

Installation 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.

© 2011 NetIQ Corporation. All rights reserved.

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 (DSSSENH)
- 989 Windows XP Enhanced Cryptographic Provider (RSAENH)
- 990 Windows XP Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSSENH)
- 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 (DSSSENH)

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

| | |
|---------------------------------------|------|
| About This Book and the Library | xi |
| Conventions | xii |
| About NetIQ Corporation | xiii |

Chapter 1

Introduction **1**

| | |
|--|----|
| What Is Security Manager? | 2 |
| What Is Security Manager Event Management? | 3 |
| What Is Security Manager Log Management? | 4 |
| How Security Manager Works | 5 |
| Understanding Product Components | 5 |
| Understanding Configuration Groups | 8 |
| Understanding the Architecture | 9 |
| Anticipating Your Hardware Needs | 11 |
| Understanding Security Manager Data Flows | 13 |
| Understanding Windows Component Communication | 18 |
| Understanding Windows Agent Communication Security | 19 |
| Understanding Self-Scaling Windows Operations | 20 |
| Understanding Supported Windows Platforms | 20 |
| Understanding Supported Data Formats | 21 |
| Managing UNIX and iSeries Agents | 21 |

Chapter 2

Planning to Install Security Manager **23**

| | |
|--------------------------------|----|
| Getting Started | 23 |
| Implementation Checklist | 25 |

| | |
|---|----|
| Planning to Roll Out Your Configuration Groups | 26 |
| Understanding Multiple Configuration Groups | 29 |
| Understanding Licensing | 32 |
| Supporting Foreign Languages | 32 |
| Naming Your Configuration Groups | 32 |
| Understanding Configuration Group Passwords | 33 |
| Installing Microsoft SQL Server | 33 |
| Installing Database Components in a Clustered Environment | 35 |
| Understanding Microsoft SQL Server Permissions | 36 |
| Configuring Microsoft SQL Server | 37 |
| Estimating Database Sizes | 39 |
| Estimating Log Archive Size | 42 |
| Planning to Install Your Database Server | 44 |
| Planning to Install Your Log Archive Servers | 47 |
| Planning to Install Your Central Computers | 52 |
| Planning to Install Your Reporting Server | 61 |
| Planning to Install Your Agents | 66 |
| Planning to Install Your User Interfaces | 74 |
| Understanding Security Manager Requirements and Permissions | 79 |

Chapter 3

| | |
|---|-----------|
| Installing Security Manager | 85 |
| Security Manager Installation Checklist | 86 |
| Obtaining the Latest Product Version | 87 |
| Permissions | 89 |
| Creating a Service Account | 89 |
| Understanding Service Account Requirements | 90 |
| Understanding Service Account Permissions Added by Security Manager | 92 |
| Creating an Email Account | 93 |
| Disabling Active Directory Integration with Message Queuing | 93 |

| | |
|--|-----|
| Installing Security Manager | 95 |
| Choosing Components to Install | 95 |
| Verifying Prerequisites | 97 |
| Running the Setup Program | 99 |
| Installing Additional Central Computers | 100 |
| Installing the Reporting Server | 101 |
| Running the Setup Program | 103 |
| Configuring and Enabling Reporting | 104 |
| Installing Agents | 105 |
| Installing Windows Agents | 105 |
| Configuring Agentless Windows Monitoring | 108 |
| Installing UNIX Agents | 108 |
| Installing iSeries Agents | 109 |
| Configuring Security Manager | 109 |
| Using the Configuration Wizard | 109 |
| Specifying Central Computers for Failover | 110 |
| Synchronizing Device Times | 112 |
| Configuring Security Manager Time Periods | 112 |
| Configuring Notification of Real-Time Alerts | 115 |
| Rolling Out Additional Configuration Groups | 117 |

Chapter 4

| | |
|--|------------|
| Manually Installing Unmanaged Windows Agents | 119 |
| Understanding Unmanaged Windows Agent Installation | 120 |
| Installing and Configuring a Windows Agent Manually | 121 |
| Installing an Unmanaged Windows Agent Manually | 122 |
| Monitoring an Unmanaged Agent with Multiple Configuration Groups | 124 |
| Uninstalling Unmanaged Windows Agents | 125 |

Chapter 5

| | |
|---|------------|
| Installing the User Interfaces | 127 |
| Installing User Interfaces Checklist | 128 |

| | |
|--------------------------------------|-----|
| Installing the User Interfaces | 129 |
| Accessing User Interfaces | 130 |

Chapter 6

| | |
|--|------------|
| What to Do Next | 133 |
| Customizing Security Manager | 133 |
| Configuring Advanced Features | 134 |
| Connecting to Multiple Configuration Groups | 134 |
| Monitoring Agents with Multiple Configuration Groups | 134 |
| Providing Additional Security | 135 |
| Customizing Rules | 136 |
| Configuring Log Archive Data Signing | 137 |
| Verifying a Successful Installation | 144 |
| Installing Additional Security Manager Components | 145 |
| Getting Started with Security Manager | 147 |

Appendix A

| | |
|---|------------|
| Setting Permissions on Computer Groups | 149 |
| Understanding Security Filtering | 150 |
| Understanding Permission Settings | 151 |
| Setting Permissions on Computers | 152 |
| Configuring Security Filtering | 153 |
| Removing OnePointOp Group Permissions | 155 |
| Restoring OnePointOp Group Permissions | 156 |
| Exporting Security Permissions | 157 |
| Importing Security Permissions | 158 |

Appendix B

| | |
|---|------------|
| Installing and Configuring Security Manager in Firewall Environments | 161 |
| Supported Environments | 161 |
| Understanding Security Manager Ports | 162 |
| Troubleshooting Firewall-Related Issues | 172 |

Appendix C

| | |
|---|------------|
| Installing Reporting Components in Clustered Environments | 175 |
| Supported Environments | 175 |
| Installing Reporting Components in a Clustered Environment | 176 |
| Configuring the Reporting Cube SQL Job in a Clustered Environment | 177 |

Appendix D

| | |
|---|------------|
| Installing Security Manager Components Silently | 179 |
| Installation Program Options | 183 |
| Installing or Upgrading Unmanaged Agents Silently | 188 |
| Verifying Silent Installation | 192 |

Appendix E

| | |
|---|------------|
| Upgrading Security Manager | 195 |
| Upgrading Security Manager Overview | 196 |
| Preparing to Upgrade | 198 |
| Upgrading Log Archive Servers | 199 |
| Upgrading Central Computers and the Database Server | 201 |
| Upgrading User Interface Computers | 205 |
| Upgrading Managed Windows Agents | 206 |
| Upgrading Unmanaged Windows Agents | 210 |
| Upgrading UNIX and iSeries Agents | 211 |
| Upgrading the Reporting Server | 212 |
| Upgrading Completed Forensic Analysis Reports and Query Schedules | 213 |
| Managing Central Computer Redundancy | 215 |
| Upgrading Modules | 216 |
| Verifying Upgrade Success | 217 |
| Obtaining New Modules and Module Updates | 218 |

Appendix F

| | |
|---|------------|
| Upgrading SQL Server Computers | 219 |
| Upgrading the Database Server to SQL Server 2008 | 220 |
| Migrating Database Server Databases to a SQL Server 2008 Database Server | 220 |
| Preparing the SQL Server 2008 Database Server | 221 |
| Detaching Security Manager Databases from the SQL Server 2005 Database Server | 223 |
| Attaching Security Manager Databases to the SQL Server 2008 Database Server | 226 |
| Configuring Migrated Databases on a SQL Server 2008 Server | 229 |
| Configuring Security Manager to Use the SQL Server 2008 Database Server | 230 |
| Migrating Reporting Data to a SQL Server 2008 Reporting Server | 233 |
| Preparing Security Manager to Migrate Reporting Components to the SQL Server 2008 Reporting Server | 234 |
| Backing Up the SQL Server 2005 Reporting Cube | 235 |
| Restoring the Reporting Cube on the SQL Server 2008 Reporting Server | 236 |
| Configuring Roles for the SQL Server 2008 Reporting Cube | 237 |
| Backing Up the SQL Server 2005 Cube Depot | 238 |
| Restoring the Cube Depot on the SQL Server 2008 Reporting Server | 239 |
| Configuring the SQL Server 2008 Cube Depot | 240 |
| Configuring Security Manager to Use the SQL Server 2008 Reporting Server | 241 |
| Verifying the Status of the SQL Server 2008 Reporting Server | 242 |

Appendix G

| | |
|---|------------|
| Uninstalling Security Manager | 245 |
| Uninstalling Security Manager Overview | 246 |
| Uninstall Windows Agents | 247 |
| Uninstalling Managed Agents | 248 |
| Uninstalling Unmanaged Agents from All Configuration Groups | 249 |
| Removing a Configuration Group that Monitors an Unmanaged Agent | 251 |
| Uninstall Security Manager Components | 251 |
| Uninstall Reporting Server Components | 252 |
| Uninstall the Databases | 253 |
| Uninstall the Log Archives | 253 |

About This Book and the Library

The installation guide provides planning and installation information for the NetIQ Security Manager product (Security Manager). The installation guide includes planning considerations, specific installation procedures, and product configuration procedures.

Intended Audience

This book provides information for individuals responsible for installing and configuring Security Manager.

Other Information in the Library

The library provides the following information resources:

User Guide

Provides conceptual information about Security Manager. This book also provides an overview of the user interfaces and the step-by-step guidance for many tasks.

Programming Guide

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

Module Documentation

Provides information to help you configure specific products to monitor with Security Manager, such as Symantec Norton AntiVirus or NetScreen Firewall.

Trial Guide

Provides product trial and evaluation instructions and a product tour.

Help

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

Conventions

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

| Convention | Use |
|---|---|
| Bold | <ul style="list-style-type: none">• Window and menu items• Technical terms, when introduced |
| <i>Italics</i> | <ul style="list-style-type: none">• Book and CD-ROM titles• Variable names and values• Emphasized words |
| Fixed Font | <ul style="list-style-type: none">• File and folder names• Commands and code examples• Text you must type• Text (output) displayed in the command-line interface |
| Brackets, such as [<i>val ue</i>] | <ul style="list-style-type: none">• Optional parameters of a command |
| Braces, such as { <i>val ue</i> } | <ul style="list-style-type: none">• Required parameters of a command |
| Logical OR, such as <i>val ue1</i> <i>val ue2</i> | <ul style="list-style-type: none">• 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.

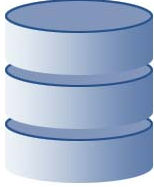
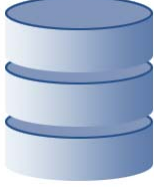

Understanding Product Components

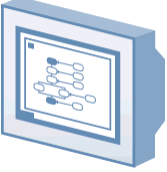
Security Manager includes a number of software components that you can distribute and install as needed to meet your security management objectives and environment.

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 |
|---|--|
| <p data-bbox="205 444 440 500">Windows, UNIX, and iSeries Agents</p>  | <p data-bbox="494 444 1143 529">Services running on Windows, UNIX, or iSeries computers to monitor operating systems, devices, or applications, such as antivirus and firewall products, in real time.</p> |
| <p data-bbox="205 764 411 820">Central Computer Components</p>  | <p data-bbox="494 764 1180 932">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.</p> <p data-bbox="494 948 1173 974">Central computers can provide the following additional services:</p> <p data-bbox="494 984 1159 1068">Correlation server – receives data forwarded by all central computers, applies correlation rules, and generates responses when rule matches occur.</p> <p data-bbox="494 1078 1174 1133">Web Console server – hosts the Web site for the Web Console computers.</p> |

| Software Component | Purpose |
|--|--|
| <p data-bbox="252 233 373 258">Databases</p>  | <p data-bbox="538 233 1202 321">Databases located on the database server store real-time events and alerts, report data resulting from Forensic Analysis queries, and configuration data.</p> <p data-bbox="538 331 1147 474">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.</p> |
| <p data-bbox="252 508 467 532">Log archive server</p>  | <p data-bbox="538 508 1229 621">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.</p> |
| <p data-bbox="252 782 447 807">Reporting server</p>  | <p data-bbox="538 782 1229 896">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.</p> <p data-bbox="538 906 1229 993">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.</p> <p data-bbox="538 1003 1216 1058">The cube depot is the staging database that receives exported log archive data and uploads it into the reporting cube.</p> |

| Software Component | Purpose |
|--|---|
| <p data-bbox="206 237 314 261">Consoles</p>  | <p data-bbox="491 237 1089 261">The consoles present information for different purposes:</p> <p data-bbox="491 272 1180 386">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.</p> <p data-bbox="491 397 1177 479">Development Console – customize processing rules, computer groups, and other Security Manager components for your environment.</p> <p data-bbox="491 490 1116 547">Web Console – monitor and resolve alerts about real-time events using Microsoft Internet Explorer.</p> |

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.

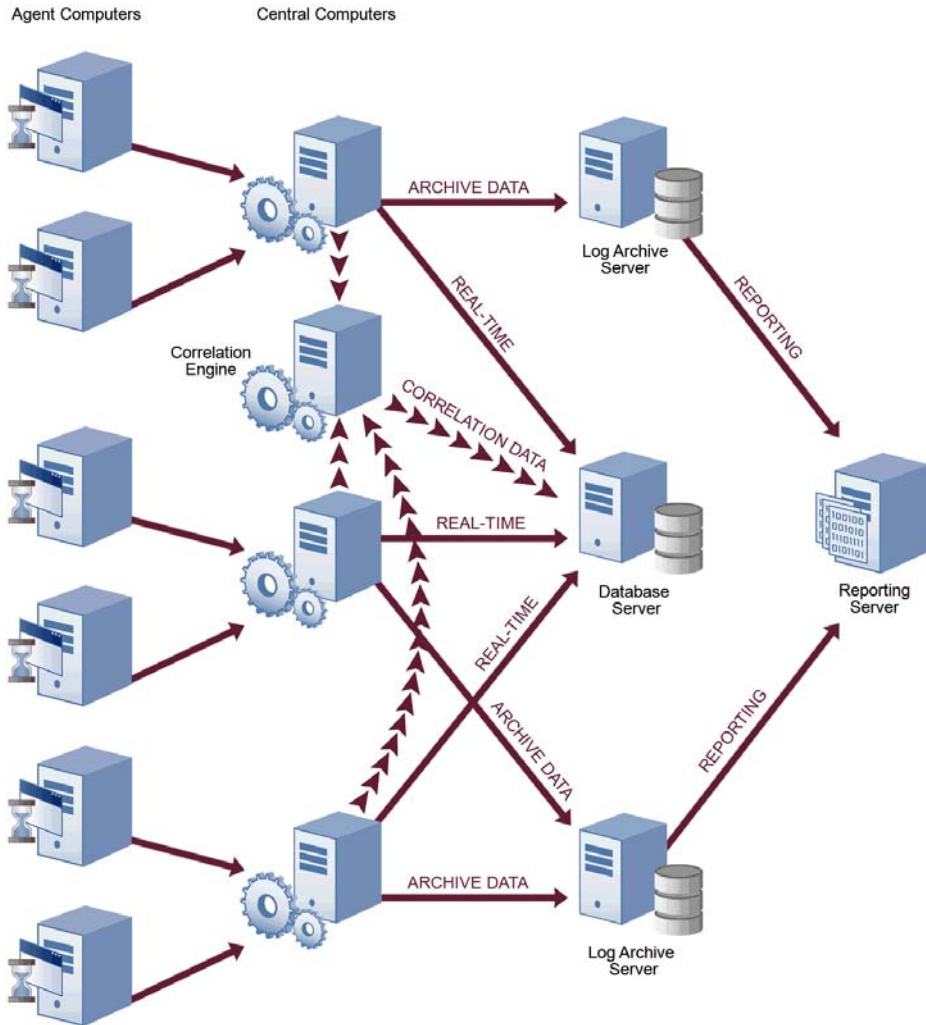
A choice of configuration options is especially important in large distributed enterprises or when communicating over slower network links, such as WANs. In some environments, you may want to optimize load balancing and performance by installing multiple configuration groups.

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 |
|--|---|
| <p data-bbox="252 781 467 805">Central computers</p>  | <p data-bbox="521 781 1180 837">Agent Manager – installs, configures, identifies, updates, and uninstalls agents on Windows computers.</p> <p data-bbox="521 849 1224 1019">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.</p> <p data-bbox="521 1031 1228 1144">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.</p> <p data-bbox="521 1156 1180 1213">Data Access Server – interacts with the database server and provides database access control.</p> <p data-bbox="521 1224 1197 1248">Log Engine – collects event data for Forensic Analysis reports.</p> <p data-bbox="521 1260 1220 1317">Web Console server – hosts the Web Console server, which is a Web site that provides alerts to the Web Console.</p> |

| Computer Roles | Software Components |
|---|---|
| <p data-bbox="205 237 413 318">Central computer selected as Correlation server</p>  | <p data-bbox="474 237 1126 318">Correlation Engine – correlates events across multiple entry points to detect complex attacks and generates responses (memory-intensive).</p> <p data-bbox="474 334 1177 443">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.</p> |
| <p data-bbox="205 570 397 594">Reporting server</p>  | <p data-bbox="474 570 1177 651">Reporting cube – stores summarized log archive data from the log archive server for use in Trend Analysis reports and in custom Summary reports.</p> <p data-bbox="474 667 1143 748">Cube depot – acts as a staging database for log archive data using a scheduled SQL Server Integration Services package to update the reporting cube.</p> |
| <p data-bbox="205 837 391 862">Database server</p>  | <p data-bbox="474 837 1085 886">OnePoint database – stores real-time alerts, events, and configuration data.</p> <p data-bbox="474 902 1173 984">LogManagerConfiguration database – stores configuration data about NetIQ UNIX Agent (UNIX agent) and NetIQ Security Agent for iSeries (iSeries agent) for use by Security Manager.</p> <p data-bbox="474 1000 1163 1081">SecurityManagerCommon database – stores user settings, Favorites, and Incident Packages for the configuration group and connected configuration groups.</p> <p data-bbox="474 1097 1177 1203">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.</p> |

| Computer Roles | Software Components |
|--|--|
| <p data-bbox="252 235 467 259">Log archive server</p>  | <p data-bbox="521 235 1180 289">Log archives – associated with one or more specified central computers to store daily log data (I/O-intensive).</p> <p data-bbox="521 305 1212 354">Fast disk access, multiple physical devices, and RAID arrays are recommended for most environments.</p> |

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:

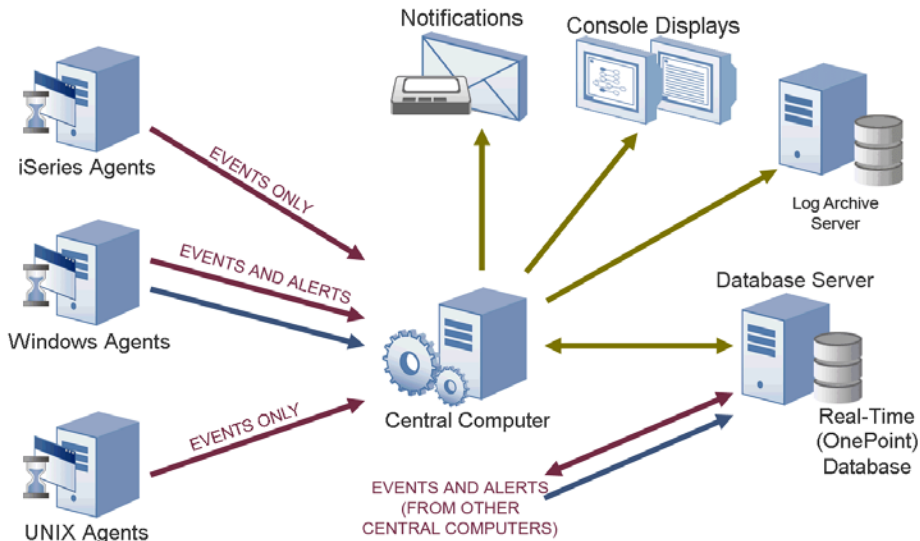
- Inform you about the current state of security (real-time alerts and events)
- Identify events indicating complex threats (correlated real-time events)
- Research significant historical security incidents (log data)
- Understand current security and trends (reporting data)

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.

