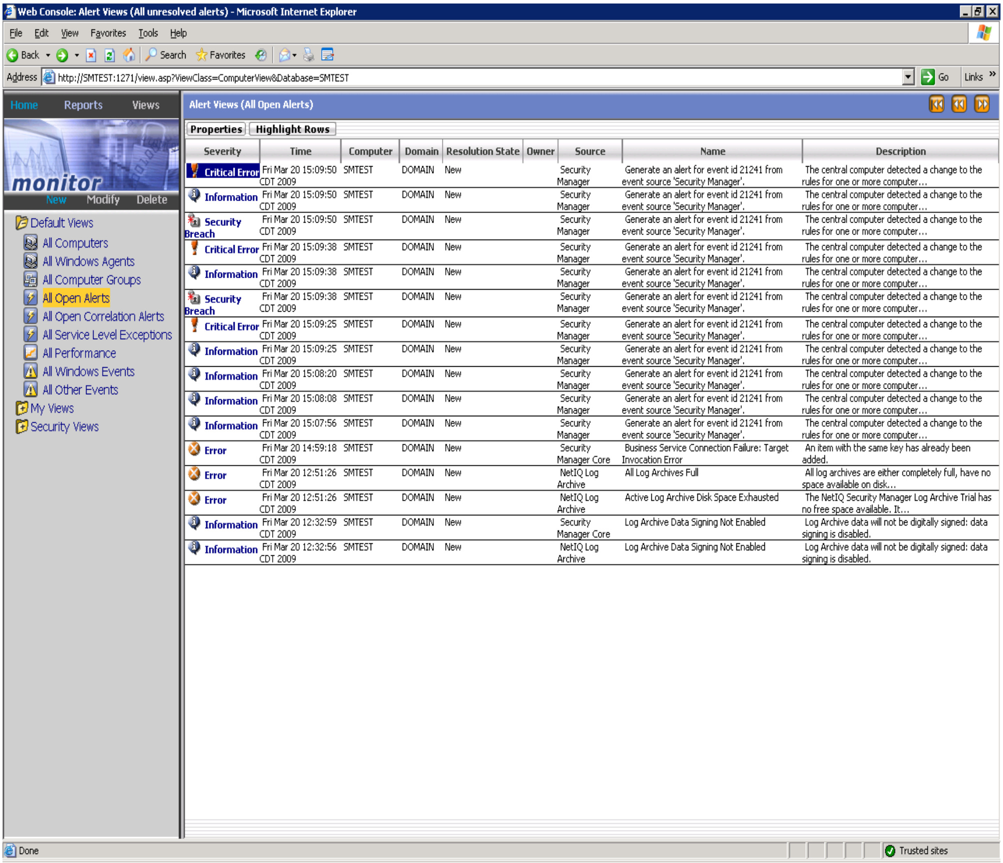
Right-click the Alert Sentry icon to access other Security Manager consoles and wizards from the Alert Sentry menu.

Exploring the Web Console

The Web Console lets you access alert and report information from any computer with Microsoft Internet Explorer 6.0, Internet Explorer 7.0, or Internet Explorer 8.0 installed. To use the Web Console, your user account must be a member of the OnePointOp Users group.

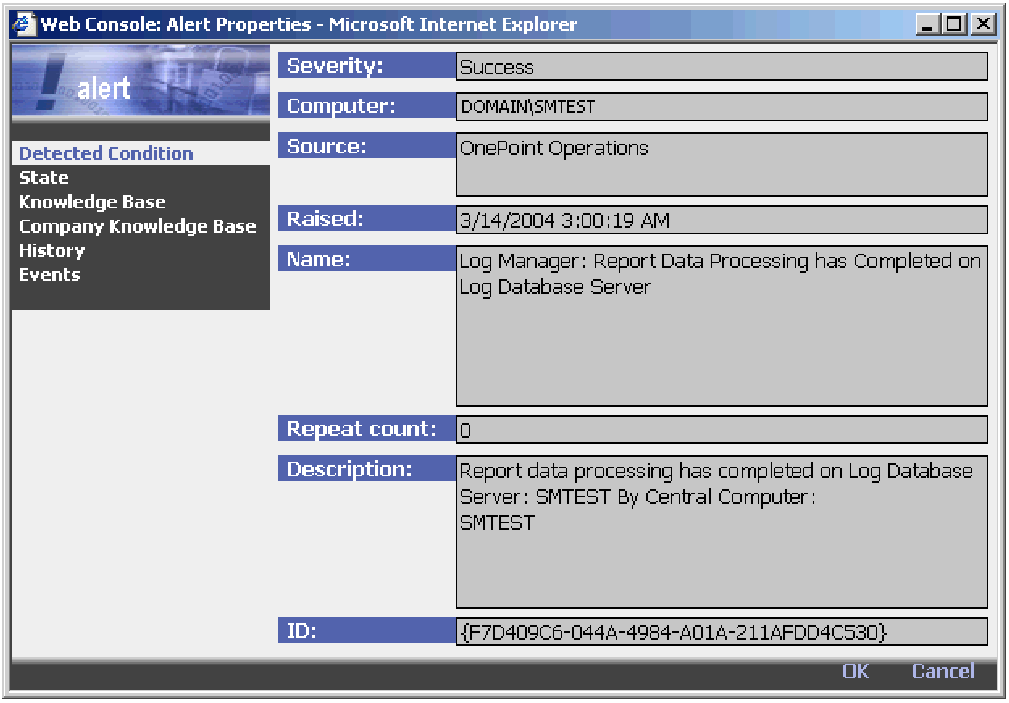
To display the Web Console, start Internet Explorer and type the following URL in the **Address** field: `http://`*`EvaluationComputerName`*`:1271`. Replace *`EvaluationComputerName`* with the name of the evaluation computer.

The Web Console offers customizable views for managing alerts. The following figure shows the All Open Alerts views in the Web Console.



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.

To view details about a specific alert, in the right pane, click the **Severity** field of an alert. The Web Console displays an alert properties window, similar to the following figure.



Severity:	Success
Computer:	DOMAIN\SMTEST
Source:	OnePoint Operations
Raised:	3/14/2004 3:00:19 AM
Name:	Log Manager: Report Data Processing has Completed on Log Database Server
Repeat count:	0
Description:	Report data processing has completed on Log Database Server: SMTEST By Central Computer: SMTEST
ID:	{F7D409C6-044A-4984-A01A-211AFDD4C530}

The Web Console can be useful if you do not want to install Security Manager user interfaces locally or if you need to view alerts and reports from a remote location.

Exploring the Development Console

The Development Console lets you configure global Security Manager settings and lets you modify and create Security Manager rules. Security Manager rules let you define how you want to manage security in your environment. For example, you can define rules that categorize your computers into groups or define the response Security Manager enforces when a specific event occurs.

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

Understanding the Configuration Snap-In

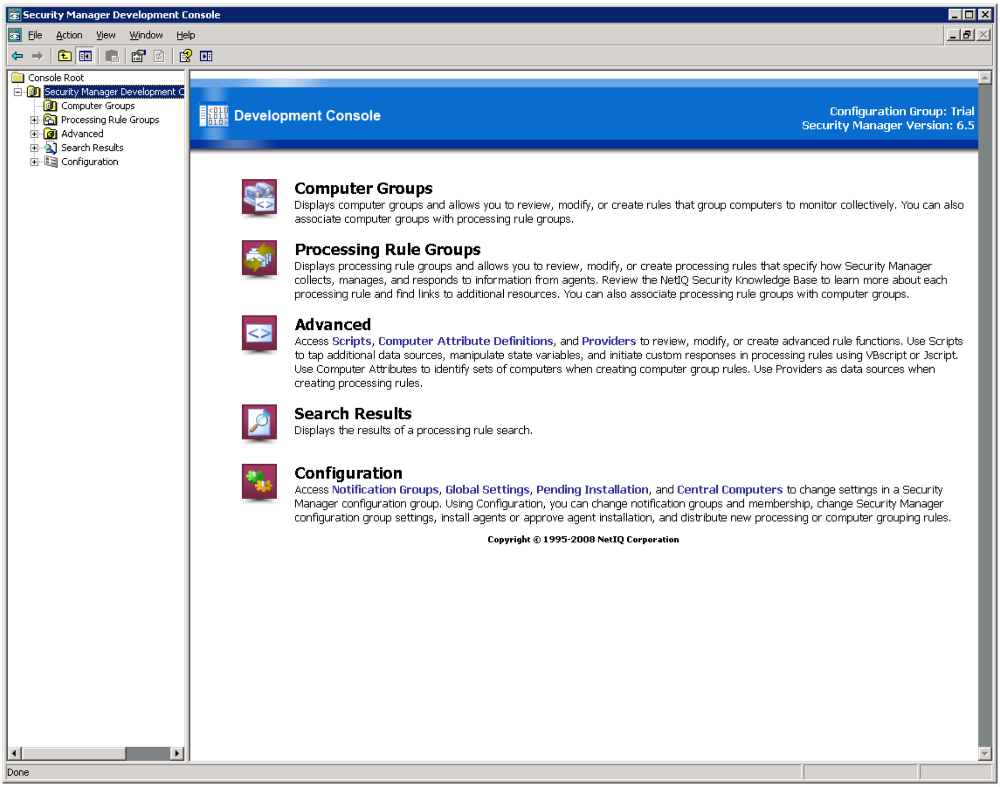
The Configuration snap-in lets you manage the way Security Manager works, including managing notification groups, agents, and Global Settings. The Configuration snap-in also lets you perform other Security Manager operations, such as the following tasks:

- View and approve Windows agent installations
- Define alert resolution states tailored to your organization
- Manage automatic database grooming settings

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

To start the Development Console, click **Development Console** in the NetIQ Security Manager program group.

When you start the Development Console, the right pane provides links to components you can configure, as shown in the following figure.



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.