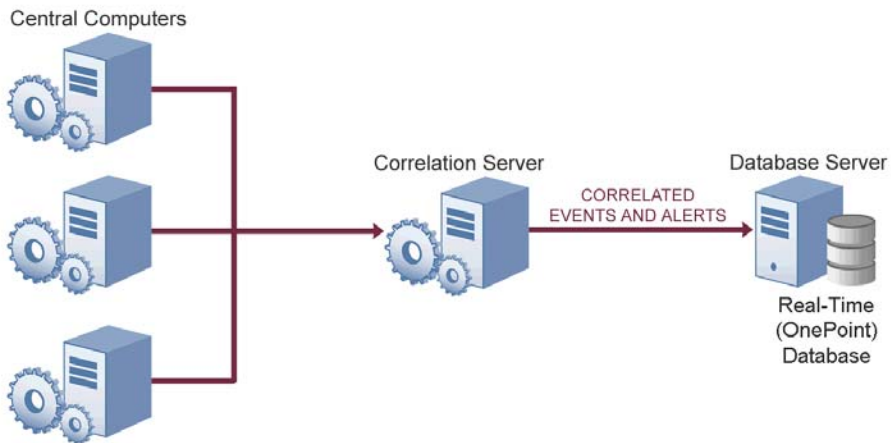
The central computers also send alert and event data to the log archive server for storage in the log archive. You can manage the automatic grooming settings for the log archive from the Log Archive Configuration utility.

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.

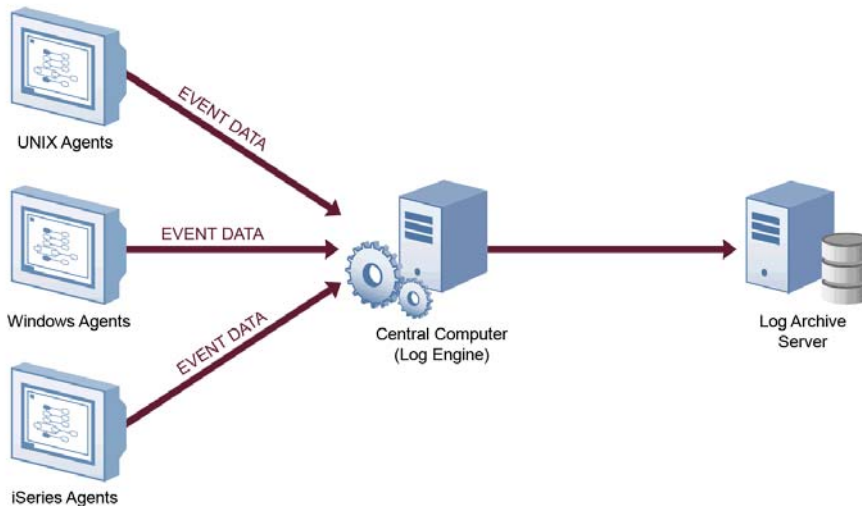


A **correlation rule** is a set of criteria that configures Security Manager to detect a pattern of real-time events and respond accordingly. The Correlation server evaluates collected alerts and events against the correlation rules as data arrives. When a rule match occurs, the Correlation server responds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



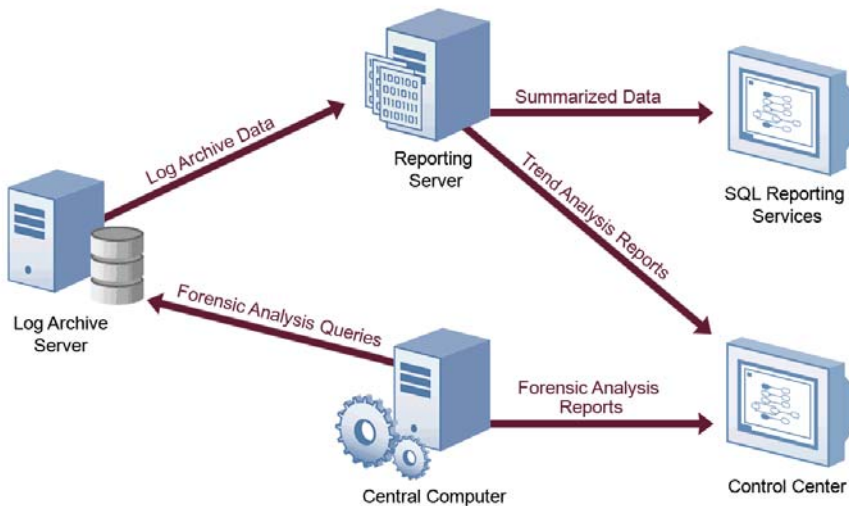
The Log Engine receives the event data and sends it to a log archive for storage. Each central computer receives only a portion of the log data, so the Log Engine on each central computer transfers its portion to a log archive on a dedicated log archive server.

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.

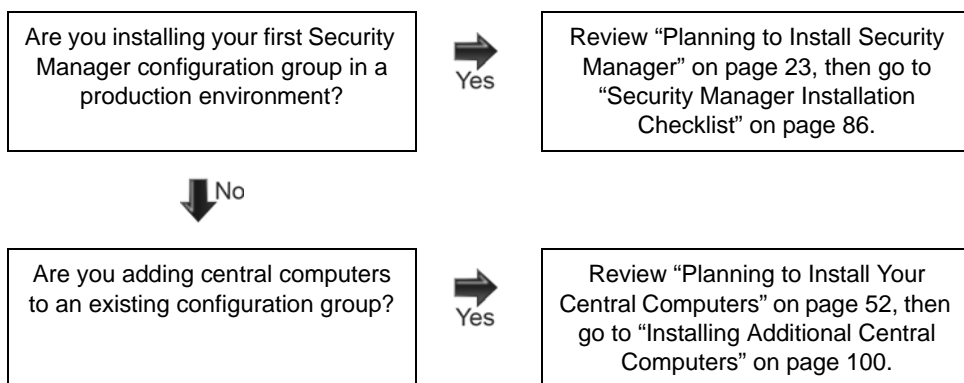
Chapter 2

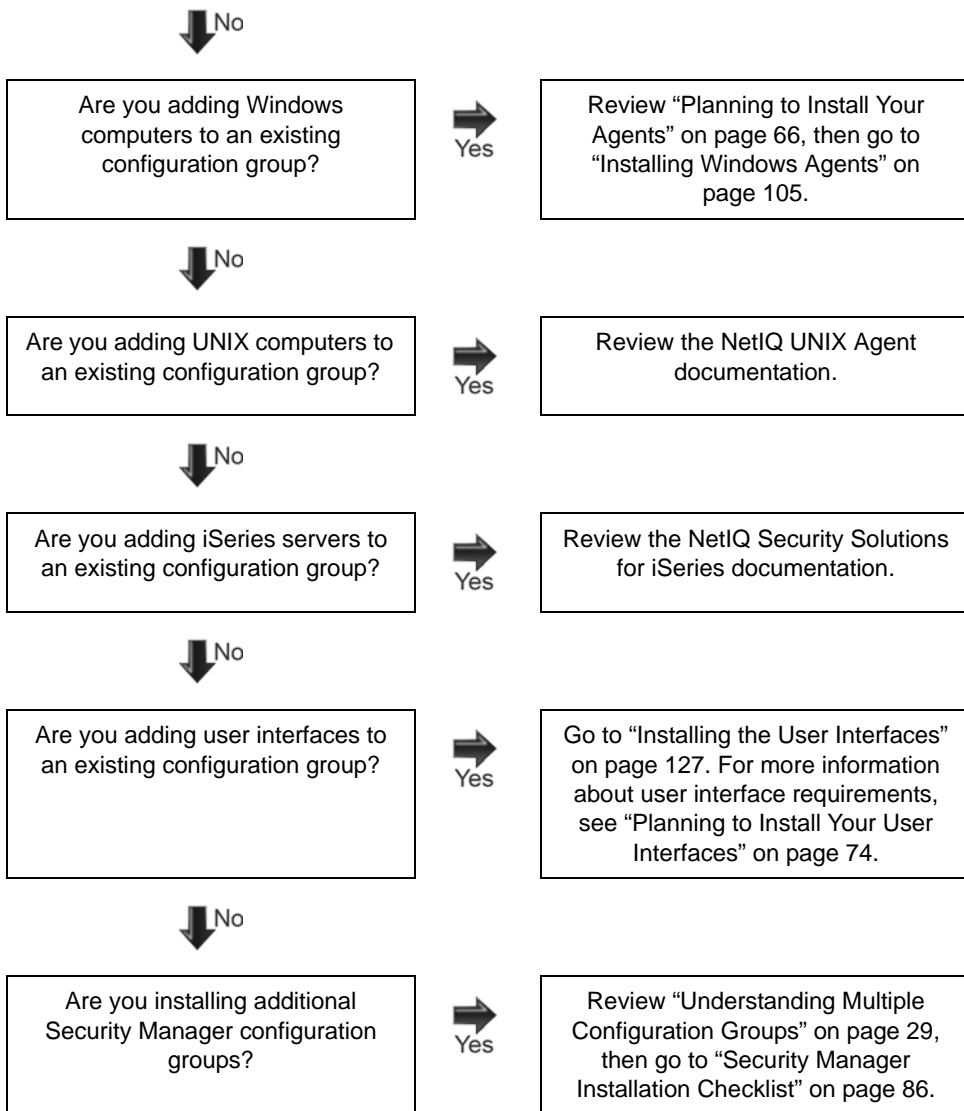
Planning to Install Security Manager

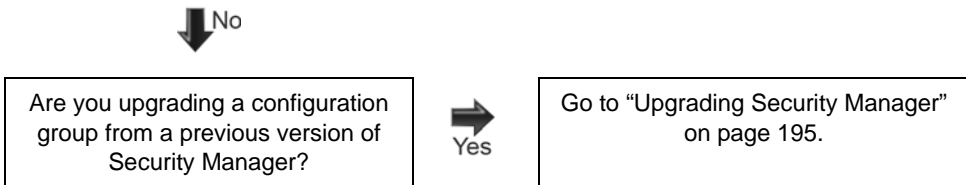
This chapter guides you through the planning issues to consider before installing Security Manager. If you want to install a configuration that is not identified in the sections that follow, or if you have any questions, contact NetIQ Technical Support.

Getting Started

The following flowchart helps you identify common Security Manager installation paths. Use the flowchart to determine the appropriate section of this book for the type of installation task you want to perform.







Implementation Checklist

Use the following checklist as a guide to the planning, installation, and configuration steps required to install Security Manager. For detailed installation checklists, see Chapter 3, “Installing Security Manager,” Chapter 4, “Manually Installing Unmanaged Windows Agents,” and Chapter 5, “Installing the User Interfaces.”

| <input checked="" type="checkbox"/> | Steps | See Section |
|-------------------------------------|---|---|
| <input type="checkbox"/> | 1. Plan to roll out your first configuration group. | “Planning to Roll Out Your Configuration Groups” on page 26 |
| <input type="checkbox"/> | 2. Install and configure Microsoft SQL Server on the database server. | “Installing Microsoft SQL Server” on page 33 “Configuring Microsoft SQL Server” on page 37 |
| <input type="checkbox"/> | 3. <i>If you are installing a reporting server</i> , install and configure Microsoft SQL Server, Microsoft SQL Server Database Services, Microsoft SQL Server Analysis Services, Microsoft SQL Server Integration Services, and Microsoft SQL Server Reporting Services on reporting server computers. | “Installing Microsoft SQL Server” on page 33 “Configuring Microsoft SQL Server” on page 37 “Planning to Install Your Reporting Server” on page 61 |

| <input checked="" type="checkbox"/> | Steps | See Section |
|-------------------------------------|--|--|
| <input type="checkbox"/> | 4. Review Security Manager groups and decide which domain groups to add to each Security Manager group. | "Understanding Security Manager Requirements and Permissions" on page 79 |
| <input type="checkbox"/> | 5. Create the global domain groups you will add to the Security Manager roles. | "Understanding Security Manager Requirements and Permissions" on page 79 |
| <input type="checkbox"/> | 6. Review default ports used by Security Manager and ensure appropriate ports are open for proper communication between Security Manager components. | "Installing and Configuring Security Manager in Firewall Environments" on page 161 |
| <input type="checkbox"/> | 7. Roll out your first configuration group. | "Security Manager Installation Checklist" on page 86 |
| <input type="checkbox"/> | 8. Roll out additional configuration groups. | "Rolling Out Additional Configuration Groups" on page 117 |
| <input type="checkbox"/> | 9. Verify your installation, customize, and begin using Security Manager. | "What to Do Next" on page 133 |

Planning to Roll Out Your Configuration Groups

Ensure you have reviewed "How Security Manager Works" on page 5 before planning the installation of your configuration groups. "How Security Manager Works" provides an overview of the product architecture, including configuration groups and data flow.

Configuration groups include the following computers:

Log archive servers

A configuration group includes one or more log archive servers. Each central computer must connect to a log archive, which is typically stored on a separate computer called a log archive server. For more information about log archives, see “Planning to Install Your Log Archive Servers” on page 47.

Database server

A configuration group includes a single database server. The database server includes the OnePoint, LogManagerConfiguration, and SecurityManagerCommon databases, depending on your configuration, in a Microsoft SQL Server repository. For more information about the database server, see “Planning to Install Your Database Server” on page 44.

Central computers

A configuration group includes one or more central computers. A central computer manages Security Manager components and the collected data. The central computer performs the following functions:

- Installs, uninstalls, and configures Windows agents
- Distributes rules to Windows agent computers
- Registers UNIX and iSeries agents
- Receives data from Windows, UNIX, and iSeries agents
- Controls data flow between all agents and the database server
- Can send log data to the log archives for archival and reporting
- Can provide data correlation for events across single or multiple sources
- Can host the Web Console server component

For more information about the central computer and its components, see “Planning to Install Your Central Computers” on page 52.

Reporting server

A configuration group includes a single reporting server. The reporting server gathers data from daily log archive partitions 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 summarized data for Trend Analysis reports and can also provide data for custom Summary reports created using SQL Server Business Intelligence Development Studio. For more information about the reporting server, see “Planning to Install Your Reporting Server” on page 61.

Agent computers

Includes Windows agent computers, UNIX agent computers, and iSeries agent computers, which send events to the central computer. For more information about agents, see “Planning to Install Your Agents” on page 66.

User interface computers

A configuration group can include computers that have Security Manager user interface components installed. You can install these user interfaces on computers with other Security Manager components already installed. The Security Manager user interfaces you can install are the Control Center, the Development Console, and the Web Console. For more information about user interface computers, see “Installing the User Interfaces” on page 127.

This section guides you through the planning process, helping you determine how many configuration groups you need and plan for each of the configuration group computers.

Notes

- Security Manager supports installing all components on both Microsoft Windows Server 2003 or Microsoft Windows Server 2008. However, NetIQ recommends you install all central computers, log archive servers, database servers, and reporting servers in a configuration group on computers using the same version of Microsoft Windows.
- In addition to installing Security Manager on physical computers, you can install Security Manager components on one or more virtual machines (VMs) and use Security Manager to monitor VMs.

However, due to the nature of shared resources in a virtual machine environment, if you install Security Manager on shared virtual machine hardware, you may experience performance issues while running Security Manager. NetIQ recommends you install Security Manager components on dedicated hardware, whether physical computers or virtual machine hardware.

- If you want to install Security Manager components on VMs, NetIQ also recommends you either use raw device mapping files (RDMs) to map the virtual disk or disks to a physical disk volume or, if you want to use virtual machine disk format files (VMDKs), ensure the datastore you want to use for the virtual machine or machines contains only one VMDK.
 - For performance reasons, NetIQ does not recommend installing Security Manager central computer components or the database server on a computer with a NetIQ Secure Configuration Manager or NetIQ Aegis core component already installed.
-

Understanding Multiple Configuration Groups

Decide how many configuration groups your enterprise requires, then roll out one configuration group at a time. Each configuration group must have a unique name.

A Windows agent can send data to more than one configuration group. For example, a Windows agent on one computer can collect Trend Micro ScanMail for Microsoft Exchange data for one configuration group and Windows XP security data for another configuration group.

Note

If you configure custom agent and system shares for an agent sending data to multiple configuration groups, ensure you specify the same shares for all configuration groups.

An iSeries agent can send data to only one configuration group. A UNIX agent can send data to multiple configuration groups for real-time monitoring, but not for correlation or log archival purposes. For more information about configuring a UNIX agent for multiple configuration groups, see the NetIQ UNIX Agent documentation, available in the NetIQ UNIX Agent installation kit.

The following list provides a few examples of why you might want more than one configuration group in your enterprise:

- Large number of monitored computers
- Dispersed geographic locations
- Diverse organizational departments
- Limited network bandwidth

Number of Monitored Computers

If you want to monitor more than 5,000 computers, consider installing multiple configuration groups. Because you can deploy Security Manager in a wide variety of situations, no simple formula exists to determine the number of agents one central computer or one configuration group can support. The number of agents depends on the hardware of the database server and the central computers.

The number of agents also depends on the log archive servers, the amount of data you are collecting, and the bandwidth of your network.

Geographic Locations

If you have multiple sites in your enterprise and these sites are geographically separated, you might want to install a configuration group at each location. You can store each site's data locally and independent from data at other sites.

Organizational Departments

You might want to separate the data collected by different organizational departments. For example, one organizational department might collect data associated with monitoring Trend Micro ScanMail. Another might collect data associated with monitoring Windows XP security. You can separate data required for each of these organizational departments by installing separate configuration groups.

Network Bandwidth

If you have a remote site that connects to a main site through a limited-bandwidth network connection, you might want to install a separate configuration group at the remote site. The configuration group at the remote site can collect data for the remote site.

Monitoring Multiple Configuration Groups

You can use the Control Center to monitor multiple configuration groups. The Control Center provides views that display alerts or events for one or more configuration groups. The Control Center also provides reports that you can run against a certain configuration group. For more information about monitoring multiple configuration groups, see the *User Guide for NetIQ Security Manager*.

Enabling Multiple Configuration Groups on Unmanaged Agents

When you install an unmanaged agent, you specify the primary configuration group for the unmanaged agent. After unmanaged agent installation is complete, you can specify additional configuration groups. For more information about adding configuration groups, see “Monitoring Agents with Multiple Configuration Groups” on page 134. For more information about upgrading unmanaged agents with multiple configuration groups, see “Upgrading Unmanaged Windows Agents” on page 210.

Enabling Multiple Configuration Groups on Managed Agents

To add configuration groups to a managed agent, assign the managed agent to a central computer in each configuration group with the Agent Administrator. An instance of Agent Administrator manages agents only for the configuration group in which it is installed. For more information about assigning an existing agent to a central computer, see the *User Guide for NetIQ Security Manager*.

Understanding Licensing

Security Manager requires a single console license for using the various product consoles and interfaces. Each module you use requires a separate license. The specific license you require depends on monitoring and logging features and the number of agents you want to install. For more information about licensing Security Manager, contact your NetIQ sales representative.

Supporting Foreign Languages

Security Manager supports Microsoft Windows and Microsoft SQL Server in English and Western European languages. The log archive servers, database server, central computers, and reporting server must all use the same language for Microsoft Windows and Microsoft SQL Server.