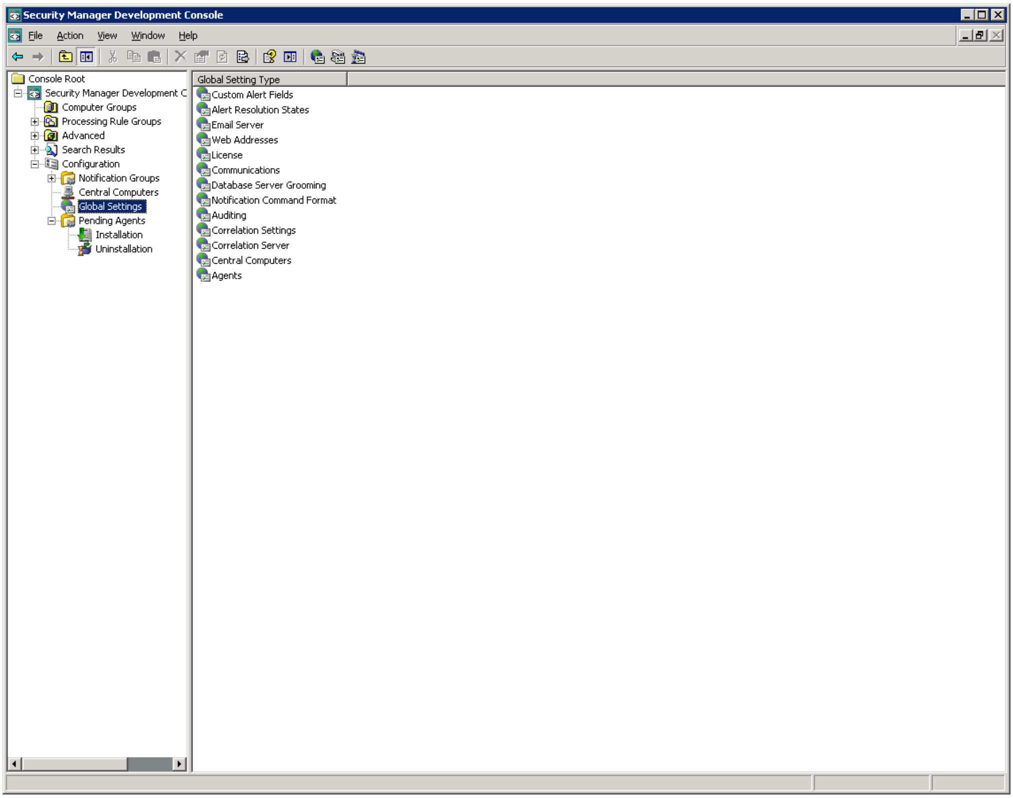
Advanced
Access Scripts, Computer Attribute Definitions, and Providers to review, modify, or create advanced rule functions. Use Scripts to tap additional data sources, manipulate state variables, and initiate custom responses in processing rules using VBscript or Jscript. Use Computer Attributes to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

To view Global Settings, in the left pane, expand **Configuration** and click **Global Settings**. The following figure shows the Global Settings you can specify using the Configuration snap-in.



Global Setting Type
Custom Alert Fields
Alert Resolution States
Email Server
Web Addresses
License
Communications
Database Server Grooming
Notification Command Format
Auditing
Correlation Settings
Correlation Server
Central Computers
Agents

Developing Rules

Developing rules through the Development Console is beyond the scope of the trial guide. For more information about developing rules using the Development Console, see the *Programming Guide for NetIQ Security Manager*.

Chapter 4

Exploring Security Manager

Security Manager analyzes event activity across your enterprise, automatically responds to threats, and provides safekeeping of critical security information, from a simple-to-use central console.

In the following product tours, you can interact with Security Manager and observe many product features. The demonstrations help you gain familiarity with several product features using the following user interfaces:

- Control Center
- Development Console
- Web Console

Note

The *Trial Guide for NetIQ Security Manager* does not provide a tour of UNIX or iSeries product capabilities. For more information about using these features, see the NetIQ UNIX Agent documentation and Security Manager for UNIX module documentation and the NetIQ Security Solutions for iSeries documentation and Security Manager for iSeries module documentation, respectively, or contact your NetIQ sales representative.

You should deploy any additional Windows agents, install Change Guardian for Windows, and configure the product before you begin the tours. For more information about deploying and configuring agents and installing Change Guardian for Windows, see “Deploying Security Manager Agents” on page 36, “Configuring Security Manager” on page 38, and “Installing Change Guardian for Windows” on page 37.

For more information about starting and using the consoles, see "Exploring the User Interfaces" on page 45.

Receiving and Managing an Alert

Members of the Administrators group can have powerful domain privileges. Attackers on the outside or employees on the inside may attempt to gain additional access permissions by adding their own user account to the Administrators group. Change Guardian for Windows can alert you when anyone attempts to change sensitive group membership.

In the following tour, you make a change to the local Administrators group and Security Manager generates an alert. In the Control Center, you view and acknowledge the alert and then add your comments to your company knowledge base.

To observe how Security Manager alerts you to changes to sensitive groups using the Control Center:

1. On the evaluation computer, add a user account to the local Administrators group. You can use a native Windows tool or another administration product, such as the NetIQ Directory and Resource Administrator product (Directory and Resource Administrator). When a member is added to this group, Security Manager generates an alert.
2. ***If it is not already running***, start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.
3. In the Navigation pane, click **All Folders > All Open Alerts**.
4. In the All Open Alerts window, select a Security Breach level alert with the following name: `Security: Built-in local group member added`.
5. In the Alert Properties window, click the Our Knowledge tab to review any existing custom Knowledge Base information for the alert.
6. ***If you want to add a comment to the company knowledge base***, click **Alert Tasks > Update Knowledge** on the Tasks menu.

7. Type your comment and click **OK**.
8. On the Tasks menu, click **Alert Tasks > Update Alert**.
9. Click **State of Alert**.
10. Select **Acknowledged**.
11. Click **Browse** to select a name for the **Alert Assigned To Owner** field, such as `Administrator`.
12. Click **OK**.
13. Click **OK**.
14. On the Tasks menu, click **Alert Tasks > View Rule** to see the details of the processing rule that generated the alert.
15. Click **Close**.

Customizing Alert Resolution States

If you want to customize the alert resolution workflow, you can explore the following feature on your own using the Development Console. The following instructions will get you started. See the Help for additional guidance.

To customize the alert resolution workflow:

1. In the left pane of the Development Console, expand **Configuration > Global Settings.**
2. In the right pane, click **Alert Resolution States**.
3. On the Action menu, click **Properties**.
4. Select a Resolution state and click **Add**, **Modify**, or **Delete** and then make your changes. For more information about fields on a window, click **Help**.

5. Click **OK**.

6. Click **OK** to close the Configuration Group Global Settings window.

Creating an Event Correlation Rule

Now that you have observed Security Manager generating alerts, you can explore creating more sophisticated event correlation rules. Correlation rules help you tame alert activity in several ways. For example, correlation rules can suppress less-important alerts. Correlation rules can also detect multiple conditions that alone may be less important, but in combination may indicate a significant security issue.

In the following demonstration, you first take actions that cause Security Manager to generate alerts. Then, using the Correlation Wizard, you create a rule based on those alerts. After Security Manager sends updated rules to the agents, repeat the actions to see how the correlation rule changes the response.

Emulating Alert Activity

When you previously configured Security Manager, you created a Change Guardian for Windows process filter specifically to generate an alert when the `ftp.exe` process starts or stops. Using the filtered process, you can see Security Manager in action in this demonstration.

In addition to running FTP, you clear the Windows security event log. These activities simulate an attacker attempting to FTP to your server and then clearing the log to remove evidence.

To emulate alerts in preparation for creating a correlation rule:

1. On the Windows task bar, click **Start > Run**.

2. Type `ftp` and click **OK**.

3. In the `ftp` window, type `quit`.

4. Click **Enter**.

5. Open the Windows Event Viewer. You can run Event Viewer from the Administrative Tools program group.

6. In the left pane of Event Viewer, select **Security**.

7. On the Action menu, click **Clear all Events**.

8. When Event Viewer prompts you to save the log, click **No**.

9. Minimize Event Viewer to use again in a later task.

Completing these steps causes Security Manager to generate two alerts. In the next task, you use the alerts as the basis for a correlation rule.

Creating a Correlation Rule

In the following task, select the alerts Security Manager generated and then run the Correlation Wizard. By answering a few simple questions, the Correlation Wizard helps you quickly create a conditional rule to help quiet event noise and detect more complex security threats.

You can start the Correlation Wizard in the Control Center. You can also create and modify correlation rule properties using the Development Console. In the Development Console you can define additional responses to correlated alerts, such as running a script or notifying a security group. You can use correlated alerts in other correlation rules to define and detect more complex threats.

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

To create a correlation rule based on existing alerts:

1. In the Navigation pane of the Control Center, click **Alert Views**.

2. Click **All Alerts**

3. In the Results window, select the following alerts:

Security Breach	Change Guardian: Unmanaged process change
Warning	Security: The audit log was cleared

4. On the Tasks menu, click **Alert Tasks > Correlate Alerts**. Security Manager starts the Correlation Wizard.
5. Read the Welcome window and click **Next**.
6. On the Events window, click **Next** to use the selected alerts.
7. On the Order window, click **Next** to specify **in any order**.

Note
If you change the event order, the later demonstration may not work as described.

8. On the Common Fields window, click **agent** and select Additional.
9. On the Additional Fields window, select **computer** as the common event field and click **OK**.
10. Click **Next**.
11. On the Time Limit window, click **Next** to specify **30 seconds** as the time frame.
12. On the Response window, complete the following steps:
    a. In the **Alert to generate** list, select **Generate a Security Breach alert**.
    b. In the **Alerts to stop** list, select both alerts. Security Manager suppresses later occurrences of either alert.
    c. Click **Next**.
13. On the Name window, type a name for the rule, such as `Eval Tour Correlation Rule`.
14. Type a description for the rule, such as `Evaluation tour correlation rule`.

15. Review the correlation rule criteria and click **Next**.

16. Review the Summary window and click **Finish**.

17. Click **OK**.

18. ***If it is not already running***, start the **Development Console** in the NetIQ Security Manager program group folder.

19. In the left pane of the Development Console, click **Configuration**.

20. On the Action menu, click **Force Configuration Changes Now,** and then click **OK**.

21. ***If Security Manager displays a confirmation window***, click **Close**.