Naming Your Configuration Groups

Each configuration group in an enterprise must have a unique name. Security Manager uses this name to distinguish one configuration group from another.

Once you name a configuration group, you cannot change the name without uninstalling, then reinstalling all Security Manager components, including all agents.

Select a unique name for your configuration group. Configuration group names cannot exceed 50 characters.

Understanding Configuration Group Passwords

Multiple central computers in a configuration group share configuration data. The data resides in a central OnePoint database in a single configuration group. This information is encrypted. To enable computers to access the shared information, each central computer must have access to a shared encryption key.

During installation of the first central computer in a configuration group, the setup program prompts you to supply a configuration group password. When you install additional central computers in the configuration group, the setup program prompts you for a configuration group password. Provide the same password you supplied when installing the first central computer. If you provide a different password, the central computer is unable to access shared information. For more information about changing this password, see the *User Guide for NetIQ Security Manager*.

Installing Microsoft SQL Server

Install Microsoft SQL Server on the database server and, if you plan to install Security Manager log management and reporting components, on the computer you want to use as the reporting server. Security Manager supports Microsoft SQL Server 2008 R2, Microsoft SQL Server 2008, or Microsoft SQL Server 2005 with Service Pack 3.

For best performance in a production environment, install Microsoft SQL Server on a dedicated computer. For more information about Microsoft SQL Server performance, see the Microsoft SQL Server documentation and the Microsoft SQL Server Web site at www.microsoft.com/sql.

Security Manager supports clustered and named instances of the Standard and Enterprise versions of Microsoft SQL Server. You can specify named instances during installation of both database server and reporting server components.

Notes

- Security Manager supports using SQL aliases when installing the reporting cube. However, Security Manager does not support using SQL aliases when installing the database server.
 - NetIQ recommends installing Microsoft SQL Server Enterprise Edition on your database server and reporting server. Microsoft SQL Server Standard Edition does not support multiple partitions. If you install the Security Manager reporting server on a computer with an instance of Microsoft SQL Server Standard Edition installed, Security Manager cannot groom old reporting data out of the reporting cube. Without the ability to groom old reporting data, the reporting cube can grow to a size where the reporting server can longer process incoming data.
 - If you install Microsoft SQL Server 2008 R2, ensure you also install Service Pack 1 and all Cumulative Updates before installing Security Manager reporting components.
-

Whether you install Microsoft SQL Server or use an existing Microsoft SQL Server implementation, ensure the implementation supports the following requirements:

- TCP/IP network protocol. By default, the Microsoft SQL Server setup program installs and configures the Net-Libraries to listen and respond to clients using the TCP/IP protocol. Ensure you configure Microsoft SQL Server on the database server and reporting server to use TCP/IP as the primary protocol. For more information about protocol support or enabling TCP/IP, see the Microsoft SQL Server documentation.
- Audit level set to None or Failure
- Dictionary order, case-insensitive sort order

For reporting servers, ensure the Microsoft SQL Server implementation includes these additional components:

- Microsoft SQL Server Database Services
- Microsoft SQL Server Analysis Services (SSAS)

- Microsoft SQL Server Integration Services (SSIS)
- Microsoft SQL Server Reporting Services (SSRS)
- Microsoft SQL Server 2008 Client Tools SDK or Microsoft SQL Server 2005 Software Development Kit
- Microsoft Analysis Management Objects (AMO)

Warning

Ensure you install all Microsoft SQL Server components at once. If you install some components during the initial setup and try to add other Microsoft SQL Server components later, your Microsoft SQL Server installation may not function properly.

For more information about version requirements for installing the reporting server, see “Reporting Server System Requirements” on page 62.

Note

The Security Manager setup program uses OLE Automation to validate the file system during database installations on the database server and reporting server. If OLE Automation is not already “on,” Security Manager turns it “on” for the installation, and then turns it “off” when installation is complete.

You can install Microsoft SQL Server using several licensing options. The Microsoft SQL Server processor licensing option includes unlimited access for users connecting from within the enterprise, the Internet, or between the firewall and the internal network. For more information about obtaining processor licensing or about other licensing options, see the Microsoft Web site or your Microsoft SQL Server documentation.

For more information about installing Microsoft SQL Server, see the Microsoft SQL Server documentation.

Installing Database Components in a Clustered Environment

Security Manager supports clustered instances of the Standard and Enterprise versions of Microsoft SQL Server. Security Manager supports both failover (active/passive) and multi-instance (active/active) SQL Server clustering for database and reporting server components.

If you want to install Security Manager database server components in a clustered environment, specify the cluster name instead of the database server name during installation and continue installing Security Manager as usual.

You can also install Security Manager reporting server components in a clustered environment. However, you must install specific Security Manager files and components on each node in a cluster. For more information about installing the Security Manager reporting server on Microsoft SQL Server cluster, see “Installing Reporting Components in Clustered Environments” on page 175.

For more information about clustered instances of Microsoft SQL Server, see the Microsoft SQL Server documentation and the Microsoft SQL Server Web site at www.microsoft.com/sql.

Understanding Microsoft SQL Server Permissions

When you install the Security Manager database server or reporting server components, the setup program automatically grants specific Microsoft SQL Server roles to the Security Manager service account you specify, as well as to the SQL Server Analysis Services service account. These roles represent the minimum level of permissions required in SQL Server for Security Manager to function.

The setup program grants the following roles to the following accounts:

Database Server (main service account)

public server role

bulkadmin server role

db_owner role in the OnePoint, LogManagerConfiguration, and SecurityManagerCommon databases

Reporting Server (main service account)

public server role

db_owner role in the SMCubeDepot database

db_dtsadmin role in the msdb database

Reporting Server (SQL Server Analysis Services service account)
db_owner role in the SMCubeDepot database

Note

You must use an account that is a member of the Microsoft SQL Server sysadmin role on the database server to use the Access Configuration utility.

Configuring Microsoft SQL Server

Before installing Security Manager, NetIQ recommends you configure Microsoft SQL Server to allow Security Manager components that use SQL Server to function properly.

Enabling and Starting the SQL Server Agent

Ensure the SQL Server Agent is running. Security Manager provides preconfigured SQL Server jobs for performing various functions in the OnePoint database and reporting cube. The SQL Server Agent runs these jobs on the database server and reporting server.

If you do not enable and start the SQL Server Agent, SQL Server does not automatically groom your databases or upload log archive data into the reporting cube. For more information about configuring Security Manager jobs in SQL Server after installation, see the *User Guide for NetIQ Security Manager*.

To enable and start the SQL Server Agent:

1. Log on to the database or reporting server using an account that is a member of the Microsoft SQL Server sysadmin role. For more information about SQL permissions, see the Microsoft SQL Server Help.
2. Start **SQL Server Configuration Manager**, located in either the Microsoft SQL Server 2008 or Microsoft SQL Server 2005 program group.
3. *If your database server uses SQL Server 2008 or SQL Server 2008 R2*, in the left pane, click **SQL Server Services**.
4. *If your database server uses SQL Server 2005*, in the left pane, click **SQL Server 2005 Services**.

5. In the right pane, click **SQL Server Agent**.
6. On the Action menu, click **Properties**.
7. Click the Service tab.
8. Click **Start Mode** and select **Automatic**.
9. Click **Apply** and then click **OK**.
10. *If the SQL Server Agent is stopped*, complete the following steps:
 - a. In the right pane, click **SQL Server Agent**.
 - b. On the Action menu, click **Start**.
11. Close SQL Server Configuration Manager.

Enabling and Starting the SQL Server Browser

NetIQ also recommends enabling and starting the SQL Server Browser in most SQL Server installations. Security Manager uses the SQL Server Browser to resolve named instances of SQL Server.

If you choose not to enable or start the SQL Server Browser on your database or reporting servers, when you install Security Manager, you must specify both the SQL Server computer name in NetBIOS format and the port used by Microsoft SQL Server.

For more information about specifying databases names and ports during installation, see the setup program Help.

To enable and start the SQL Server Browser:

1. Log on to the database or reporting server using an account that is a member of the Microsoft SQL Server `sysadmin` role. For more information about SQL permissions, see the Microsoft SQL Server Help.
2. Start **SQL Server Configuration Manager**, located in either the Microsoft SQL Server 2008 or Microsoft SQL Server 2005 program group.
3. *If your database server uses SQL Server 2008 or SQL Server 2008 R2*, in the left pane, click **SQL Server Services**.

4. *If your database server uses SQL Server 2005*, in the left pane, click **SQL Server 2005 Services**.
5. In the right pane, click **SQL Server Browser**.
6. On the Action menu, click **Properties**.
7. Click the Service tab.
8. Click **Start Mode** and select **Automatic**.
9. Click **Apply** and then click **OK**.
10. *If the SQL Server Browser is stopped*, complete the following steps:
 - a. In the right pane, click **SQL Server Browser**.
 - b. On the Action menu, click **Start**.
11. Close SQL Server Configuration Manager.

Estimating Database Sizes

Use the information in this section to estimate the size of your Microsoft SQL Server databases to determine disk space requirements. This section provides methods for estimating the size of your database server databases and reporting cube databases.

Estimating Reporting Server Database Sizes

Configure one computer in a configuration group to act as the reporting server. The reporting server runs Microsoft SQL Server Analysis Services, which uses the data in the reporting cube depot database to create a cube for Trend Analysis and Summary reporting.

Estimating Reporting Cube Database Size

Estimating the size of the reporting cube database cannot be done using a simple formula. The size is highly dependent on the variability of the data. In other words, the size of data being added to the cube depends on whether the data values are new values or repetitions of existing values. Estimate the reporting cube database size to be in the range of 10-35% of the total size of all log archives in a configuration group. For example, if the log archives estimate equals 270 GB, the computer that serves as the reporting server will need between 27 and 94.5 GB of storage.

A size near the lower 10% number will be more common. The cube size required for an environment increases as the number of firewall and other network devices sending large amounts of complex data increases. Because the data content and the resulting size of the reporting cube are difficult to predict, monitor the reporting cube size over time. You may want to evaluate and decrease your data retention period to reduce size requirements.

Estimating Cube Depot Database Size

The reporting cube depot is a staging database that holds only a few hours of data at a time, and should not grow long-term. Data collected and stored in the log archives is uploaded to the cube depot, and then processed into the reporting cube periodically, every three hours by default. The size of the cube depot is primarily dependent on the events/second rate and the cube processing interval.

This section provides a sample worksheet for computing the size of your cube depot. The following factors are likely to affect cube depot size:

Events per second

The events per second rate is the number of events received by Security Manager from all data sources in your environment in one second. Typical data sources include domain servers, email servers, print servers, file servers, application servers, routers, and firewalls.

Number of source log archives

The number of log archives sending data to the cube depot is a simple multiplier for the data coming in the cube depot. You may only have one log archive that was created by the installation program.

Processing interval

Specify the number of hours between each processing of cube depot data into the reporting cube. This processing occurs every three hours by default.

To create an estimate, review the sample worksheet and complete the values in the second worksheet as appropriate for your enterprise.

| Sample Worksheet | | |
|--|---|---------------|
| Events per second | | 1500 |
| Seconds per hour | x | 3600 |
| Processing interval (hours) | x | 3 |
| Average size of an event (bytes) | x | 300 |
| Number of source log archives | x | 1 |
| Safety margin | x | 1.15 |
| Total cube depot required size (bytes) | = | 5,589,000,000 |
| Total cube depot size required (gigabytes) | = | 5.59 GB |

| My Worksheet | | |
|--|---|------|
| Events per second | | |
| Seconds per hour | x | 3600 |
| Processing interval (hours) | x | |
| Average size of event (bytes) | x | 300 |
| Number of source log archives | x | |
| Safety margin | x | 1.15 |
| Total cube depot required size (bytes) | = | |
| Total cube depot size required (gigabytes) | = | |

Estimating Database Server Database Sizes

For Security Manager installations, configure one computer in a configuration group to act as the database server. The database server hosts the OnePoint database, the LogManagerConfiguration database, and the SecurityManagerCommon database, depending on your configuration, in a Microsoft SQL Server repository. The SecurityManagerCommon database is of negligible size, but you may want to consider the size of the other two databases:

OnePoint database

The OnePoint database is 2 GB by default. The OnePoint database contains real-time event and alert data and your custom Forensic Analysis queries. If you receive a large number of real-time events and alerts or create a large number of queries, you may need to expand the OnePoint database.

LogManagerConfiguration database

The LogManagerConfiguration database contains your completed Forensic Analysis reports. The size varies depending on the number of queries you run.

Estimating Log Archive Size

Use the information in this section to estimate the size of your log archives to determine disk space requirements. This section provides a sample worksheet for computing the size of your log archives.

Each log archive stores raw data collected from monitored data sources in your enterprise.

The following factors are likely to affect log archive size:

Number of days before grooming

Security Manager stores log archive data in daily log archive partitions. To reclaim disk space, Security Manager grooms or removes log archive partitions that are older than a specified time period, which is 90 days by default. If you want to reduce log archive size and hardware requirements, consider reducing the number of days before grooming in the Log Archive Configuration utility. For more information about modifying grooming settings, see the *User Guide for NetIQ Security Manager*.

Data sources

Typical data sources include domain servers, email servers, print servers, file servers, application servers, routers, and firewalls. The number of data sources you specify in the worksheet affects log archive size.

Average number of events per data source per day

Use native log viewers, such as the Windows Event Viewer, to estimate an average number of events per day based on several days of observation. Specify the average number of events for each data source per day in the worksheet.

To create an estimate, write your answers in the following worksheet. Modify the estimate as appropriate for your enterprise.

| Sample Worksheet | | |
|--|---|-----------------|
| Number of days in data retention period | | 90 |
| Number of data sources | x | 200 |
| Number of events per data source per day | x | 40,000 |
| Average event size in archive (bytes) | x | 300 |
| Safety margin | x | 1.25 |
| Number of indexing processes [2] x 32 GB (bytes) | + | 64,000,000,000 |
| Total log archive size required (bytes) | = | 334,000,000,000 |
| Total log archive size required (gigabytes) | = | 334 GB |

| My Worksheet | | |
|--|---|------|
| Number of days in data retention period | | |
| Number of data sources | x | |
| Number of events per data source per day | x | |
| Average event size in archive (bytes) | x | 300 |
| Safety margin | x | 1.25 |

| My Worksheet | | |
|--|---|--|
| Number of indexing processes [M] x 32 GB (bytes) | + | |
| Total log archive size required (bytes) | = | |
| Total log archive size required (gigabytes) | = | |

Planning to Install Your Database Server

A configuration group includes a single database server. The database server includes the OnePoint database, LogManagerConfiguration database, and the SecurityManagerCommon database.

Note

Do not install the database server on a central computer.

Because you can deploy Security Manager in a wide variety of situations, there is no simple formula for determining database server location and required hardware.

The database server should be a server-class computer and should be located to allow maximum bandwidth between the database server and the central computers in its configuration group.

Depending on your event rate and number of computers or devices you are monitoring, you may be able to obtain adequate performance running the product on lesser equipment. Consider conducting a pilot study to determine the event load in your environment.

The following table lists system requirements and recommendations for the database server.

| Category | Requirements |
|-----------------|---|
| Processor | Dual processor dual-core AMD/Intel configuration recommended. Quad processors recommended in environments expecting more than one million total events per day. |

| Category | Requirements |
|------------------|--|
| Disk Space | <ul style="list-style-type: none"> • Ensure you have adequate disk space based on the event load estimated for your environment. For more information about disk space requirements, see “Estimating Database Server Database Sizes” on page 42. • Fast disk access, multiple physical devices, and RAID arrays recommended for most environments. |
| Memory | 4 GB recommended. |
| Operating System | <ul style="list-style-type: none"> • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2008 (32- and 64-bit) • Microsoft Windows Server 2003 Service Pack 2 (32- and 64-bit) |

| Category | Requirements |
|----------------|--|
| Network Access | <ul style="list-style-type: none"> • Install in a domain environment with access to a domain controller. Do not change the domain of the database server computer after installing Security Manager. • 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. • Ensure the domain containing the database server trusts the domain in which the service account is a member. A service account is a Windows security account used by services to log on to a Windows computer. • On Windows Server 2003 and Windows Server 2008 computers, ensure you enable MSDTC and configure Network DTC Access in the Component Services administrative tool to enable the following minimum required settings: <ul style="list-style-type: none"> • Allow Remote Clients • Allow Inbound • Allow Outbound • Mutual Authentication Required <p>You must specify the same type of authentication for all Security Manager components in order for Windows servers to communicate with one another.</p> <p>For more information about configuring DTC security, see the Help for Component Services. For more information about configuring Security Manager to work with firewalls, see “Installing and Configuring Security Manager in Firewall Environments” on page 161.</p> |

| Category | Requirements |
|----------|--|
| Software | <p>The Security Manager setup program provides the Verify Prerequisites tool, from which you can install some of the required software. For more information about the Verify Prerequisites tool, see “Verifying Prerequisites” on page 97.</p> <p>The database server requires the following software:</p> <ul style="list-style-type: none"> • Microsoft SQL Server 2008 R2, Microsoft SQL Server 2008, or Microsoft SQL Server 2005 with Service Pack 3, Standard or Enterprise Edition. For more information about installing Microsoft SQL Server for use with Security Manager, see “Installing Microsoft SQL Server” on page 33. • .NET Framework 2.0 Service Pack 1 or later • Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package |

Notes

- Before installing your Security Manager database server, ensure the SQL Server Agent is running. Security Manager provides preconfigured SQL Server jobs for performing various functions in the OnePoint database. The SQL Server Agent runs these jobs on the database server. For more information about configuring the SQL Server Agent, see “Configuring Microsoft SQL Server” on page 37.
- NetIQ recommends installing the latest Microsoft Windows service packs and hotfixes on all computers before installing Security Manager components.

Planning to Install Your Log Archive Servers

In order to store collected data, you must configure each central computer to connect to one or more log archive servers. Install a log archive server on a separate computer before installing other Security Manager components.

The Security Manager service account creates a log archive on the log archive server computer you specify in the setup program or in the Log Archive Configuration utility. The NetIQ Security Manager Log Archive service then creates a new log archive partition each day to store data sent by the associated central computer.

Although it is possible to configure the database server as a log archive server or, in some cases, configure the central computer as a log archive server, these configurations are not recommended for most environments. For optimal performance, configure a separate log archive server computer. For more information about the different configurations available, see “Understanding Configuration Groups” on page 8.

Determine how many log archive servers you will need. Each central computer can connect to its own log archive server or to a log archive server shared with other central computers. While one or more central computers can share a log archive server, a central computer can only connect to one log archive server.

Grooming Log Archives

Each day, Security Manager creates a separate log archive partition that contains that day’s collected events. Security Manager grooms log archives by deleting daily partitions that have expired. Security Manager removes expired log archives early each morning. Consider establishing a process to back up the log archives to a permanent storage location with adequate disk space.

Notes

- Ensure you back up the log archives before Security Manager deletes them. After the log archives are deleted, you cannot retrieve this data.
 - If you want to restore log archives for reports, ensure backed-up log archives retain or can be restored to their original format.
 - When configuring your process for backing up log archive files, NetIQ recommends you back up only the actual `.nds` data files and exclude the `VolumeInfo.xml` file and `index_data` and `CubeExport` subfolders located in the main log archive folder and the `PartitionInfo.xml` files and `index` subfolders located in each log archive partition.
 - If you back up only the `.nds` files in your partitions, when you restore a backed-up log archive partition, you need to reindex your log archive data using the Log Archive Reindexer tool included in the Log Archive Resource Kit. For more information about reindexing log archive data, see the *NetIQ Security Manager Log Archive Resource Kit Technical Reference*.
-

Note that if you restore a groomed log archive partition, Security Manager will not groom the log archive partition a second time. If you want to remove the restored partition, you must do so manually.