You created a correlation rule and instructed the central computer to begin enforcing the changes you made. By default, Windows agents check with the central computer for configuration changes every 300 seconds.

Wait 5 minutes to ensure the rules are updated at the Windows agent before starting the next task. If you prefer, you can reduce the Windows agent heartbeat interval in the Development Console using **Configuration > Global Settings > Agents**. For more information about modifying the Windows agent heartbeat interval, see the Help.

Triggering the Correlation Rule

Now that you have emulated alerts and created a correlation rule, and have waited 5 minutes for Security Manager to distribute the rules to agents, you can repeat the original actions to observe how Security Manager applies the new rule. The following task repeats the emulation steps you performed earlier in this demonstration.

To trigger the correlation rule and observe the responses:

1. Click **Start > Run** on the Windows task bar.

2. Type `ftp` and click **OK**.

3. In the `ftp` window, type `quit`.

4. Restore the Windows Event Viewer.

5. On the Action menu, click **Clear all Events**.

Note

If you are logged onto the central computer as Administrator, you may also trigger a built-in correlation rule when you clear the security log.

6. Close the Event Viewer window.
7. In the Navigation pane of the Control Center, click **Alert Views**.
8. Click **All Open Alerts**.
9. Notice that the alerts in the view are the ones Security Manager generated before you implemented the correlation rule. Security Manager suppresses later occurrences of the alerts.
10. Allow a few moments for Security Manager to receive the correlated events and apply the correlation rule. If you do not see the alert quickly, on the View menu, click **Refresh**.
11. In the Results window, click the new Security Breach alert.
12. Review the tabs in the Alert Properties window for more details about the new alert.
13. On the Tasks menu, click **Alert Tasks > Update Knowledge**.
14. Add your own comments to this alert.
15. Click **OK**.

When you apply this correlation rule, Security Manager takes several actions:

- Suppresses the alerts normally generated for the events that triggered the rule
- Identifies and correlates the alerts according to the rule criteria
- Generates one alert reporting the combined actions and takes any additional responses associated with the rule

Exploring Security Manager Log Management

Now that you understand how monitoring real-time events can help you better approach security event management, take some time to explore the important reporting features Security Manager offers.

Security Manager collects, consolidates, and archives event log data from operating systems and software throughout your enterprise. Security Manager offers the following useful report types created using these data:

- Forensic Analysis reports that itemize each archived normalized event, such as every unsuccessful logon or other audited event.
- Trend Analysis reports that accumulate multi-dimensional data to answer questions such as, “Which production servers in my network were most highly targeted by attacks this quarter versus last quarter?”
- Summary reports created from reporting cube data using SQL Server Reporting Services. For more information about creating and viewing Summary reports, see the *User Guide for NetIQ Security Manager.*

These types of reports, especially when used in conjunction with the real-time information Security Manager provides, can help you more rapidly identify, research, and prevent security incidents. The following tour lets you explore Forensic Analysis and Trend Analysis reports in more detail.

Exploring Forensic Analysis Queries and Reports

Forensic Analysis reports give a consolidated view of the raw data for all collected logs on different computers, devices, firewalls, routers, or switches. In the My Queries folder, Security Manager provides a number of example Forensic Analysis queries on a variety of platforms or potential problems. You can also create your own custom queries from which you can run Forensic Analysis reports.

To run and view Forensic Analysis reports:

1. Start the **Security Manager Control Center** in the NetIQ Security Manager program group folder.
2. In the Navigation pane, click **Forensic Analysis**.
3. Click the **Forensic Analysis Wizard** icon.
4. 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.
5. Click **Finish**.
6. Click **OK**.
7. In the Navigation pane, click **Completed Reports**.
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.
   - 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**.
   - To print the report, on the Options menu, click **Print**.

- 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** dialog box and click **Find Next**.

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

Continue to explore the Forensic Analysis report displays and controls on your own.

Exploring Trend Analysis Reports

Trend Analysis reports allow you to view a wide range of data, summarized into understandable charts or graphs, across your entire configuration group. Unlike Forensic Analysis reports, which report on specific events, Trend Analysis reports summarize events. Trend Analysis reports allow you to view trends and pinpoint possible future trouble areas.

Uploading Data to the Reporting Cube

Before exploring Trend Analysis reports, you must have log data uploaded into the reporting cube. The cube depot processes and uploads log archive data every three hours by default, using the `NetIQ_SM_SSIS` SQL Server processing job.

To view Trend Analysis report data quickly, change the processing job schedule using SQL Server Management Studio.

To modify the reporting cube processing job schedule:

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** in the Microsoft SQL Server 2005 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. Expand **SQL Server Agent > Jobs**.
7. Right-click **NetIQ_SM_SSIS** and select **Properties**.
8. Click **Schedules**.
9. Click **Edit**.
10. Under **Occurs every**, specify **2 minutes**.
11. Click **OK**.
12. Click **OK** again.
13. In the Object Explorer, right-click **Job Activity Monitor** and select **View Job Activity**.
14. Click **F5** to refresh the Job Activity Monitor until the Last Run Outcome for the `NetIQ_SM_SSIS` job is `Succeeded`.
15. Click **Close**.
16. Close SQL Server Management Studio.