If log archives have been deleted and your company has established a backup procedure to permanently archive this data, you may need to restore some data to see Forensic Analysis reports for these dates.

For more information about backing up and restoring log archive partitions and configuring grooming settings, see the *User Guide for NetIQ Security Manager*.

Restricting Permissions on Log Archives

Security Manager creates the first log archive during installation. You can create additional log archives at any time, using the Log Archive Configuration utility. To reduce the possibility of data alterations, you can restrict the permissions on your log archives so that unauthorized users cannot access the data from the file system. Both the setup program and the Log Archive Configuration utility allow you to choose restrictive permissions.

If you choose to restrict permissions on a log archive, members of the OnePointOp ConfigAdms groups and the local Administrator are granted full control. Other users have no access to the log archive from the file system. Setting permissions on a log archive does not affect the ability of users to view log archive data in the Control Center.

Log Archive Server System Requirements

The following table lists system requirements and recommendations for the log archive server.

| Category | Requirements |
|-----------|---|
| Processor | Dual processor dual-core AMD/Intel configuration recommended. Quad processors recommended in environments expecting more than one million total events per day. |

| Category | Requirements |
|------------------|---|
| Disk Space | <ul style="list-style-type: none"> • Ensure you have adequate disk space based on the event load estimated for your environment. For more information about disk space requirements, see “Estimating Log Archive Size” on page 42. • NTFS file system with block size of 4 KB or less. NetIQ does not support using a NAS device for a log archive server. • Fast disk access, multiple dedicated, high-performance physical devices, and RAID arrays are recommended for most environments. <p>NetIQ recommends using a RAID array with 1.5-2 drives with 10-15K RPM spindles and one core per 1200 events per second (EPS) of log archival data.</p> |
| Memory | 4 GB minimum |
| Operating System | <ul style="list-style-type: none"> • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2008 (32- and 64-bit) • Microsoft Windows Server 2003 Service Pack 2 (32- and 64-bit) |
| Network Access | <ul style="list-style-type: none"> • Install in a domain environment with access to a domain controller. • Install in the same domain as the central computer. • 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. |

| Category | Requirements |
|-------------------------|--|
| Software | <p>The Security Manager setup program provides the Verify Prerequisites tool, from which you can install some of the required software. For more information about the Verify Prerequisites tool, see “Verifying Prerequisites” on page 97.</p> <p>The log archive server requires the following software:</p> <ul style="list-style-type: none"> • Microsoft Message Queuing (MSMQ) 3.0 (at least 8 GB) • Microsoft .NET Framework 4.0 or later • Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package • Microsoft Core XML Services (MSXML) 6.0 or later • Microsoft Server Support Tools |
| Additional Requirements | <ul style="list-style-type: none"> • On each log archive server you scan for viruses, configure your antivirus software to exclude from scanning the top-level log archive folder that contains the log archive partitions. For example, exclude the folder C: \NetIQSMLogArchive from virus scanning. • NetIQ also recommends you disable the Windows Indexing Service on all log archive servers before installing Security Manager. • Any computer on which you want to install log archive server components must have a NetBIOS-compliant name. |

Notes

- Although you must install all Security Manager components in a configuration group in domains that trust each other, you can query a log archive server located in an untrusted domain. For more information about querying log archive servers, see the *User Guide for NetIQ Security Manager*.
 - NetIQ recommends installing the latest Microsoft Windows service packs and hotfixes on all computers before installing Security Manager components.
 - If you use different service accounts on the central computer and the log archive server in the same configuration group, ensure the central computer service account is a member of the OnePointOp System group on the log archive server. If the central computer service account does not have sufficient access to the log archive server, Security Manager cannot send MSMQ messages from the central computer to the log archive.
 - After you install the Microsoft Message Queuing prerequisite, NetIQ recommends disabling the Active Directory Integration sub-component of MSMQ. For more information about disabling Active Directory Integration, see “Disabling Active Directory Integration with Message Queuing” on page 93.
-

Planning to Install Your Central Computers

A central computer manages configuration group components and the collected data. Configuration groups can have multiple central computers. The central computer performs the following functions:

- Installs, uninstalls, and configures Windows agents
- Distributes rules to Windows agent computers
- Controls data flow between all agents and the database server
- Can send log data to the log archives for archival and reporting
- Can provide data correlation for events across single or multiple sources
- Can host the Web Console server component

Understanding Central Computer Components

The setup program installs the following Security Manager components on the central computer:

Agent Manager

Installs and configures agents on Windows computers.

Consolidator

Receives collected information from Windows, UNIX, and iSeries agents. Performs central actions specified by processing rules, such as running a script or a batch file or notifying an operator of a detected condition. Forwards information to the Data Access Server (DAS).

If a change occurs to a processing rule that applies to a Windows agent on a Windows computer, the Consolidator ensures that the change reaches the Windows agent. The Consolidator sends processing rules to agents on Windows computers when the Windows agent is installed and whenever the rules change. You can configure how often the Consolidator polls for rule changes.

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.

Correlation Engine

Provides data correlation capability for events across single or multiple sources.

Data Access Server (DAS)

Controls the flow of data between the Windows agents, the database server, the Consolidators, the Control Center, and the Web Console.

Log Engine

The Log Engine is the central computer component that collects event data for Forensic Analysis reports.

Understanding Central Computer Roles

After installing Security Manager, specify one or more of the following roles for a central computer:

Correlation server

The Correlation server is the central computer that hosts the Correlation Engine. The Correlation server uses the Correlation Engine to monitor a stream of events over time, watching for patterns that indicate threatening behavior. By default, the Correlation server is the first central computer installed.

Note

If you licensed the correlation feature, the first central computer you install is the Correlation server. Do not use this computer to manage agents. Install one or more additional central computers to monitor agents, including the central computer monitoring UNIX computers and iSeries servers.

Web Console server

The Web Console server hosts a web site that allows you to view database information from the Web Console user interface, accessible from any Windows computer with Microsoft Internet Explorer. The Web Console provides remote monitoring and easy access for roaming administrators.

You can configure a central computer to act as the Web Console server when you install the central computer. For more information about additional requirements for the Web Console server, see “Central Computer System Requirements” on page 56.

Understanding User Interfaces on the Central Computer

Security Manager user interfaces allow you to view the security details of monitored computers and configure product functionality. You can install the user interfaces on a central computer and on additional computers. For more information about installing user interfaces, see “Installing the User Interfaces” on page 127.

- The Control Center serves as the central monitoring point for multiple configuration groups. The Control Center also provides Trend Analysis reports and Forensic Analysis reports of log data and allows you to configure Security Manager.
- The Development Console provides advanced configuration capabilities for Security Manager through Microsoft Management Console (MMC) snap-ins.
- The Web Console provides views of database information accessible from Windows platforms supporting Microsoft Internet Explorer.

Note

If you plan to install user interfaces on your central computer, be sure to review user interface computer requirements before running the setup program. For more information about user interface computer requirements, see “Planning to Install Your User Interfaces” on page 74.

Multiple Central Computers

Configuration groups can contain more than one central computer. Configuring more than one central computer in a configuration group could be necessary for the following reasons:

Load balancing

When assigning agents to central computers, assign no more agents to the central computer than it can handle.

Note

The number of agents you can assign to a central computer depends on your environment, such as the total number of events you expect agents to send to the central computer. If you need help planning your Security Manager environment, contact NetIQ Technical Support.

Following installation of central computers and agents, you can rebalance the distribution of agents across central computers, using the Agent Administrator to assign agents to different central computers. If you install more than one central computer, use the Agent Administrator to reassign agents among central computers

Redundancy (Failover)

If a central computer fails or a managed or unmanaged agent cannot otherwise contact the central computer, the agent can temporarily send event and alert data to another central computer. If you want to ensure data is delivered to the databases when a central computer is unavailable, you can install multiple central computers for redundancy. The central computer assigned to manage the agent still retains control over the agent for upgrade, installation, and uninstallation purposes. For more information about configuring failover, see “Specifying Central Computers for Failover” on page 110.

Multiple domains

If you want a configuration group to monitor computers in different supported domains and do not want the central computers to share a common service account, you can install multiple central computers, with different service accounts. For more information about creating service accounts, see “Creating a Service Account” on page 89.

Central Computer System Requirements

Because you can deploy Security Manager in a wide variety of situations, there is no simple formula for determining the required number of central computers, their location, or the required hardware. The central computers should be server-class computers and should be located to allow maximum bandwidth between the databases, the central computers, and the agent computers.

Notes

- Do not install the database server on a central computer.
 - You cannot install a central computer on an existing managed agent computer.
-

The following table lists the system requirements and recommendations for the central computers and specifies additional requirements for central computers serving as Correlation or Web Console servers.

| Category | Requirement |
|------------------|---|
| Processor | Dual processor dual-core AMD/Intel configuration recommended. |
| Disk Space | <ul style="list-style-type: none">• Ensure you have adequate disk space based on the event load estimated for your environment.• Fast disk access, multiple physical devices, and RAID arrays recommended for most environments. |
| Memory | 4 GB recommended. |
| Display | 1024 x 768 resolution minimum. |
| Operating System | <ul style="list-style-type: none">• Microsoft Windows Server 2008 R2• Microsoft Windows Server 2008 (32- and 64-bit)• Microsoft Windows Server 2003 Service Pack 2 (32- and 64-bit) |

| Category | Requirement |
|----------------|---|
| Network Access | <ul style="list-style-type: none"> • Install in a domain environment with access to a domain controller. • Install in the same domain as the log archive server. • All other 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. • If installing a central computer behind a firewall, ensure you open the appropriate ports to allow proper communication between the central computer and other Security Manager components. For more information about the default ports Security Manager uses, see “Installing and Configuring Security Manager in Firewall Environments” on page 161. • On Windows Server 2003 and Windows Server 2008 computers, ensure you enable MSDTC and configure Network DTC Access in the Component Services administrative tool to enable the following minimum required settings: <ul style="list-style-type: none"> • Allow Remote Clients • Allow Inbound • Allow Outbound • Mutual Authentication Required <p>You must specify the same type of authentication for all Security Manager components in order for Windows servers to communicate with one another.</p> <p>For more information about configuring DTC security, see the Help for Component Services.</p> |

| Category | Requirement |
|----------|---|
| Software | <p>The Security Manager setup program provides the Verify Prerequisites tool, from which you can install some of the required software. For more information about the Verify Prerequisites tool, see “Verifying Prerequisites” on page 97.</p> <p>The central computer requires the following software:</p> <ul style="list-style-type: none"> • Microsoft Message Queuing (MSMQ) 3.0 • .NET Framework 2.0 Service Pack 1 or later • Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package • Microsoft Core XML Services (MSXML) 6.0 or later • COM+ Network Access for the Application Server • If you want the central computer to serve as the Web Console server, Microsoft Internet Information Services (IIS) 5.0 is required. <p>Consider configuring Internet Information Services to use secure HTTP (HTTPS). For more information about installing the Web Console, see “Web Console Requirements” on page 77.</p> <ul style="list-style-type: none"> • If using a central computer with Microsoft Windows Server 2008 installed as the Web Console server, both IIS 7.0 and the IIS 6.0 Management Compatibility components are required. |

| Category | Requirement |
|-------------------------|---|
| Additional Requirements | <p>On each central computer and agent computer you scan for viruses, configure your antivirus software to exclude from scanning the specified folders and files.</p> <p>On Windows Server 2003 computers, exclude:</p> <ul style="list-style-type: none"> • All files in the service account and All Users user profile folders, <i>USERPROFILE</i>\Application Data\NetIQ, where <i>USERPROFILE</i> is the path to the user profile on the computer. • All *.dat files in the <i>installation folder</i>\NetIQ Security Manager\OnePoint folder, where <i>installation folder</i> is the location where you installed Security Manager user interfaces. <p>On Windows Server 2008 computers, exclude:</p> <ul style="list-style-type: none"> • All files in the ProgramData\NetIQ folder • All *.dat files in the <i>installation folder</i>\NetIQ Security Manager\OnePoint folder, where <i>installation folder</i> is the location where you installed Security Manager user interfaces. • Any computer on which you want to install central computer components must have a NetBIOS-compliant name. |

Notes

- On Windows Server 2003 computers, enable Network COM+ access for the Application Server using the Add/Remove Windows Components wizard, which is available from Add or Remove Programs in the Control Panel.
 - On Windows Server 2008 computers, enable Network COM+ access for the Application Server by using the Server Manager Administrative Tool to install the Application Server role and the COM+ Network Access service.
 - When you install central computer components on a Windows Server 2008 computer, the setup program prompts you to restart the central computer to finish the installation process. The setup program does not require that you restart Windows Server 2003 computers.
 - NetIQ recommends installing the latest Microsoft Windows service packs and hotfixes on all computers before installing Security Manager components.
 - If you use different service accounts on the central computer and the log archive server in the same configuration group, ensure the central computer service account is a member of the OnePointOp System group on the log archive server. If the central computer service account does not have sufficient access to the log archive server, it cannot send MSMQ messages from the central computer to the log archive.
 - After you install the Microsoft Message Queuing prerequisite, NetIQ recommends disabling the Active Directory Integration sub-component of MSMQ. For more information about disabling Active Directory Integration, see “Disabling Active Directory Integration with Message Queuing” on page 93.
-

Planning to Install Your Reporting Server

After Security Manager sends log data from the log archives to the reporting server, the reporting server summarizes the data, stores the summarized reporting data in the reporting cube, and assembles dimension information for Trend Analysis reports. After cube processing is complete, you can view the Trend Analysis report graphs in the Control Center. You can also access reporting cube data directly using Microsoft SQL Server Reporting Services. Reporting cube processing occurs every three hours by default.

Understanding Reporting Server Grooming

Reporting server data is groomed or deleted when it reaches a specified number of days old, which is 365 days by default. Before reporting server cube data is groomed, archive the data for permanent storage using your organization's backup procedure.

Reporting Server System Requirements

The following table lists system requirements and recommendations for the reporting server computer.

| Category | Requirements |
|-----------------|--|
| Processor | Dual processor dual-core AMD/Intel configuration recommended. Quad processors recommended in environments expecting more than one million total events per day. |
| Disk Space | <ul style="list-style-type: none">• Ensure you have adequate disk space based on the event load estimated for your environment. For more information about disk space requirements, see "Estimating Reporting Server Database Sizes" on page 39.• Fast disk access, multiple dedicated, high-performance physical devices, and RAID arrays are recommended for most environments. |
| Memory | 4 GB recommended. |

| Category | Requirements |
|------------------|--|
| Operating System | <ul style="list-style-type: none"> • Microsoft Windows Server 2008 R2 Service Pack 1 • Microsoft Windows Server 2008 (32- and 64-bit) • Microsoft Windows Server 2003 Service Pack 2 (32- and 64-bit) |
| Network Access | <ul style="list-style-type: none"> • Install in a domain environment with access to a domain controller. • 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. |

| Category | Requirements |
|-------------------------|--|
| Software | <p>The Security Manager setup program provides the Verify Prerequisites tool, from which you can install some of the required software. For more information about the Verify Prerequisites tool, see “Verifying Prerequisites” on page 97.</p> <p>The reporting server requires the following software:</p> <ul style="list-style-type: none"> • Microsoft SQL Server 2008 R2, Microsoft SQL Server 2008, or Microsoft SQL Server 2005 with Service Pack 3. Microsoft SQL Server Enterprise Edition is recommended, and is required if you want to groom data from the reporting cube. For more information about installing Microsoft SQL Server for use with Security Manager, see “Installing Microsoft SQL Server” on page 33. • Microsoft SQL Server Database Services • Microsoft SQL Server 2008 Analysis Services or Microsoft SQL Server 2005 Analysis Services with Service Pack 3 • Microsoft SQL Server Integration Services (SSIS) • Microsoft SQL Server Reporting Services (SSRS) • Microsoft Analysis Management Objects (AMO) from Microsoft SQL Server 2008 Feature Pack, October 2008 • Microsoft SQL Server 2008 Client Tools SDK or Microsoft SQL Server 2005 Software Development Kit. You must install the version of the SDK that matches the version of SQL Server you want to use. • .NET Framework 2.0 Service Pack 1 or later • Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package |
| Additional Requirements | <p>Any computer on which you want to install reporting server components must have a NetBIOS-compliant name.</p> |

Notes

- Before installing your Security Manager reporting server, ensure the SQL Server Agent is running. Security Manager provides a preconfigured SQL Server Integration Services job for uploading log archive data from the cube depot to the reporting cube. The SQL Server Agent runs this job on the reporting server. For more information about configuring the SQL Server Agent, see “Configuring Microsoft SQL Server” on page 37.
 - If you want to install Security Manager reporting server components on different SQL Server computers, you must run the setup program from a computer with SQL Server Integration Services and either the Microsoft SQL Server 2008 Client Tools SDK or the Microsoft SQL Server 2005 Software Development Kit, depending on the version of SQL Server you want to use.
 - The Microsoft Analysis Management Objects version included in the Microsoft SQL Server 2008 Feature Pack, October 2008, is compatible with both Microsoft SQL Server 2005 and Microsoft SQL Server 2008.
 - If you want to install Security Manager reporting server components on a computer with Microsoft SQL Server 2008 R2 installed, ensure you also install Service Pack 1 and all Cumulative Updates before installing the reporting server.
 - When installing, you must specify the SQL Server Integration Services instance that resides on the same computer as the reporting cube depot. You cannot use a SQL Server Integration Services instance on a different SQL Server computer.
 - However, the computer on which you run the reporting setup program does not need to be the computer you want to use as your SQL Server Integration Services computer. You can install SQL Server Integration Services on a completely separate computer from the computer you want to be the reporting SSIS computer and use that computer to install reporting components remotely. Wherever you choose to run the setup program, you must specify the SSIS instance on the computer you want to use as the reporting cube depot.
 - If you install SQL Server Analysis Services on a different computer than the reporting cube depot, ensure SQL Server Analysis Services uses a domain user account that can access the remote computer as a service account. You should not use the **Local System** account on the SQL Server Analysis Services computer as the Analysis Services service account.
-

Notes

- You can install Security Manager reporting server components on a SQL Server cluster, first installing the reporting server on the cluster node that owns the shared cluster resources. For more information about installing the reporting server on a cluster, see “Installing Reporting Components in Clustered Environments” on page 175.
 - NetIQ recommends installing the latest Microsoft Windows service packs and hotfixes on all computers before installing Security Manager components.
-

Planning to Install Your Agents

Security Manager monitors computers using host-based agents and proxy agents. An agent is a service that runs on a monitored computer to collect events and execute automatic responses. A proxy agent allows you to monitor computers and devices without installing the agent directly on the monitored computer or device. Windows agents that a central computer deploys and manages are called **managed agents**. Windows agents you manually install and that require manual installation of software upgrades are **unmanaged agents**.

You can configure Security Manager to automatically install agents on Windows computers using the Agent Administrator. The **Agent Administrator** allows you to create discovery rules, deploy managed agents, authorize unmanaged agents, and configure agentless Windows monitoring.

You can also configure central computer Global Settings to require approval before installing agents on Windows computers.

If you want to monitor or collect data from a UNIX or Linux computer using Security Manager, you can also deploy agents to UNIX or Linux computers. For more information about installing agents on UNIX or Linux computers, see the NetIQ UNIX Agent documentation, available in the NetIQ UNIX Agent installation kit.

If you want to monitor or collect data from an iSeries server using Security Manager, you must install NetIQ Security Solutions for iSeries on each server you want to monitor. For more information about collecting data from iSeries servers, see the NetIQ Security Solutions for iSeries documentation, available in the NetIQ Security Solutions for iSeries installation kit.

Windows agents in this version of Security Manager communicate with the central computer using more secure methods of authentication and encryption than previous (legacy) versions of the agent. Legacy and current agents are assigned different default ports, so that a Security Manager central computer can communicate with both types of agents if desired. For more information about default ports, see “Installing and Configuring Security Manager in Firewall Environments” on page 161.

Understanding Relationships Between Agents and Central Computers

When you deploy a managed agent or install an unmanaged agent you assign that agent to a central computer.

For a managed agent, a central computer performs the following functions:

- Installs and upgrades the managed agent
- Scans the managed agent to check for configuration changes
- Sends rules and configuration information to the managed agent
- Receives events from the managed agent

For an unmanaged agent, a central computer performs the following functions:

- Sends rules and configuration information to the unmanaged agent
- Receives events from the unmanaged agent

The central computer cannot install, upgrade, or scan, an unmanaged agent.

Understanding Agent Deployment and Manual Agent Installation

This section describes when you can automatically deploy agents and when you must manually install them.

Installing Windows Agents

You can configure Security Manager to automatically deploy agents to Windows computers using the Agent Administrator in the Control Center. The Agent Administrator allows you to deploy agents to Windows computers by name or by domain with matching criteria. For example, you can specify that Security Manager deploy agents to all Windows computers in a specified domain that contain a prefix in the computer name. You can also specify that certain computers be excluded from Windows agent deployment. For more information about automatically deploying Windows agents on Windows computers, see “Installing Agents” on page 105.

Security Manager cannot deploy managed Windows agents to remote Windows computers that are located outside a firewall. In this circumstance, manually install an unmanaged agent. For more information about installing agents in firewall environments, see “Installing and Configuring Security Manager in Firewall Environments” on page 161.

You should also consider installing an unmanaged agent to access the network over a WAN or a slow connection. For more information about manually installing the unmanaged agent on a Windows computer, see “Manually Installing Unmanaged Windows Agents” on page 119.

The following table lists the system requirements for a Windows agent computer.

| Category | Requirement |
|-----------------|--|
| Processor | 500 MHz Intel Pentium or equivalent. |
| Disk Space | 100 MB disk space. |
| 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 documentation for your installed modules. |

| Category | Requirement |
|-------------------|--|
| Operating Systems | <ul style="list-style-type: none"> • 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 |
| Network Access | <ul style="list-style-type: none"> • 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. |

| Category | Requirement |
|-------------------------|--|
| Additional Requirements | <ul style="list-style-type: none"> • 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 \Appl i cati on Data\NetIQ folder for each Windows user profile and all *. dat files in the <i>installation folder</i>\NetIQ Securi ty Manager\OnePoi nt folder, where <i>installation folder</i> 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 <i>installation folder</i>\NetIQ Securi ty Manager\OnePoi nt folder, where <i>installation folder</i> is the location where you installed the agent. • Any computer using Windows Server 2008 R2 Server Core on which you want to install an agent must have the Windows-on-Windows 64-bit (WoW64) feature installed. • 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.

Installing UNIX Agents

Security Manager supports numerous UNIX and Linux operating systems. For more information about the UNIX and Linux operating systems Security Manager supports or configuring Security Manager support for UNIX, see the NetIQ UNIX Agent documentation, available in the NetIQ UNIX Agent installation kit.

Installing iSeries Agents

Security Manager supports iSeries servers. For more information about iSeries system requirements or configuring Security Manager support for iSeries, see the NetIQ Security Solutions for iSeries documentation, available in the NetIQ Security Solutions for iSeries installation kit.

Understanding Agentless Windows Monitoring and Proxy Agents

If you do not want to install an agent on a Windows computer, you can monitor the computer using a **proxy agent**. A proxy agent is a Windows agent that you specify to monitor and collect events from another computer that has no agent, which is called an **agentless monitored computer**. For example, if you want to monitor multiple computers with only one agent, you can install a managed proxy agent and assign it to monitor the computers. For more information about configuring proxy agents, see “Configuring Agentless Windows Monitoring” on page 108.

Note

For more information about the number of computers one agent can support, see the NetIQ Security Manager Knowledge Base Article NETIQKB51403 at www.netiq.com/support/sm.

A proxy agent for Windows can monitor the following Windows event logs on multiple Windows computers:

- Application
- System
- Security
- DNS
- File Replication
- Directory Service

Note

A proxy agent can also monitor endpoints other than Windows computers, including non-Windows computers, devices, databases, applications, and custom providers.

Proxy Agent Responses

No responses are supported on the agentless monitored computer. However, some responses are supported on the proxy agent computer. Proxy agents do not support script responses. The following responses are supported and run on the proxy agent computer:

- Send a notification to a notification group
- Send an email
- Send a page
- Send an external command notification
- Execute a command or batch file
- Send a Simple Network Management Protocol (SNMP) trap
- Change state variables

Proxy Agent Requirements

The proxy agent logs on to the agentless monitored computer by using credentials you supply in the Agent Administrator. The account must be a member of the Administrators group on the agentless monitored computer. The proxy agent cannot use the local system account to log on to the agentless monitored computer.

The proxy agent requirements are similar to Windows agent requirements. For more information about Windows agent requirements, see “Installing Windows Agents” on page 68. However, the proxy agent is limited as follows:

- Proxy agents and the agentless computers they monitor must run the same Windows operating system, including the same application software associated with the computer’s role. For example, if you are monitoring a Windows Server 2003 domain controller, the proxy agent must also be a Windows Server 2003 domain controller.
- Proxy agents can monitor multiple agentless monitored computers.
- Multiple proxy agents cannot monitor the same agentless monitored computer.
- Proxy agents do not support a firewall between the proxy agent and agentless monitored computer.

Deploying Agents to Workstation Computers

Since Windows workstation computers typically send relatively few events to the central computer compared with Windows servers, Security Manager agents deployed on workstation computers may need to communicate less frequently with their central computer than agents deployed on server computers. A workstation is a computer with Microsoft Windows 2000 Professional, Windows XP, Windows Vista, or Windows 7 installed.

However, even when an agent has few events to send to the central computer, the agent must heartbeat regularly and keep in communication with the central computer in order to remain active. This requirement limits the number of agents a central computer can monitor, in spite of usage.

Security Manager uses a workstation scalability multiplier setting to allow workstation agents to communicate at longer intervals than server agents. Security Manager multiplies default agent communication settings, including heartbeat, computer availability, and connection retry intervals, by the scalability multiplier value for all workstation computers.

For example, when a central computer uses the default multiplier value of 36 for all workstations, all workstation computers heartbeat every 3 hours instead of the default 300 seconds. The delay reduces the performance load on the central computer, allowing one central computer to monitor a large number of workstation computers.

If your configuration group includes no workstation computers, changes to the workstation scalability multiplier setting do not affect your agent computers.

Note

When you deploy an agent to a workstation computer, the workstation uses the server agent heartbeat setting until the central computer sends initial configuration information to the workstation agent. After receiving configuration information, the workstation agent uses the scalability multiplier when heartbeating.

Using the Development Console, you can modify the default scalability multiplier setting. For more information about modifying global agent settings in the Development Console, see the *User Guide for NetIQ Security Manager*.

Planning to Install Your User Interfaces

This section describes the system requirements for the Security Manager user interfaces. For more information about installing Security Manager user interfaces, see “Installing the User Interfaces” on page 127.

To avoid compatibility issues, use the same language version for both Internet Explorer and the operating system. For example, use the French version of Internet Explorer to connect to the French version of Windows Server 2003. Attempting to connect the French version of Internet Explorer to a database server running the English version of Windows Server 2003 may adversely affect Security Manager performance.

Control Center Requirements

The Control Center allows you to quickly view and resolve alerts using views that can provide information for multiple configuration groups. The Control Center also allows you to create Trend Analysis and Forensic Analysis reports of archived log data, and compile your research into incident packages.

Some tasks within the Control Center require your user account to be a member of the OnePointOp Users group or the OnePointOp Reporting group. For more information about the group membership, see “Understanding Security Manager Requirements and Permissions” on page 79.

The following table lists the system requirements for the Control Center.

| Category | Requirement |
|------------|--|
| Processor | 1 GHz Intel Pentium 3 processor or equivalent. |
| Disk Space | 300 MB disk space. |
| Memory | 100 MB typical usage. |
| Graphics | 1024 x 768 resolution minimum. |

| Category | Requirement |
|-------------------|---|
| Operating Systems | <ul style="list-style-type: none"> • Microsoft Windows 7 (32- and 64-bit) • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2008 (32- and 64-bit) • Microsoft Windows Server 2003 R2 (32- and 64-bit) • Microsoft Windows Vista (32- and 64-bit) • Microsoft Windows Server 2003 (32- and 64-bit) • Microsoft Windows XP Service Pack 2 (32- and 64-bit) • Microsoft Windows 2000 |
| Network Access | <ul style="list-style-type: none"> • 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. |
| Software | <ul style="list-style-type: none"> • Microsoft Internet Explorer 7.0 • .NET Framework 2.0 Service Pack 1 or later • Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package • Microsoft Office 2003 Web Components (Office Web Components 11) • Microsoft ADOMD.NET • Microsoft SQL Server 2008 Analysis Services 10.0 OLE DB Provider • Microsoft SQL Server 2005 Analysis Services 9.0 OLE DB Provider • Microsoft Core XML Services (MSXML) 6.0 • Microsoft DHTML Editing Control for Applications 1.0 (only required for computers running Windows Vista and later) |

Notes

- The Control Center requires Microsoft Office 2003 Web Components but also supports Microsoft Office 2003 Web Components Service Pack 1 for the 2007 Microsoft Office System.
 - NetIQ recommends installing the latest Microsoft Windows service packs and hotfixes on all computers before installing Security Manager components.
-

Development Console Requirements

Security Manager provides a Development Console based on Microsoft Management Console (MMC) technology. The Development Console is the central configuration point for configuration groups.

Tasks within the Development Console require your user account to be a member of the OnePointOp Operators group or the OnePointOp ConfigAdms group. For more information about the group membership required for particular tasks, see “Understanding Security Manager Requirements and Permissions” on page 79.

The following table lists the system requirements for the Development Console.

| Category | Requirement |
|-----------------|--|
| Processor | 500 MHz Intel Pentium processor or equivalent. |
| Disk Space | 64 MB disk space. |
| Memory | 40 MB typical usage. |
| Graphics | 1024 x 768 resolution minimum. |

| Category | Requirement |
|------------------|---|
| Operating System | <ul style="list-style-type: none"> • Microsoft Windows 7 (32- and 64-bit) • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2008 (32- and 64-bit) • Microsoft Windows Server 2003 R2 (32- and 64-bit) • Microsoft Windows Vista (32- and 64-bit) • Microsoft Windows Server 2003 (32- and 64-bit) • Microsoft Windows XP Service Pack 2 (32- and 64-bit) • Microsoft Windows 2000 |
| Network Access | <ul style="list-style-type: none"> • 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. |
| Software | <ul style="list-style-type: none"> • Microsoft Internet Explorer 7.0 • .NET Framework 2.0 Service Pack 1 or later • Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package • Microsoft Core XML Services (MSXML) 6.0 • Microsoft DHTML Editing Control for Applications 1.0 (only required for computers running Windows Vista and later) |

Note

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

Web Console Requirements

The Web Console brings the functionality of the Control Center to the Web. Using a combination of HTML, Javascript, and Microsoft Internet Information Services (IIS) extensions, you can monitor Security Manager over the Internet and intranet using Microsoft Internet Explorer.

Because of the nature of Web browser technology, the monitoring computer does not need to be running a specific version of Windows. You can run the Web Console from any Windows computer running Internet Explorer that has access to the central computer hosting the Web Console server.

The Web Console requires Microsoft Internet Explorer 6.0, Internet Explorer 7.0, or Internet Explorer 8.0, Microsoft Internet Information Services (IIS) 5.0, and a screen resolution of at least 1024 x 768.

Notes

- You must run the Web Console as a 32-bit application. If you install the Web Console on a Windows Server 2003 computer, this may cause issues with any 64-bit Web applications installed on the same computer. NetIQ recommends you install the Web Console on a computer with only 32-bit Web applications running.
- If you install the Web Console on a Windows Server 2003 computer, Security Manager modifies Microsoft IIS to allow Active Server Pages and Server Side Includes.
- If you want to install the Web Console on a Microsoft Windows Server 2008 computer, you must first install IIS 7.0, including Active Server Pages for IIS, followed by the IIS 6.0 Management Compatibility components.

To use the Web Console, your account must be a member of the OnePointOp Users group. Your account must also be a member of the EeaDasLocator role in the OnePoint database. For more information about groups and permissions, see “Understanding Security Manager Requirements and Permissions” on page 79.

Understanding Security Manager Requirements and Permissions

Security Manager uses Windows groups and database roles to restrict access to product functionality. The Security Manager setup program creates the Windows groups and database roles, and then adds the service account and installation account to appropriate groups and roles.

Note

Members of the local Administrators group on a central computer have permission to use all Security Manager user interfaces on the computer, regardless of their OnePointOp group memberships.

At the end of installation, you can launch the Security Manager **Access Configuration** utility to add global groups you want to give access to the Security Manager user interfaces. The Access Configuration utility allows you to control Security Manager permissions by managing membership in OnePointOp groups. Access Configuration enforces the use of global groups in OnePointOp groups and creates appropriate database logins. Later, when you want to change who has access to the user interfaces, you can modify the global group membership.

Note

The Security Manager Access Configuration utility does not manage membership in global groups. Use Active Directory Users and Computers to manage account memberships within the global domain groups that are members of the OnePointOp groups.

For more information about the Security Manager Access Configuration utility, see the *User Guide for NetIQ Security Manager*. To use the Security Manager Access Configuration utility, you must be a member of the local Administrators group on the central computer and the Microsoft SQL Server `sysadmin` role on the database server.

For an additional layer of security, you can also configure security filtering. **Security filtering** allows you to set permissions on Security Manager computer groups to limit the data users can see or modify. A **computer group** is a collection of computers with some attribute in common. Computer groups are defined by computer grouping rules. For more information about security filtering, see Appendix A, “Setting Permissions on Computer Groups”.

Understanding Security Manager OnePointOp Groups

Security Manager provides the following Windows local groups to which you can add Windows global or universal groups following Security Manager installation.

Note

Security Manager does not support using nested Active Directory groups within OnePointOp groups.

OnePointOp Reporting

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

Note

The OnePointOp Reporting group does not control access to Summary reports, either through the Microsoft SQL Server Management Studio or the Web Console.

Use either the Microsoft SQL Server Management Studio or the Report Manager Website to configure permissions for accessing Summary reports. For more information about configuring SQL Server permissions, see the Microsoft SQL Server Management Studio Help.

OnePointOp Users

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

OnePointOp Operators

User accounts in the OnePointOp Operators group have all the permissions of the OnePointOp Users group. In addition, operators can modify the rules that configure Security Manager to monitor and collect events. Operators typically use the Control Center and the Development Console.

OnePointOp ConfigAdms

User accounts in the OnePointOp ConfigAdms group have all the permissions of the OnePointOp Operators group. In addition, users in the ConfigAdms group can also modify the computers where Security Manager installs agents, as well as configure settings in the Configuration Wizard. Security Manager configuration administrators typically use the Control Center, Development Console Configuration snap-ins, Configuration Wizard, and Agent Administrator.

Warning

Maintain tight control over members of the OnePointOp Operators and OnePointOp ConfigAdms groups. Members of these groups can define rules that can make widespread changes throughout your enterprise.

OnePointOp TrustedServiceAccounts

Service accounts from a remotely connected configuration group that are members of the local OnePointOp TrustedServiceAccounts group have access to data in the local configuration group. A **service account** is a Windows security account used by services to log on to a Windows computer.

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

Understanding Console Requirements

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

Control Center

To access views in the Control Center, your user account must be a member of the OnePointOp Users group. Your account must also be a member of the EeaDasLocator role in the OnePoint database.

To access reports in the Control Center, your user account must be a member of the OnePointOp Reporting group. Your account must also be a member of the following roles in the databases:

- the EeaDasLocator role in the OnePoint database
- the Vi gi l EntUserAccess role in the LogManagerConfiguration database

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

| Task | Group Membership |
|---|---|
| Launching the Configuration Wizard | OnePointOp ConfigAdms |
| 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 ConfigAdms |
| Creating a custom task available to all users | OnePointOp Operators |
| Modifying a private or public view | OnePointOp ConfigAdms (or the user account that created the view) |
| Ignoring agent status and stopping ignoring agent status | OnePointOp ConfigAdms |
| Installing or uninstalling modules | OnePointOp Operators |
| Launch Summary Reports | OnePointOp Reporting |

Development Console

To use the Development Console, your user account must be a member of the OnePointOp Operators group. Your account must also be a member of the EeaDasLocator role in the OnePoint database.

Configuration Snap-in

To use the Configuration snap-in, your user account must be a member of the OnePointOp ConfigAdms group. However, you can still access notification groups if you are a member of OnePointOp Operators group. Your account must also be a member of the EeaDasLocator role in the OnePoint database.

Log Archive Configuration Utility

To use the Log Archive Configuration utility, your user account must be a member of the OnePointOp ConfigAdms group. Your account must also be a member of the EeaDasLocator role in the OnePoint database.

Web Console

To use the Web Console, your account must be a member of the OnePointOp Users group. Your account must also be a member of the EeaDasLocator role in the OnePoint database.

Creating Global Domain Groups

Following installation, you use the Security Manager Access Configuration utility to populate Security Manager OnePointOp groups and database roles with global groups that contain the users to whom you want to grant Security Manager access permissions.

Create your global groups and populate them with users before installing Security Manager. You can use Active Directory Users and Computers to create and populate your global groups. When you run the Security Manager Access Configuration utility, the utility adds the global groups to the appropriate OnePointOp groups and creates the necessary database logon permissions.

Chapter 3

Installing Security Manager

Complete the steps described in “Planning to Install Security Manager” on page 23 before installing Security Manager. For an overview of the installation and configuration process, see “Security Manager Installation Checklist” on page 86.

The Security Manager setup program allows you to specify either a trial or production installation. This chapter documents how to install Security Manager in a production environment. In a trial installation, you install all components on one computer. In a production environment, you install components on multiple computers to allow Security Manager to support the following features:

- Monitor computers
- Maintain dedicated databases
- Allow different groups within your organization to control their Security Manager implementation
- Install redundant components

Note

NetIQ does not recommend installing all components on one computer in a production environment for performance reasons.

Security Manager does not support an upgrade from a trial installation to a production installation. You must uninstall a trial installation before installing a production installation. For more information on trial installations, see the *Trial Guide for NetIQ Security Manager*.

Security Manager Installation Checklist

Install Security Manager by rolling out one configuration group at a time.

This section guides you through the process of rolling out a configuration group. You can repeat this section for each additional configuration group you want to install.