Note

Even after you modify the reporting cube schedule, the log archive may not yet contain enough log data to begin sending that data to the reporting cube depot for processing.

After you can view summarized log data in a Trend Analysis report using the Control Center, you should use SQL Server Management Studio to change the `NetIQ_SM_SSIS` job schedule back to the default schedule of every 3 hours.

Viewing Trend Analysis Reports

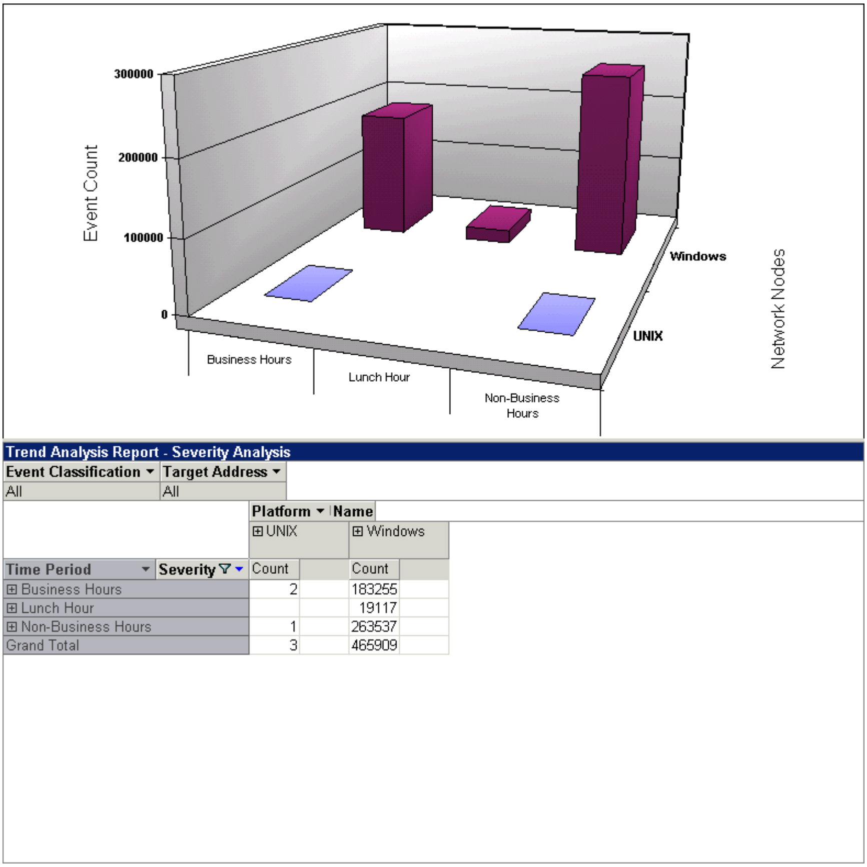
After the cube depot processes and uploads log data to the reporting cube, you can view the data in Trend Analysis reports using the Control Center. You can use the Control Center user interface to modify and customize the default Trend Analysis reports Security Manager provides.

To view a Trend Analysis report:

1. ***If the Control Center is not currently running***, start the **Security Manager Control Center** from the NetIQ Security Manager program group.
2. In the Navigation pane, click **Trend Analysis > Severity Analysis**. In the Trend Analysis Reports window, Security Manager displays a chart representing the number of high, low, and medium severity events for the identified network nodes.

   In the lower pane of the Trend Analysis Reports window, Security Manager displays the default dimension controls and the detail data used in the chart.
3. Drag the **Time Period** dimension control from the top of the pivot table and drop it to the left of the **Severity** dimension in the pivot table.

When you drop the **Time Period** dimension control to the left of the **Severity** dimension control, the chart now looks similar to the following figure.



Trend Analysis Report - Severity Analysis

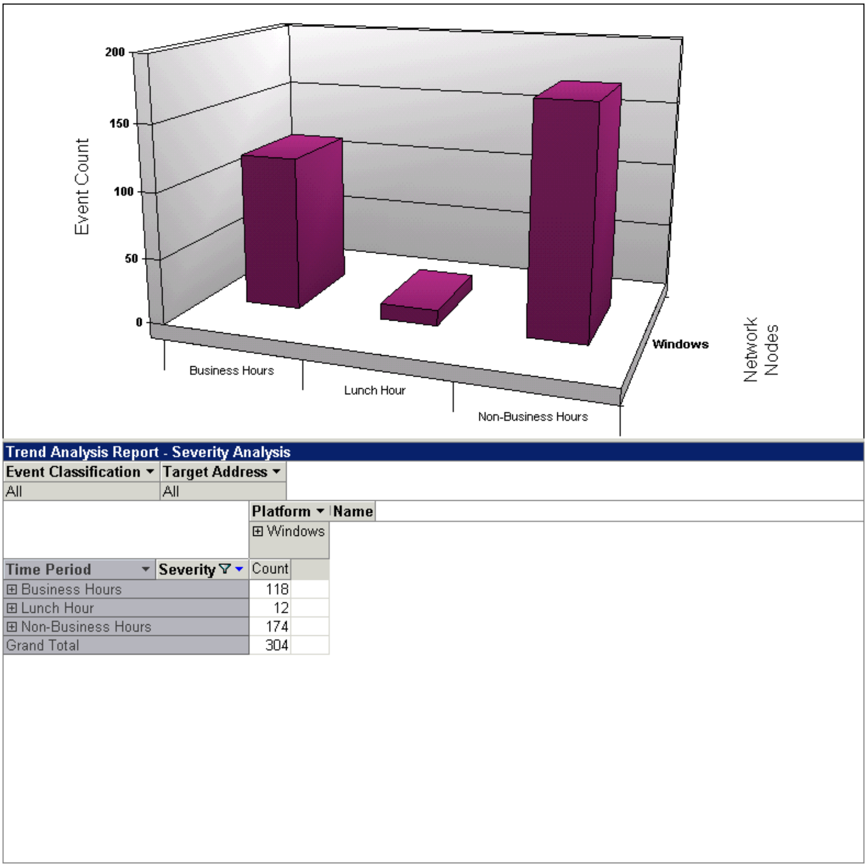
Event Classification	Target Address
All	All