Install Security Manager by completing the following checklist.

| <input checked="" type="checkbox"/> | Steps | See Section |
|-------------------------------------|--|--|
| <input type="checkbox"/> | 1. Review planning and system requirements. | "Implementation Checklist" on page 25 |
| <input type="checkbox"/> | 2. Ensure you have the latest software versions. | "Obtaining the Latest Product Version" on page 87 |
| <input type="checkbox"/> | 3. Verify logon account permissions. | "Permissions" on page 89 |
| <input type="checkbox"/> | 4. Create service accounts. | "Creating a Service Account" on page 89 |
| <input type="checkbox"/> | 5. Create email accounts. | "Creating an Email Account" on page 93 |
| <input type="checkbox"/> | 6. Disable MSMQ Active Directory Integration, if not needed. | "Disabling Active Directory Integration with Message Queuing" on page 93 |
| <input type="checkbox"/> | 7. Install Security Manager components and licensed modules. | "Installing Security Manager" on page 95 |
| <input type="checkbox"/> | 8. Install any additional central computers. | "Installing Additional Central Computers" on page 100 |

| <input checked="" type="checkbox"/> | Steps | See Section |
|-------------------------------------|--|--|
| <input type="checkbox"/> | 9. Install and configure reporting server components. | "Installing the Reporting Server" on page 101 |
| <input type="checkbox"/> | 10. Deploy or manually install agents. | "Installing Agents" on page 105 |
| <input type="checkbox"/> | 11. Configure Security Manager using the Configuration Wizard. | "Configuring Security Manager" on page 109 |
| <input type="checkbox"/> | 12. Configure monitoring for other security products or operating systems. | See the module documentation for products you want to monitor. |
| <input type="checkbox"/> | 13. Specify central computers for failover. | "Specifying Central Computers for Failover" on page 110 |
| <input type="checkbox"/> | 14. Synchronize device time properties across your network. | "Synchronizing Device Times" on page 112 |
| <input type="checkbox"/> | 15. Customize Security Manager time periods for Trend Analysis. | "Configuring Security Manager Time Periods" on page 112 |
| <input type="checkbox"/> | 16. Configure notification groups. | "Configuring Notification of Real-Time Alerts" on page 115 |
| <input type="checkbox"/> | 17. Install the user interfaces. | "Installing the User Interfaces" on page 127 |
| <input type="checkbox"/> | 18. Return to the implementation checklist. | "Implementation Checklist" on page 25 |

Obtaining the Latest Product Version

You can access a list of the latest software versions and service packs in the Support area of the NetIQ Web site.

To ensure you have the latest product capabilities, verify you have the latest version of Security Manager. Every Security Manager component in your implementation must be the same version. If you want to upgrade or install a product version that is newer than existing components, upgrade the existing components at the same time. For more information about upgrading, see “Upgrading Security Manager” on page 195.

To verify you have the latest version of Security Manager:

1. Log on with an administrator account to a computer on which you want to install Security Manager components.
2. Close all open applications.
3. Run the setup program from the Security Manager installation kit.
4. Click **Check Version** on the Production Setup tab to check the product version in the installation kit against the newest available product version on the Web site.
5. *If you do not have the latest version of the product*, download and extract the setup program for the latest product version. Use this version instead to install Security Manager.
6. Close the Web browser.

Permissions

Before installing Security Manager, ensure your logon account is a member of the local Administrators group on the computers where you install Security Manager components. Also ensure your logon account is a member of the Microsoft SQL Server `sysadmin` role on the database server and on the reporting server.

Notes

- You do not need an Administrator account or SQL Server `sysadmin` account to run most Security Manager consoles or utilities *after* installation.
- You must use an account that is a member of the Microsoft SQL Server `sysadmin` role on the database server to use the Access Configuration utility.
- In Windows Server 2008 and Windows Vista environments, users added to the Administrators group do not have built-in administrator privileges by default and are subject to User Account Control restrictions.

When you manually install an agent on a computer with Windows Server 2008 or Windows Vista installed, you may need to run the setup program using the built-in administrator account. To run `Manual Agent.msi` as the administrator, open the command-line interface using the `runas` command:

```
runas /user: administrator cmd
```

In the command-line interface, run the `.msi` according to the installation instructions.

Creating a Service Account

The central computer uses a service account, which is a Windows user account, to log on to the database server, log archive server, central computer, and agent computers.

Understanding Service Account Requirements

All Security Manager service accounts must meet the following requirements in order for Security Manager to function properly:

- The account must be a domain account.
- The account cannot have a blank password.
- The account must be in a trusted domain or in the same domain as the database server and reporting server.

- The account must be a member of the local Administrators group on the central computer and all agent computers that the central computer will manage in the domain. If you want the service account to have rights to install agents in other trusted domains, the service account must be a member of the local Administrators group on all agent computers that the central computer will manage in the trusted domain.
- The account must be able to access the private keys of self-signed certificates installed in the Local Machine certificate store on the central computer. When you install a Security Manager central computer, the setup program creates a self-signed certificate and installs the certificate and corresponding private key in the Local Machine > NetIQ Security Manager certificate store.

Notes

- If your enterprise has a password expiration policy, consider exempting the service account from your password expiration policy.
 - If you want a configuration group to monitor computers in different domains and do not want the central computers to share a common service account, you can install multiple central computers with different service accounts. However, for redundancy to function properly, ensure the service account used by each backup central computer is a member of the local Administrators group on all agents managed by the primary central computer. For more information about configuring primary and backup central computers, see the *User Guide for NetIQ Security Manager*.
 - If you have multiple configuration groups, create a different service account for each configuration group. Since monitoring a remote configuration group requires adding your local service account to the OnePointOp TrustedServiceAccounts group on the remote central computer, and **not** on your local central computer, the configuration group service accounts cannot be the same.
 - After you install Security Manager using your service account, NetIQ does not recommend modifying service account permissions. Security Manager uses the service account to run services and access configuration information in the OnePoint, LogManagerConfiguration, and SecurityManagerCommon databases. If you modify service account permissions either on Security Manager component computers or in SQL Server, Security Manager may no longer be able to function.
-

Notes

- In addition, NetIQ does not recommend configuring security filtering for the OnePointOp System group to which the service account belongs. In order to run Forensic Analysis queries on all computers in your environment, the OnePointOp System group and service account must have **Read** permissions for all computer groups. For more information about configuring security filtering and setting permissions on computers, see “Setting Permissions on Computer Groups” on page 149.
- If the service account cannot access the private key for the default Security Manager certificate, the NetIQ Security Manager service cannot start, and the central computer generates an event 21337 in the Application event log.

To resolve this issue, review the access control list (ACL) of the key container file to ensure the service user has Read and Execute permissions, at minimum. The event 21337 description identifies the key container file name. Check the ACL of the key container file located in the %ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\RSA\MachineKeys folder to ensure the Security Manager service account has at least Read and Execute permissions. For more information about key containers, see the following article on the Microsoft support site:

[http://msdn.microsoft.com/en-us/library/bb204778\(v=85\).aspx](http://msdn.microsoft.com/en-us/library/bb204778(v=85).aspx)

Understanding Service Account Permissions Added by Security Manager

When you install Security Manager, the 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 an Email Account

If you plan to use email notification for real-time alerts, create a dedicated email account for the central computer account to use. Security Manager supports SMTP for email notification.

Configure the email account so that it does not save sent email messages. If you configure the email account to save sent email messages, you must occasionally delete these messages from the email account. Store the mailbox on the email server so that the mailbox is accessible from all central computers.

After installing Security Manager, use the Global Settings option in the Configuration Wizard to configure email notification using a specified email account. For more information about configuring notifications, see “Configuring Security Manager” on page 109.

Note

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

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

Disabling Active Directory Integration with Message Queuing

Security Manager 6.5.4 requires that you install the Message Queuing Windows component on a computer before installation of some Security Manager components. However, unless you actively use the Active Directory Integration sub-component of the Message Queuing Windows component, NetIQ recommends you disable Active Directory Integration. You can either disable Active Directory Integration when installing Message Queuing or disable it after installation.

For more information about Security Manager prerequisites, see “Planning to Install Security Manager” on page 23.

Note

In Windows Server 2008, the Active Directory Integration sub-component is called Directory Services Integration.

To disable Active Directory Integration after installing Message Queuing:

1. Log on to the computer on which you installed the Message Queuing Windows component and you want to install Security Manager components, using an account that is a member of the local Administrators group.
2. *If the computer uses Windows Server 2003*, perform the following steps:
 - a. Open the Add or Remove Programs Control Panel.
 - b. Click **Add/Remove Windows Components**.
 - c. Select **Application Server** and click **Details**.
 - d. Select **Message Queuing** and click **Details**.
 - e. Clear the **Active Directory Integration** check box.
 - f. Click **OK**.
 - g. Click **OK**.
 - h. Click **Next**. The Windows Component Wizard configures Message Queuing.
 - i. Click **Finish**.
 - j. Close the Control Panel.
3. *If the computer uses Windows Server 2008 or Windows Server 2008 R2*, perform the following steps:
 - a. Open the Server Manager.
 - b. In the left pane, click **Features**.
 - c. In the right pane, click **Remove Features**.

- d. Expand **Message Queuing** > **Message Queuing Services**.
 - e. Clear the **Directory Service Integration** check box.
 - f. Click **Next**.
 - g. Click **Remove**. The Remove Features Wizard removes the Directory Service Integration feature.
 - h. Click **Close**.
 - i. Close the Server Manager.
4. Log off of the computer.

Installing Security Manager

This section explains how to use the setup program to install Security Manager components. Follow the procedures to install a database server, log archive servers, central computers, and user interfaces. For more information about hardware requirements and other planning considerations, see “Planning to Roll Out Your Configuration Groups” on page 26.

After installation, use the Configuration Wizard to configure Security Manager to monitor your environment using the modules you install.

Choosing Components to Install

The setup program allows you to select which Security Manager components you want to install.

The components are listed in the order indicated:

| <input checked="" type="checkbox"/> | Steps | Description |
|-------------------------------------|-------------------------------|--|
| <input type="checkbox"/> | 1. Database Server | Select this component to install the database server on the local computer or to a remote location. |
| <input type="checkbox"/> | 2. Log Archive Server | Select this component to install the log archive server on the local computer. |
| <input type="checkbox"/> | 3. Central Computer | <p>Select this component to install the central computer on the local computer. You can also select the Database Server component and install the database server remotely during the same installation run.</p> <p>You cannot install a central computer on an existing managed agent computer.</p> |
| <input type="checkbox"/> | 4. Web Console Server | <p>Select this component to install the Web Console server on the local computer.</p> <p>For more information about installing the user interfaces, see “Installing the User Interfaces” on page 127. You can install the Web Console server only on a central computer.</p> |
| <input type="checkbox"/> | 5. Control Center | <p>Select this component to install the Control Center on the local computer.</p> <p>For more information about installing the user interfaces, see “Installing the User Interfaces” on page 127. You can choose to install the Control Center during the same installation run with other components.</p> |
| <input type="checkbox"/> | 6. Development Console | <p>Select this component to install the Development Console on the local computer.</p> <p>For more information about installing the user interfaces, see “Installing the User Interfaces” on page 127. You can choose to install the Development Console during the same installation run with other components.</p> |

Notes

- If you want to install the log archive server on a separate computer, you must install log archive server components on that computer before installing the central computer or user interface components on other computers in the configuration group.
 - Ensure you install all Security Manager components in an environment with access to a domain controller.
 - Before installing Security Manager components, review the group policy for your environment and ensure the policy does not contain any specific requirements that could restrict communication between component computers. For example, if your group policy requires LDAP server signing on a server where you want to install Security Manager, other computers may not be able to communicate with that server.
 - After you install all Security Manager components, you should use the Agent Administrator to deploy agents to monitor the log archive server, reporting server, and database server. The setup program only automatically installs an agent on the central computer. For more information about installing agents, see “Installing Windows Agents” on page 105.
 - If you install a log archive server at a later date that you want to communicate with existing central computers or reporting servers, you must configure this communication. For more information about configuring a central computer for a log archive, see the *User Guide for NetIQ Security Manager*. For more information about configuring a log archive server for a reporting server, see “Configuring and Enabling Reporting” on page 104.
-

Verifying Prerequisites

Security Manager includes a Verify Prerequisites tool with the Security Manager installation kit. The Verify Prerequisites tool helps you ensure the computer on which you install Security Manager is ready for the Security Manager implementation. Run the Verify Prerequisites tool before installing Security Manager.

For more information about prerequisites, see the following:

- For database server prerequisites, see “Planning to Install Your Database Server” on page 44.
- For log archive server prerequisites, see “Planning to Install Your Log Archive Servers” on page 47.
- For central computer prerequisites, see “Planning to Install Your Central Computers” on page 52.
- For agent prerequisites, see “Planning to Install Your Agents” on page 66.

To run the Verify Prerequisites tool:

1. Log on to the computer on which you want to install the Security Manager component using an account that is a member of the local Administrators group.
2. Close all open applications.
3. Run the setup program from the Security Manager installation kit.
4. Click the Production Setup tab and click **Verify Prerequisites**.
5. Click **Run**.
6. *If you receive a second security warning*, click **Run** again.
7. Click **Next**.
8. On the **Select Security Manager Components** window, select the components for which you want to verify prerequisites and click **Next**.
9. Follow the instructions until you have verified all the necessary prerequisites for the Security Manager components you want to install. You can install some of the required software using the Verify Prerequisites tool.
10. When you finish verifying prerequisites, click **Finish**.

Note

You may not be able to install all prerequisites automatically. The Verify Prerequisites tool specifies what prerequisites you need to install and either provides the software to install automatically or directs you to the location of the prerequisite elsewhere.

Running the Setup Program

Before running the setup program, ensure the computer on which you are installing Security Manager has access to a domain controller. The following procedure guides you through the process of installing a Security Manager components.

To install Security Manager:

1. Log on to the computer on which you want to install the Security Manager component using an account that is a member of the local Administrators group. Also ensure your logon account is a member of the Microsoft SQL Server `sysadmin` role on the database server and reporting server.

Note

You do not need an Administrator account or SQL Server `sysadmin` account to run most Security Manager consoles or utilities *after* installation.

You must use an account that is a member of the Microsoft SQL Server `sysadmin` role on the database server to use the Access Configuration utility.

2. Close all open applications.
3. Run the setup program from the Security Manager installation kit.
4. Click the Production Setup tab and click **Begin Production Setup**.
5. Click **Run**.
6. *If you receive a second security warning*, click **Run** again.
7. Click **Next**.
8. On the **License Agreement** window, select **I accept the terms in the license agreement** and click **Next**.
9. On the **Select Security Manager Components** window, select the components you want to install and click **Next**.
10. Follow the instructions in the setup program until you reach the Finished window.

11. *If you are installing a central computer and have not previously installed modules*, click **Launch Module Importer**. For more information about fields on a window, see the Help.
12. *If you are installing a central computer and want to add global domain groups to the OnePointOp groups and database roles*, click **Launch Access Configuration**. For more information about fields on a window, see the Help.

Note

You can also launch the Security Manager Access Configuration utility at a later time. However, you must complete this step on each central computer before other user accounts can access the Security Manager user interfaces. For more information about user interface permissions, see the *User Guide for NetIQ Security Manager*.

13. Click **Finish**.
14. Repeat Steps 1 through 13 to install additional Security Manager components, as necessary.

Installing Additional Central Computers

You may want to install additional central computers in your configuration group. You can use additional central computers to do any of the following activities:

- Enable load balancing
- Enable redundancy (failover)
- Monitor computers in multiple domains

For more information about the reason to install multiple central computers, see “Multiple Central Computers” on page 55.

Note the following points when installing additional central computers:

- Use the same database server for each central computer in the same configuration group.
- If you want the additional central computer for load balancing or redundancy, use the same service account as the original central computer.

To install an additional central computer:

1. Repeat the procedures in “Installing Security Manager” on page 95 for each central computer you want to install.

Note

If you have already installed modules on a central computer in a configuration group, you do not need to install modules again when adding additional central computers to the configuration group.

2. *If you have installed agents and would like to configure the new central computer to manage them*, reassign agents to the new central computer. You can use the Agent Administrator to reassign agents. For more information about managing agents, see the *User Guide for NetIQ Security Manager* or the Help.

Installing the Reporting Server

The following sections document how to install the Security Manager reporting server. Follow this procedure to install reporting components and databases to store summarized log archive data for use in Trend Analysis reports and in custom Summary reports. The setup program verifies prerequisites before installing.

For more information about hardware requirements and other planning considerations, see “Understanding Security Manager Requirements and Permissions” on page 79.

Notes

- You can specify default or named instances for SQL Server Analysis Services or the reporting cube depot.
 - If you want to install Security Manager reporting server components on different SQL Server computers, you must run the setup program from a computer with SQL Server Integration Services and either the Microsoft SQL Server 2008 Client Tools SDK or the Microsoft SQL Server 2005 Software Development Kit, depending on the version of SQL Server you want to use.
 - When installing, you must specify the SQL Server Integration Services instance that resides on the same computer as the reporting cube depot. You cannot use a SQL Server Integration Services instance on a different SQL Server computer.
 - However, the computer on which you run the reporting setup program does not need to be the computer you want to use as your SQL Server Integration Services computer. You can install SQL Server Integration Services on a completely separate computer from the computer you want to be the reporting SSIS computer and use that computer to install reporting components remotely. Wherever you choose to run the setup program, you must specify the SSIS instance on the computer you want to use as the reporting cube depot.
 - If you install SQL Server Analysis Services on a different computer than the reporting cube depot, ensure SQL Server Analysis Services uses a domain user account that can access the remote computer as a service account. You should not use the **Local System** account on the SQL Server Analysis Services computer as the Analysis Services service account.
 - You can install Security Manager reporting server components on a SQL Server cluster, first installing the reporting server on the cluster node that owns the shared cluster resources. For more information about installing the reporting server on a cluster, see “Installing Reporting Components in Clustered Environments” on page 175.
-

Running the Setup Program

Before running the setup program, ensure the computer on which you are installing the reporting server has access to a domain controller. The following procedure guides you through the process of installing a reporting server.

To install the reporting server:

1. Log on to the computer on which you want to install the reporting server using an account that is a member of the local Administrators group. Also ensure your logon account is a member of the Microsoft SQL Server `sysadmin` role on the database server and reporting server.

Note

You do not need an Administrator account or SQL Server `sysadmin` account to run most Security Manager consoles or utilities *after* installation.

You must use an account that is a member of the Microsoft SQL Server `sysadmin` role on the database server to use the Access Configuration utility.

2. Close all open applications.
3. Run the setup program from the Security Manager installation kit.
4. Click the Production Setup tab and click **Begin Reporting Setup**.
5. Click **Run**.
6. *If you receive a second security warning*, click **Run** again.
7. Click **Next**.
8. On the **License Agreement** window, select **I accept the terms in the license agreement** and click **Next**.
9. Follow the instructions in the setup program until you reach the Finished window.
10. Click **Finish**.

Configuring and Enabling Reporting

To access Trend Analysis reports on summarized log data and create and view custom Summary reports using SQL Server Business Intelligence Development Studio, configure the log archive servers to upload data to the reporting server. Also enable your log archives to upload summarized data and enable the reporting server to receive the summarized data. Both settings, available in the Log Archive Configuration utility, are required for Trend Analysis and Summary reports to function properly.

To specify the reporting server computer for your log archive server and enable data transfer:

1. Log on to the log archive server using an account that is a member of the OnePointOp ConfigAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start **Log Archive Configuration** in the NetIQ Security Manager > Configuration program group.
3. In the left pane, click **Log Archive Server Settings**.
4. Under **Reporting**, select **Reporting Server Name** and type the name of your reporting server computer.
5. Select **Enable Summarized Data Export** and select **True** from the list.
6. Select **Enable Summarized Data Upload** and select **True** from the list.
7. Click **Apply**, and then click **Yes**.
8. Click **Close**.
9. Click **Yes** on the confirmation message to restart the NetIQ Security Manager Log Archive service.

Note

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

10. Click **Yes** again to exit the wizard.
11. Repeat Steps 1 through 10 for each additional log archive server you want to send data to the reporting server.

Note

After you configure and enable reporting, you can use SQL Server Business Intelligence Development Studio to create custom Summary reports or download preconfigured Summary reports from the NetIQ Support site for Security Manager at www.netiq.com/support/sm.

For more information about creating or uploading Summary reports, see the *User Guide for NetIQ Security Manager*.

Installing Agents

Security Manager supports monitoring and collecting logs from Windows, UNIX, and iSeries environments. This section provides an overview of how to install agents on Windows, UNIX, and iSeries computers.

Note

Depending on the number of computers you want to monitor, deploying agents may take some time. You can begin configuring Security Manager while Security Manager deploys agents. For more information about deploying agents, see “Configuring Security Manager” on page 109.

Installing Windows Agents

You can configure Security Manager to automatically deploy agents to Windows computers using the Agent Administrator, which is available from the Control Center.

The Agent Administrator guides you through the deployment of agents to Windows computers on your network. The Agent Administrator allows you to add Windows computers by name or by domain with matching criteria.

The Agent Administrator also allows you to find computers on which you want to deploy agents with **discovery rules**. For example, you can specify that Security Manager deploy agents to all Windows computers in a specified domain that contain a prefix in the computer name.

You can also specify computers on which to deploy agents with Light Directory Access Protocol (LDAP) queries of the Active Directory.

Notes

- Ensure the Remote Registry Service is started on the Windows computer and central computer before attempting to deploy Windows agents. You can review services using the Component Services Administrative tool, located in the Control Panel.
- Ensure the central computer service account has write access to the Windows agent share on Windows Server 2003 computers.
- Ensure the service account is a member of the local Administrators group on all agent computers that the central computer will deploy and manage.
- NetIQ Corporation does not support monitoring managed agents located on the outside of a firewall from the central computer. If you want to monitor computers behind a firewall, NetIQ Corporation recommends installing unmanaged agents on your remote computers. For more information about installing unmanaged agents, see “Manually Installing Unmanaged Windows Agents” on page 119.

To deploy managed agents to Windows computers using the Agent Administrator:

1. Log on to the central computer as a member of the OnePointOp ConfgAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Click **Configuration Groups**.
4. In the Tasks pane, click **Launch Agent Administrator**.
5. In the left pane, click **Managed Agents**.
6. In the right pane, click **Configure Agent Discovery Rules**.

7. Click **Add**.
8. Select **Include Computers**, and then click **Next**.
9. Complete the wizard, specifying parameters that select the computers you want to discover. For more information about fields on a window, see the **Help**.
10. Select the check box and row corresponding to the rule you created with the wizard.
11. Click **Next**.
12. *If you want to deploy agents to the discovered computers at the next scan*, click **No**.
13. *If you want to immediately deploy agents to the discovered computers*, click **Yes**.
14. If you clicked **Yes**, select the central computer that will manage the computers.
15. Click **Yes** again to deploy agents immediately.
16. Click **Next**.
17. Select the discovered computers to which you want to deploy agents.
18. Click **Next**.
19. Click **Finish**.
20. Click **Close**.

Notes

- When you deploy a managed agent to a new computer, Security Manager does not immediately begin receiving data from the new agent. The agent first sends a heartbeat to the central computer and receives configuration data from Security Manager. At the next agent heartbeat, the agent sends configuration information back to the central computer. The agent then starts sending data to the central computer.
 - If you installed the correlation feature, the first central computer you installed is the Correlation server. Do not use this computer to manage agents. Install one or more additional central computers to monitor agents, including the central computer monitoring UNIX computers and iSeries servers.
-

For more information about installing the Windows agent manually, see “Manually Installing Unmanaged Windows Agents” on page 119.

Configuring Agentless Windows Monitoring

After you install a Windows agent, you can configure it to be a proxy agent. A proxy agent monitors another Windows computer that does not have an agent. Using a proxy agent allows you to collect Windows event logs for Windows computers on which you cannot install an agent. For more information about proxy agent requirements, see “Understanding Agentless Windows Monitoring and Proxy Agents” on page 71.

To configure agentless monitored computers:

1. Log on to the central computer as a member of the OnePointOp ConfigAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. Click **Configuration Groups**.
4. In the Tasks pane, click **Launch Agent Administrator**.
5. In the left pane, click **Agentless Monitored Computers**.
6. In the right pane, click **Configure Agentless Windows Monitoring**.
7. Complete the wizard to select proxy agents, proxy agent credentials, and agentless monitored computers. For more information about fields on a Window, see the Help.

Installing UNIX Agents

If you want to monitor or collect logs from UNIX or Linux computers, install and configure UNIX agents. For more information about monitoring UNIX or Linux computers, see the NetIQ UNIX Agent documentation, available in the NetIQ UNIX Agent installation kit, and the Security Manager for UNIX Release Notes.

Installing iSeries Agents

If you want to monitor or collect logs from iSeries servers, you must manually install the iSeries agents. For more information about monitoring iSeries servers, see the NetIQ Security Solutions for iSeries documentation, available in the NetIQ Security Solutions for iSeries installation kit, and the Security Manager for iSeries Release Notes.

Configuring Security Manager

Security Manager provides default settings for most monitoring tasks. To use some features, you need to provide additional information that is unique to your network. For example, to process alert notifications, you need to provide the name of your email server.

Note

If you install a log archive server or reporting server, ensure you configure each server within the first day of installation. Also ensure that you configure custom Security Manager time periods on the central computer, if necessary.

Using the Configuration Wizard

The Configuration Wizard guides you through the configuration of critical global settings and parameters. You can run the Configuration Wizard at any time to reconfigure these parameters.

To configure Security Manager for your environment using the Configuration Wizard:

1. Log on to the central computer as a member of the OnePointOp ConfigAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.

4. On the Tasks menu, click **Global Tasks > Launch Configuration Wizard**.
5. Click any link in the left pane, then follow the instructions in the Configuration Wizard until you have completed configuring Security Manager for your environment. For more information about fields on a window, see the Help.

You may also need to complete additional configuration for third-party products you want to monitor. For more information about monitoring third-party products, see the module documentation for your product.

Specifying Central Computers for Failover

Under certain circumstances, such as maintenance or communication problems, an agent may not be able to communicate with the central computer to which it is assigned. Security Manager does not leave any agent without a central computer. Instead, Security Manager temporarily assigns the agent to another central computer, chosen from a list you specify.

When failover to another central computer occurs, the backup central computer provides many of the functions the primary central computer provided until the primary central computer is again accessible. Following failover, agents send events to the backup central computer. The backup central computer can pass rules and configuration to the agent and can scan the agent. The backup central computer cannot install updates or new agent software on the agent.

By default, Security Manager specifies one or more central computers managed and unmanaged agents can contact in the event that their assigned central computer is unavailable. However, you can disable this setting and specify backup central computers for each central computer in your configuration group.

Each central computer can have more than one backup computer specified. Failover occurs in the order you specify.

To manually specify central computers for failover:

1. *If the central computers use different service accounts*, ensure the service account used by each backup central computer is a member of the local Administrators group on all agents managed by the primary central computer.
2. Log on to the Development Console computer using an account that is a member of the OnePointOp ConfigAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
3. Start the **Development Console** in the NetIQ Security Manager program group.
4. Disable automatic failover by completing the following steps:
 - a. In the left pane, expand **Security Manager Development Console > Configuration > Global Settings**.
 - b. In the right pane, click **Central Computers**.
 - c. On the Action menu, click **Properties**.
 - d. Click **Redundancy Policy**.
 - e. Clear **System Controlled**.
 - f. Click **OK**.
5. In the left pane, expand **Security Manager Development Console > Configuration > Central Computers**.
6. In the right pane, select a central computer for which you want to specify backup central computers.
7. On the Action menu, click **Properties**.
8. Click **Redundant Central Computers**.
9. In Available Central Computers, select a computer.
10. Click **>>**.
11. Repeat Steps 9 through 10 for each central computer you want to designate as a backup central computer.

12. Click **Move Up** and **Move Down** to arrange the computers in the order you want failover to occur.
13. Click **OK**.

Synchronizing Device Times

To ensure Security Manager displays the correct time for detected events and correlates events in a timely fashion, periodically synchronize the time properties for all computers and devices across your network.

Configuring Security Manager Time Periods

You can configure the time periods used to filter data in Trend Analysis reports. The Time Period filters allow you to filter data for events occurring during a specific time period, such as lunch time or the end of the work day. For more information about Trend Analysis reports, see the *User Guide for NetIQ Security Manager*.

Time periods are defined on each central computer using the Configuration Wizard and are applied across all computers in the configuration group. You can configure specific time ranges in hourly increments of a 24-hour-day to indicate what time of day an event occurred. For example, you could designate between the hours of 9:00 AM and 12:00 PM as “Morning Work Hours,” with 12:00 to 1:00 PM designated as “Lunch Hour.”

Default time periods are:

- Business Hours (8 AM - 5 PM)
- Lunch Hour (12 AM - 1 PM)
- Non-Business Hours (5 PM - 8 AM)

You must define and name a time period for each hour of the day.

Note

If you need to modify the time periods, you should do so immediately after installation. If you modify the time periods later, the data in the report for previous days reflects the previously defined time periods and you will not be able to accurately compare trends by time for the previous dates.

Creating Security Manager Time Periods

Using the Configuration Wizard, you can create new time periods for use in filtering Trend Analysis report data.

To create a new time period for Trend Analysis:

1. Log on to a central computer as a member of the OnePointOp ConfigAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.
4. On the Tasks menu, click **Global Tasks > Launch Configuration Wizard**.
5. Click **Global Settings**.
6. Click **Log Archive Configuration**.
7. Click **Configure Time Periods**.
8. Click **Create**.
9. Specify the appropriate settings. For more information about fields on a window, see the Help.

10. Click **OK**.

11. Click **Finish**.

Note

Configured time periods are not immediately displayed in the Control Center. To display time periods in Trend Analysis reports, the reporting server must process the data using the new or modified time period settings.

The default processing time for the reporting server is 3 hours. For more information about configuring the reporting server processing job, see the *User Guide for NetIQ Security Manager*.

Modifying Security Manager Time Periods

Using the Configuration Wizard, you can modify the time ranges of existing time periods.

To modify a time period:

1. Log on to a central computer as a member of the OnePointOp ConfigAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.
4. On the Tasks menu, click **Global Tasks > Launch Configuration Wizard**.
5. Click **Global Settings**.
6. Click **Log Archive Configuration**.
7. Click **Configure Time Periods**.
8. Select the time period to change.
9. Click **Modify**.
10. Specify the appropriate settings. For more information about fields on a window, see the Help.

11. Click **OK**.
12. Click **Finish**.

Deleting Security Manager Time Periods

If a time period is no longer necessary, you can delete the time period using the Configuration Wizard. You must define a time period for each hour of the day.

To delete a time period:

1. Log on to a central computer as a member of the OnePointOp ConfigAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.
4. On the Tasks menu, click **Global Tasks > Launch Configuration Wizard**.
5. Click **Global Settings**.
6. Click **Log Archive Configuration**.
7. Click **Configure Time Periods**.
8. Select the time period to delete.
9. Click **Delete**.
10. Click **Yes**.
11. Click **Finish**.

Configuring Notification of Real-Time Alerts

This section provides tasks for configuring email or paging notification of real-time alerts. Security Manager supports SMTP for email and paging notification.

Security Manager uses **notification groups** to control email and paging notification recipients. Notification groups are lists of operators that receive notifications when specified alerts occur. An **operator** is a person and specific schedule configured to receive real-time email or page notifications from Security Manager. Security Manager provides built-in notification groups configured to notify the operators when an alert of severity level **Error** or higher is generated.

Default Notification Groups

Security Manager provides the following default notification groups. Add operators to these notification groups if you want automatic notification to occur when Security Manager generates an alert of severity level **Error** or higher.

Network Administrators

Responsible for maintaining monitored networks. Security Manager, by default, notifies operators in the Network Administrators notification group when alerts of severity level **Error** or worse occur for Security Manager components.

Security Manager Administrators

Responsible for monitoring and maintaining Security Manager itself. Security Manager notifies operators in this notification group when the Security Manager product experiences various kinds of issues that can affect the product's ability to monitor the environment. NetIQ recommends that all administrators be members of this group.

Other products that provide Security Manager modules may include additional notification groups.

Adding Operators to Notification Groups

To enable Security Manager to notify key personnel when an alert occurs, add operators to a notification group. NetIQ modules automatically send alerts to default notification groups, such as Network Administrators.

To add operators to notification groups:

1. Ensure you create an email address for each operator you want to receive notification from Security Manager. For more information about creating email addresses, see the SMTP documentation.
2. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group.
3. Start the **Development Console** in the NetIQ Security Manager program folder.
4. In the left pane, expand **Security Manager Development Console**, and then expand **Configuration > Notification Groups**.
5. Add an operator to the notification group by completing the following steps:
 - a. Select the notification group in the right pane.
 - b. On the Action menu, click **Create Operator**.
 - c. Follow the instructions until you have finished creating an operator. For more information about fields on a window, click **Help**.
6. Repeat Step 5 for each notification group.

Rolling Out Additional Configuration Groups

In some large environments, you may want to use multiple configuration groups. For more information about whether additional configuration groups are appropriate for your environment, see “Understanding Multiple Configuration Groups” on page 29.

Repeat the procedures in “Planning to Roll Out Your Configuration Groups” on page 26 and “Security Manager Installation Checklist” on page 86 for each configuration group you want to install.

Chapter 4

Manually Installing Unmanaged Windows Agents

Under certain circumstances, installing an agent manually on a Windows computer is preferable to allowing the central computer to automatically deploy the Windows agent. Consider the following situations where manually installing a Windows agent could save time, money, security, and configuration costs:

- The monitored Windows computer accesses the network over a WAN connection. Manual Windows agent installation saves both connectivity time and expense.
- The monitored Windows computer is outside your interior network firewall. Manual Windows agent installation saves configuration time and allows you to monitor this computer without jeopardizing network security. For more information about installing unmanaged agents in a firewall environment, see “Installing and Configuring Security Manager in Firewall Environments” on page 161.
- The monitored Windows computer is in a controlled environment that requires you to know exactly what, when, and how Windows agents are installed, and you need to retain complete control over the process. Manual Windows agent installation gives you this control.

You manually install and upgrade unmanaged agents. System requirements are the same for managed (automatically deployed) and unmanaged (manually installed) Windows agents. For more information about Windows agent system requirements, see “Installing Windows Agents” on page 68.

Note

The steps in the following sections describe manually installing unmanaged agents on Windows computers.

For more information about installing UNIX agents on UNIX or Linux computers, see the NetIQ UNIX Agent documentation, available in the NetIQ UNIX Agent installation kit. For more information about installing iSeries agents on iSeries servers, see the NetIQ Security Solutions for iSeries documentation, available in the NetIQ Security Solutions for iSeries installation kit.

Understanding Unmanaged Windows Agent Installation

The unmanaged Windows agent setup program installs an agent on the local Windows computer.

When you manually install an unmanaged agent on a Windows computer, the unmanaged agent attempts to connect to the central computer that you specify in the setup program. An unmanaged agent identifies itself to the central computer at the time of the first successful connection. However the central computer does not accept communication from the agent until you authorize it with the Agent Administrator.

Notes

- You cannot install an unmanaged agent on a Security Manager central computer or user interface computer. However, you can install an unmanaged agent on a log archive server or database server.
 - You cannot install an unmanaged agent on a computer that already has a managed Security Manager agent installed.
 - You cannot install Security Manager components on a computer that already has an unmanaged agent installed.
-

Installing and Configuring a Windows Agent Manually

You can manually install an unmanaged agent on a Windows computer. After you install an unmanaged agent, you can make changes to its configuration. For more information about reassigning an unmanaged agent to a different central computer, see the *User Guide for NetIQ Security Manager*.

For more information about monitoring an unmanaged agent with multiple configuration groups, see “Monitoring an Unmanaged Agent with Multiple Configuration Groups” on page 124.

When you install an unmanaged agent on a new computer, Security Manager does not immediately display the new computer in the Infrastructure Components > Agents view.

You must first authorize the new unmanaged agent, after which the agent sends a heartbeat to the central computer. Security Manager sends the unmanaged agent configuration data, and at the next agent heartbeat, the agent sends configuration information back to the central computer. Security Manager then assigns the new unmanaged agent computer to all applicable computer groups and displays the agent in the Agents view.

For more information about configuring the heartbeat interval for agents, see the *User Guide for NetIQ Security Manager*.

Installing an Unmanaged Windows Agent Manually

The manual Windows agent setup program installs an agent on the local Windows computer and guides you through Windows agent configuration. You can also silently run the setup program. For more information about installing unmanaged agents silently, see “Installing or Upgrading Unmanaged Agents Silently” on page 188.

To manually install an agent on a Windows computer:

1. Log on with an administrator account to the computer on which you want to install an unmanaged agent.
2. Close all open applications.

3. Run the `Manual Agent.msi` program located in the `Additional Setups\Manual Agent Installation` folder in the installation kit.

Note

When you manually install an agent on a computer with Windows Server 2008 or Windows Vista installed, you may need to run the setup program using the built-in administrator account.

To run `Manual Agent.msi` as the administrator, open the command-line interface using the `runas` command:

```
runas /user:administrator cmd
```

In the command-line interface, enter the following command:

```
msiexec /i c:\installation folder\Additional Setups\Manual Agent Installation\Manual Agent.msi
```

where *installation folder* is the location where you saved the installation kit.

4. Follow the instructions until you have finished manually installing the unmanaged Windows agent.
5. Log on to the central computer as a member of the `OnePointOp ConfigAdms` group.
6. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
7. In the Tasks pane, click **Launch Agent Administrator**.
8. In the left pane, click **Unmanaged Agents**.
9. In the right pane, click **Authorize Unmanaged Agents**.
10. Select the unmanaged agent you want to authorize.
11. Click **OK**.
12. Select **Apply configuration changes now**.
13. Click **OK**.

14. Verify the selected central computer and click **OK**.
15. Click **Close**.

Monitoring an Unmanaged Agent with Multiple Configuration Groups

You can monitor an unmanaged agent using more than one configuration group. For more information about multiple configuration groups, see “Understanding Multiple Configuration Groups” on page 29.

To add configuration groups to an unmanaged agent:

1. Log on to the unmanaged agent computer as a member of the local Administrators group.
2. Start the **Configure Multiple Configuration Groups** utility in the NetIQ Security Manager > Configuration Utilities program group.
3. Select **Add this agent to another configuration group**.
4. In the **Configuration Group Name** field, type the configuration group name you want to add.
5. In the **Central Computer Name** field, type the central computer you want assigned to the unmanaged agent.
6. Click **OK**, and then click **OK**.
7. In the configuration group you added, log on to the central computer as a member of the OnePointOp ConfigAdms group.
8. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
9. Click **Configuration Groups**.
10. In the Tasks pane, click **Launch Agent Administrator**.
11. In the left pane click **Unmanaged Agents**.

12. In the right pane, click **Authorize Unmanaged Agents**.
13. Complete the wizard, specifying the unmanaged agent you are adding to the configuration group. For more information about fields on a window, see the Help.
14. Click **OK**.

Uninstalling Unmanaged Windows Agents

When you no longer want to monitor an unmanaged agent computer, uninstall the unmanaged agent with the Add or Remove Programs utility. For more information about uninstalling unmanaged Windows agents, see “Uninstalling Unmanaged Agents from All Configuration Groups” on page 249.

Chapter 5

Installing the User Interfaces

This chapter describes how to install the Security Manager user interfaces:

Security Manager Control Center

Allows you to manage alerts about real-time events, create Trend Analysis and Forensic Analysis reports of archived log data, compile your research into incident packages, and configure Security Manager. The Control Center also allows you to monitor this data across multiple configuration groups.

Security Manager Development Console

Allows you to customize processing rules, computer groups, and other Security Manager components for your environment.