Time Period	Severity	Platform / Name: UNIX	Windows
		Count	Count
Business Hours		2	183255
Lunch Hour			19117
Non-Business Hours		1	263537
Grand Total		3	465909

The bottom axis is now divided into three time periods, business hours, lunch hour, and non-business hours, showing the number of high, low, and medium events during each time period.

4. Click the down arrow on the **Severity** dimension control to choose which severity levels to include in the Trend Analysis report.

5. Clear **Low** and click **OK**. Security Manager removes the low severity events from the display, resulting in a graph similar to the following figure.



Trend Analysis Report - Severity Analysis

Event Classification ▾	Target Address ▾
All	All

Platform ▾	Name
⊞ Windows	

Time Period ▾	Severity ▾	Count
⊞ Business Hours		118
⊞ Lunch Hour		12
⊞ Non-Business Hours		174
Grand Total		304

Continue to explore the Trend Analysis displays and controls on your own. To customize Trend Analysis reports to display any of the dimensions available in the reporting cube, right-click in the lower pane of the Trend Analysis Reports window and select **Field List**. Drag any dimensions you want to display to the pivot table.

In addition, the Tasks menu offers tools that let you export, print, rotate, and save your graphs. Especially useful is the **Restore Report** command, which resets the report to its default dimensions and display parameters.

Exploring Security Manager Event Management

Security Manager provides support for monitoring a variety of security point products, including antivirus, firewall, and intrusion detection systems (IDS). In addition, Security Manager can monitor routers or switches that log activity in a Cisco IOS log.

The trial installation automatically downloads all the Security Manager modules that monitor these security point products. For a production installation, you install only the modules you need based on the point products used in your environment. For example, if your enterprise standardized using Symantec Norton antivirus products, you would install the Security Manager module for this brand of antivirus products.

In addition, you may need to run the Configuration Wizard to instruct Security Manager to monitor the products you use and to enable Security Manager to acquire and store the corresponding event data.

Configuring Event Management

The Configuration Wizard helps you configure Security Manager to work with best-of-breed security point products your enterprise uses. The Configuration Wizard modifies Security Manager modules, the rules Security Manager uses to monitor the product making it easy for you to start monitoring many other security products.

To configure Security Manager to monitor security point products:

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

2. On the Tasks menu, click **Global Tasks > Launch Configuration Wizard**.

3. In the Configuration Wizard, click the Support For tab for the product you want to configure, such as **Support For Firewalls**.

4. In the right pane, click the specific item to configure, such as **Configure the module for Cisco Firewalls**.
5. Follow the wizard instructions to configure support for your product and click **Finish**. For more information about the fields on a window, see the Help.
6. Select **Populate computer groups now** and **Apply configuration changes to installed agents now**, and then click **OK**.
7. Click **OK**.
8. Repeat Steps **3** through **6** to configure additional products for Security Manager to monitor.
9. Click **Close**.

When you configure support for a security product, Security Manager may also perform the following steps:

- Create a Security Manager computer group rule that identifies computers running the selected product.
- Initiate product log collection for Security Manager.
- Start collecting performance data from the product.
- Choose to backup configuration information about the product.

For more information, see the *Installation Guide for NetIQ Security Manager*.

Monitoring Security Products Using Security Manager

In the following sections, you can explore how Security Manager helps you manage and monitor your security products using the Control Center. The following steps get you started, and then you can explore the product further using the Control Center.

To explore security product monitoring using Security Manager:

1. In the Navigation pane, click **All Folders**.
2. Expand **Security Views** and a module sub-folder. For example, click **Event Manager for Firewalls**.

3. To view the alerts for a specific product, expand to a product name. For example, expand **Secure Computing Sidewinder > All Sidewinder Events (last 72 hours)**.

4. When you select a view in the Navigation pane, the Results window displays the view.

5. To select another view, expand a view folder in the Navigation pane, click the plus sign, and then click the view.

The following sections provide additional descriptions of Security Manager capabilities.

Exploring Event Manager for Firewalls

Firewalls are most commonly installed using default configuration settings. The International Computer Security Association (ISCA) estimates that 70 percent of all firewalls in production today are configured incorrectly, thereby lulling many enterprises into a false sense of security.

Firewalls can be tedious to monitor because they can generate high levels of event activity. Security personnel find it difficult to sift through events to determine which events need further investigation and which can be safely acknowledged as acceptable. In addition, new security personnel may take added time while learning to use multiple firewall user interfaces.

Event Manager for Firewalls works with your installed firewall applications by filtering firewall events to identify critical events that require your response. Event Manager for Firewalls also helps you locate weaknesses in your firewall configuration so you can strengthen firewall policy. The product reports firewall activity to the Control Center so your security personnel need to learn only one user interface to manage all your security and firewall events.

In addition, Event Manager for Firewalls can correlate data to identify complex threats and then respond to them. For example, if multiple port scans originate from a single source, Event Manager for Firewalls recognizes the series and can block all activity from that source. Event Manager for Firewalls also offers the following features:

- Alerts in real time for incorrect firewall configurations
- Alerts in real time for firewall policy breaches
- Backs up firewall configuration so you can restore to a known secure state

Security Manager provides built-in rules and knowledge, called modules, to monitor several different firewall products.

To explore Event Manager for Firewalls views, in the Navigation pane of the Control Center, expand **Security Views > Event Manager for Firewalls** and select a firewall view.

Exploring Event Manager for Antivirus

Event Manager for Antivirus delivers and correlates information from your existing antivirus solution. Event Manager for Antivirus can alert you when a computer is vulnerable to a virus attack because it does not have the latest antivirus definition files. Event Manager for Antivirus can alert you when a scheduled virus file update was unsuccessful. You can then respond to this alert and update the definition files to safeguard the computer.

Event Manager for Antivirus can correlate events from your enterprise-wide antivirus solution to help you take quick and decisive action to correct and prevent virus outbreaks from spreading. Event Manager for Antivirus serves as a central point from which to monitor your antivirus solution across your enterprise. Security personnel need to learn only the Security Manager user interfaces to monitor antivirus products as well as firewall and IDS solutions.

If you do not use one of the antivirus products Security Manager monitors installed in your trial environment, you can still view the Unprotected Computer views to see how Event Manager for Antivirus works.

To explore Event Manager for Antivirus views, expand **Security Views > Event Manager for Antivirus** in the Navigation pane of the Control Center and select an antivirus view folder and view.

Exploring Event Manager for IDS

Intrusion Detection Systems (IDS) can generate an overwhelming number of events for security administrators to monitor. Event Manager for IDS filters the data to help you more easily ascertain a potential security threat and respond before the threat causes downtime. Event Manager for IDS also helps you enforce your IDS configuration policies.

Event Manager for IDS can help you pinpoint vulnerabilities in your network and identify computers that do not comply with your security policies. You can also use Event Manager for IDS to track IDS policy changes to ensure that all changes are necessary and meet your security policy settings. Real-time collection of events from your IDS solution allows your security administrators to respond quickly to potential security threats.

Event Manager for IDS improves the return on your IDS investment by centralizing IDS event monitoring and correlation. Event Manager for IDS not only allows your organization to gain greater value from your existing IDS solution, but also reduces personnel training costs.

Event Manager for IDS uses the Security Manager user interfaces, so security administrators need to learn only the Security Manager user interfaces to manage your IDS solution in addition to your antivirus and firewall solutions.

You can explore Event Manager for IDS views in the Control Center.

To explore Event Manager for IDS views, expand **Security Views > Event Manager for IDS** in the Navigation pane of the Control Center and select an IDS product view folder and view.

Exploring Event Manager for Routers and Switches

Security Manager collects and analyzes events logged by Cisco IOS devices, including routers and switches. Event Manager for Routers and Switches consolidates Cisco IOS device alerts and messages to filter less important activity but alert you about important events. The product also alerts you to operational problems and suspicious activity. Event Manager for Routers and Switches can most monitor devices that record activity in a Cisco IOS syslog.

Normally a router or switch sends event log activity to a computer for storage. When you install a Windows agent on the computer hosting the IOS log, you can monitor the device log. Run the Configuration Wizard to associate the logging host with the devices. You can also archive data sent by routers and switches by using Log Manager for Routers and Switches.

Security Manager for Routers and Switches filters or consolidates the following information to reduce alert noise in the Control Center:

- Filters debugging and information-only messages (severity level 6 messages)
- Consolidates Cisco IOS audit trail and access log messages periodically

In addition, Event Manager for Routers and Switches sends alerts to the Control Center for many conditions, such as the following causes:

- DHCP address conflicts, overwritten MTU settings, or a DMA parity errors
- A sub-system software error, possible imminent hardware failure, or important hardware recovery
- Unexpected power failures on a sub-system, significant hardware failures, and other failures that can leave the system in an unusable state

You can explore Event Manager for Routers and Switches views in the Control Center.

To explore Event Manager for Routers and Switches views, expand **Security Views > Event Manager for Routers and Switches** in the Navigation pane of the Control Center and select an router or switch product view folder and view.