Security Manager Web Console

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

Note

The Web Console requires Microsoft Internet Explorer 6.0, Internet Explorer 7.0, or Internet Explorer 8.0, Microsoft Internet Information Services (IIS) 6.0, 7.0, or 7.5, and access to the Web Console server.

If installed on a Windows Server 2008 computer, the Web Console also requires the IIS 6.0 Management Compatibility components.

For more information about Web Console prerequisites, see “Web Console Requirements” on page 77.

Installing User Interfaces Checklist

This section guides you through the process of installing additional user interfaces on computers other than the central computer. You can install user interfaces by completing the following checklist:

| <input checked="" type="checkbox"/> | Steps | See Section |
|-------------------------------------|--|---|
| <input type="checkbox"/> | 1. Review the user interface requirements. | “Planning to Install Your User Interfaces” on page 74 |
| <input type="checkbox"/> | 2. Ensure you have the proper group memberships. | “Planning to Install Your User Interfaces” on page 74 |
| <input type="checkbox"/> | 3. Install the user interfaces you need. | “Installing the User Interfaces” on page 129 |
| <input type="checkbox"/> | 4. Review how to access the user interfaces. | “Accessing User Interfaces” on page 130 |
| <input type="checkbox"/> | 5. Return to the installation checklist. | “Security Manager Installation Checklist” on page 86 |

Installing the User Interfaces

To install user interfaces, ensure your user account is a member of the local Administrators group on the user interface computer and has network access to a central computer and the database server.

To install the user interfaces:

1. Log on as a member of the local Administrators group to the computer on which you want to install the Security Manager user interfaces.
2. Close all open applications.
3. Run the setup program from the Security Manager product installation kit.
4. Click **Verify Prerequisites** on the Setup tab.
5. Follow the instructions until you have installed all the necessary prerequisites for the Security Manager user interfaces you want to install. You can install some of the required software using the Verify Prerequisites tool.
6. When you finish installing prerequisites, click **Finish** on the NetIQ Security Manager Verify Prerequisites window.
7. *If the setup program is not open*, run the setup program from the Security Manager installation kit.
8. Click **Begin Setup** on the Production Setup tab.
9. Follow the instructions in the setup program until you reach the Installation Type window.
10. Select **User Interface Computer** on the Installation Type window, and then click **Next**.
11. Select the user interfaces you want to install, and then click **Next**.
12. Follow the instructions in the setup program until you finish installing Security Manager user interfaces.

13. Click **Finish**.
14. Close the Web browser.

Accessing User Interfaces

To access the Control Center or Development Console, click the name of the console in the NetIQ Security Manager program folder.

You can run the Web Console from any Windows computer running Internet Explorer that has access to the central computer hosting the Web Console server.

To run the Web Console:

1. Start Internet Explorer.
2. Set your Internet Explorer Intranet security levels by completing the following steps:
 - a. On the Tools menu, click **Internet Options**.
 - b. Click the Security tab.
 - c. Click **Local intranet**.
 - d. Click **Custom Level**.
 - e. Select **Medium** in the **Reset to** list.
 - f. Click **Reset**.
 - g. Click **Yes**.
 - h. Select **Prompt** in the **Download unsigned ActiveX controls in the Settings** list.
 - i. Click **OK** on the Security Settings window.
 - j. Click **Yes** to confirm.
 - k. Click **OK** on the Internet Options window.

3. Type `https://WebConsoleServerName:1271` in the **Address** field, where *WebConsoleServerName* is the name of the Web Console server computer.

Note

If you are not using secure HTTP, type `http://WebConsoleServerName:1271` in the **Address** field.

4. Click **Go**.
5. *If you want to view reports*, click **Reports**. You must have the SQL Server Reporting Services Report Server configured before you can access published Summary reports. For more information about configuring the Report Server Web address, see the *User Guide for NetIQ Security Manager*.
6. Click **Go**.

For more information about using the interfaces, see the *User Guide for NetIQ Security Manager*.

Chapter 6

What to Do Next

After you have installed Security Manager, you can customize it for your environment and begin monitoring the security of your network.

Customizing Security Manager

You can customize your Security Manager implementation to suit the specific needs of your environment using the following tools:

Control Center

Provides alerts and customizable views to monitor real-time events, reports to examine archived log data, incident packages to gather and share your research, and wizards that allow you to configure Security Manager. You can customize the Control Center to allow you to monitor this data across multiple configuration groups. You can also customize the Today page to provide graphs of data. For more information about customizing with the Control Center, see the *User Guide for NetIQ Security Manager* or the Help.

Development Console

Provides advanced development features that allow you to create, modify, and delete processing rules and configure other Security Manager components. Processing rules configure Security Manager to collect or filter information, such as an event, or automatically react to a detected condition with an alert or response. For more information about customizing with the Development Console, see the *Programming Guide for NetIQ Security Manager* or the Help.

Configuring Advanced Features

Security Manager provides advanced features to help you customize your monitoring environment. You can use the Development Console to create rules that collect, process, and respond to information. You can also configure Security Manager to send and receive SNMP traps, and extend Security Manager monitoring abilities using Windows Management Instrumentation (WMI). For more information about configuring Security Manager monitoring, see the *Programming Guide for NetIQ Security Manager*.

Connecting to Multiple Configuration Groups

If you have multiple configuration groups and want to monitor them with a single Control Center, configure a central computer to connect to the configuration groups. For more information about configuring multiple configuration group connections, see the *User Guide for NetIQ Security Manager*.

Monitoring Agents with Multiple Configuration Groups

You may want to use multiple configuration groups to monitor an agent. You can specify additional configuration groups after agent installation is complete. The following procedure assumes you have already installed multiple configuration groups and installed the managed agent in one configuration group.

To add a managed to agent to additional configuration groups:

1. In the configuration group you want to add, start the **Security Manager Control Center** in the NetIQ Security Manager program group.
2. Click **Configuration Groups**.
3. In the Tasks pane, click **Launch Agent Administrator**.
4. In the left pane, click **Managed Agents**.
5. In the right pane, click **Deploy Agents**.
6. Click **Add**.
7. Specify the managed agent you want to monitor.
8. Click **OK**.
9. Repeat Steps 1 through 8 for each configuration group you want to monitor the managed agent.

You can also monitor an unmanaged agent with multiple configuration groups. For more information about monitoring unmanaged agents, see “Monitoring an Unmanaged Agent with Multiple Configuration Groups” on page 124.

Providing Additional Security

For an additional level of security, you can assign security permissions to administrative groups for all folders within the NetIQ Security Manager program folder on the central computer. These folders contain agent configuration and installation files. Ensuring only administrators can edit these folders provides additional security.

You can also configure the permissions global groups have over Security Manager computer groups. Configuring global group permissions to computer groups allows you to limit the computer data users can see in views and reports. For more information about configuring global group permissions, see Appendix A, “Setting Permissions on Computer Groups”.

Customizing Rules

Processing rules configure Security Manager to process events, alerts, and responses. You can review configuration information for processing rules using the Development Console.

Review processing rules that contain the word **Customize** to see if you want to customize them for your environment. You can perform a search for these rules in the Development Console, and then read the Knowledge Base for each rule.

You may want to customize these processing rules for several reasons:

- You use Security Manager in a non-English environment.
- You changed the name of the administrator or guest accounts.

You can customize any processing rule. For more information about working with rules, see the *Programming Guide for NetIQ Security Manager*.

To review configuration information for rules you should customize:

1. Log on to the Development Console computer using an account that is a member of the OnePointOp Operators group.
2. Start the **Development Console** in the NetIQ Security Manager program folder.
3. In the left pane, expand **Security Manager Development Console**, and then click **Processing Rule Groups**.
4. On the Action menu, click **Find Processing Rules**.
5. Click **All processing rule groups**.
6. Click **Next**.
7. Select **Rule name**, select **contains substring** from the list, and then type **Customize** in the blank field.
8. Click **Next**.
9. Click **Finish**.
10. Double-click a rule in the results pane.

11. Click the Knowledge Base tab.
12. Repeat Steps 10 through 11 to examine the Knowledge Base for each rule.
13. *If you need to customize the rule for your environment*, follow the instructions in the Knowledge Base to customize the rule as required.

Configuring Log Archive Data Signing

To ensure the integrity of your log archive data, you can choose to digitally sign log data from some or all of your central computers. You must specify settings and digital signatures on the log archive server and any central computers you want to sign data. Security Manager adds a digital signature to each message block from configured central computers. The log archive server adds a second level of protection by signing each completed log archive file, which is a collection of message blocks.

If you want to sign your log archive data, enable and configure data signing after installing Security Manager. For more information about digitally signing log archive data, see the *User Guide for NetIQ Security Manager*. Configuring data signing in Security Manager includes performing the following tasks on the log archive server and on each central computer:

- Creating and managing certificates
- Enabling data signing on the log archive server and configuring settings as necessary, including the distinguished name of the certificate subject and the certificate store location
- Enabling data signing on each central computer, as necessary

Notes

- You typically configure the use of data signing immediately after installation, during initial product configuration. Log archive data will *not* be signed until you enable data signing and provide the appropriate certificates.
- When you configure data signing on the log archive server, ensure the service account used to run the NetIQ Security Manager Log Archive service has Read and Write access on the certificate you want to use to sign data. Review the access control list (ACL) of the key container file to ensure the service user has Read and Write permissions, at minimum. For more information about key containers, see the following article on the Microsoft support site:

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

Warning

You must enable data signing on the log archive server before enabling data signing on any central computer. If you enable data signing on a central computer but not on the log archive server, your data will remain in the import message queue and will not be processed for storage in the log archive.

Creating and Managing Certificates

If Microsoft Certificate Services is available on a server in your environment, you can use its Web user interface to manage your local certificates. Alternatively, you can use the MMC Certificates snap-in to request and manage certificates from accessible Certification Authorities (CA). You can create, install, and manage different types of certificates, including signing certificates and root CA certificates. For more information about managing certificates, search for the following Microsoft TechNet articles at technet.microsoft.com:

- “How IT Works: Certificate Services”
- “Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure”
- “Certificate Revocation and Status Checking”

Perform the following tasks on the log archive server and on each signing central computer:

- Request a signing certificate from a CA, with an appropriate name for the certificate subject and any other options appropriate for your environment. For example, you could specify `NetIOSMCore-DataSigning` as the certificate subject name.
- Ensure the certificate includes the private key. Exporting the key to a file may remove the private key from the certificate.
- Ensure the `keyUsage` setting for the certificate includes the `DigitalSignature` value.
- Ensure the certificate includes the private key. Exporting the key to a file may remove the private key from the certificate.
- Ensure the private key in the certificate does not require a password. When requesting the certificate, clear **Enable strong private key protection** before submitting your request.

- Install the signing certificate in the **Personal** container of either the **CurrentUser** or **Local Machine** certificate store. If you want to install the certificate in the **CurrentUser** certificate store, ensure you log in using the service account for the log archive server or central computer.
- Obtain and install the CA root certificate for the issuing server in the **Trusted Root Certification Authorities** container of either the **CurrentUser** or **Local Machine** certificate store.

Enabling and Configuring Data Signing on the Log Archive Server

You can enable and configure data signing on the log archive server using the Log Archive Configuration utility. If you modify your log archive data signing settings, you must restart the NetIQ Security Manager Log Archive service.

To enable and configure log archive data signing on the log archive server:

1. Log on to the log archive server using an account that is a member of the OnePointOp ConfigAdms group. For more information about groups and permissions, see “Understanding Security Manager Requirements and Permissions” on page 79.
2. Start **Log Archive Configuration** in the NetIQ Security Manager > Configuration program group.
3. Click **Log Archive Server Settings**.
4. Select **Enable Data Signing** and select **True** from the list.
5. *If you want to use a certification store for the current user*, click the **Data Signing Certificate Store** field and select **CurrentUser**.
6. *If you want to use a certification store for the local computer*, click the **Data Signing Certificate Store** field and select **Local Machine**.
7. Type the distinguished name of the certificate subject in the **Data Signing Certificate Subject Name** field, as in the following example:

CN=NetIQSMCore-DataSigning

Warning

You must specify the complete distinguished name for the certificate subject, including other information specified when you requested the certificate. For example:

E=testuser@company.com, CN=NetIQSMCore-DataSigning

If you do not specify the full name, the NetIQ Security Manager Log Archive service cannot initialize when Security Manager restarts the service. For more information about determining the complete distinguished name, contact NetIQ Technical Support.

8. Click **Apply**, and then click **Yes**.
 9. Click **Close**.
 10. Click **Yes** on the confirmation message to restart the NetIQ Security Manager Log Archive service.
-

Note

If you modify any log archive setting, you must restart the NetIQ Security Manager Log Archive service for the change to take effect.

Enabling Data Signing on Central Computers

You can turn data signing on and off on each central computer by editing the service configuration file. The NetIQ Security Manager Core service must be restarted for the change to take effect.

Warning

You must enable data signing on the log archive server before enabling data signing on any central computer. If you enable data signing on a central computer but not on the log archive server, your data will remain in the import message queue and will not be processed for storage in the log archive.

To enable log archive data signing on central computers:

1. Log on to a central computer you want to digitally sign data, using an account that is a member of the OnePointOp ConfigAdms group. For more information about groups and permissions, see “Understanding Security Manager Requirements and Permissions” on page 79.
2. Navigate to *installation folder*\NetIQ Security Manager\NetIQ Security Manager Core, where *installation folder* is the location where you installed Security Manager.
3. Edit SMServicelHost.exe.config and locate the DataSigning section.
4. Change the enable entry to enable="true".
5. *If you want to use a certification store for the current user*, set the location entry to certStoreLocation="CurrentUser".
6. *If you want to use a certification store for the local computer*, set the location entry to certStoreLocation="Local Machine".
7. Change the distinguished name of the certificate subject in the **Data Signing Certificate Subject Name** field, as in the following example:

```
certSubjectDN="CN=NetIQSMCore-DataSigning, OU=Engineering,  
O=NetIQ Corporation, L=Houston, S=Texas, C=US"
```

Warning

You must specify the complete distinguished name for the certificate subject, including other information specified when you requested the certificate.

If you do not specify the full name, the NetIQ Security Manager Core service cannot initialize when Security Manager restarts the service. For more information about determining the complete distinguished name, contact NetIQ Technical Support.

8. Save and close the file.
9. Restart the NetIQ Security Manager Core service.
10. Repeat Steps 1 through 9 for each central computer you want to digitally sign its collected log data.

Troubleshooting Log Archive Data Signing

If you encounter issues configuring Security Manager data signing or using data signing certificates, you may need to verify the following settings.

Note

If you revoke a previously valid digital certificate being used to sign log archive data, Security Manager continues to use the certificate until Windows updates the local Certificate Revocation List (CRL).

Microsoft Windows certificate management caches the CRL locally for a predetermined amount of time, typically a week, after which Windows updates the local CRL and effectively revokes the certificate. Until Windows updates the CRL, you can use a revoked digital certificate to sign log archive data in Security Manager. For more information about this issue, see the Microsoft TechNet Website.

Log Archive Server Service Account

Ensure the service account used to run the `NetIQ Security Manager Log Archive` service has access to the private key in the log archive server signing certificate. By default, private keys are stored in one of the following locations on the log archive server:

```
CurrentUser: \Documents and Settings\USER_NAME\Application  
Data\Microsoft\Crypto\ALGORITHM_TYPE\USER_SID
```

```
Local Machine: \Documents and settings\All Users\Application  
Data\Microsoft\Crypto\ALGORITHM_TYPE\Machinekeys
```

Where *USER_NAME* is the name of the user account used to request and install the certificate, *ALGORITHM_TYPE* is *RSA* or *DSA*, depending on which algorithm the certificate uses, and *USER_SID* is the security identifier (SID) of the user account used to request and install the certificate.

Invalid or Expired Certificate

Ensure the certificates you install on both the log archive server and any central computers are signing certificates and have not expired. If you try to use an expired certificate to sign data, Security Manager cannot restart the `NetIQ Security Manager Log Archive` or `NetIQ Security Manager Core` services.

Strong Private Key Protection Option Selected

When requesting a certificate, ensure you clear **Enable strong private key protection** before submitting your request. If you select this option and then request and install a certificate, Security Manager cannot restart the NetIQ Security Manager Log Archive or NetIQ Security Manager Core services.

Verifying a Successful Installation

After you install Security Manager, verify that the setup program correctly installed the product and the product is functioning correctly.

Note

Security Manager may experience a delay before generating alerts, depending on the Windows agent heartbeat and processing time. For more information about configuring agent heartbeat settings, see the Help.

To verify that Security Manager is installed and functioning correctly:

1. Log on to the computer where you installed your central computer components with a user account that is a member of the OnePointOp Users group.
2. Open the Event Viewer located in the Control Panel.
3. Click **Application**.
4. Click the **Source** column to sort by event source.
5. Scroll down until you find one or more events with the source **Msi Installer**.
6. Right-click the first **Msi Installer** event and select **Properties**.
7. Use the down arrows to search through all **Msi Installer** events.

If you find an Information event with the Description **Successfully installed X**, the setup program installed Security Manager successfully.

If you find an Error event, the setup program could not install all Security Manager components.

8. Log on to a Control Center computer with a user account that is a member of the OnePointOp Users group. For more information about groups and permissions, see “Understanding Security Manager Requirements and Permissions” on page 79.
9. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
10. In the Navigation pane, click **Infrastructure Components > Central Computers**.
11. Verify that all central computers in your configuration group display an Agent Status of Running.
12. In the Navigation pane, click **Agents**.
13. Verify that all deployed agents in your configuration group display an Agent Status of Running.

Installing Additional Security Manager Components

After installing Security Manager, you can install additional components by running the setup program again on existing Security Manager computers.

For more information about installing components using the setup program, see “Installing Security Manager” on page 85.

To install additional Security Manager components on a computer with Security Manager components installed:

1. Log on to the computer on which you want to install additional Security Manager components using an account that is a member of the local Administrators group. Also ensure your logon account is a member of the Microsoft SQL Server `sysadmin` role on the database server and reporting server.
2. Close all open applications.

3. *If the Alert Sentry is running*, right-click the Alert Sentry icon in the system tray, select **Exit** on the menu, and then click **OK**.
4. *If you want to install an additional component on a computer with Windows 2000, Windows Server 2003, or Windows XP installed*, complete the following steps:
 - a. Navigate to the setup program in the Security Manager installation kit.
 - b. Run the setup program.
5. *If you want to install an additional component on a computer with Windows Vista, Windows Server 2008, or Windows 7 installed*, complete the following steps:
 - a. Navigate to the setup program in the Security Manager installation kit.
 - b. Right-click the setup program and select **Run as administrator**.
 - c. Click **Continue**.
6. Click the **Production Setup** tab and click **Begin Production Setup**.
7. Click **Run**.
8. *If you receive a second security warning*, click **Run** again.
9. Click **Next**.
10. Select **Modify**.
11. Click **Next**.
12. On the **Select Security Manager Components** window, select the new component you want to install and click **Next**.
13. Follow the instructions in the setup program until you reach the **Finished** window.
14. Click **Finish**.

Getting Started with Security Manager

The Security Manager Today page (Today page) in the Control Center allows you to obtain an overview of the security status over multiple configuration groups. You can also customize the graphs on this Today page. For more information about this Today page, see the *User Guide for NetIQ Security Manager*.

The Today page in the Control Center is a good page to examine after you first install Security Manager. The Today page provides a quick overview of the status of Security Manager and all monitored computers. You can also use Configuration Groups window in the Control Center to configure Security Manager, deploy agents, and import NetIQ modules.

You must be a member of the OnePointOp Operators or OnePointOp ConfigAdms groups to access the configuration features in the Control Center. For more information about permissions, see “Planning to Install Your User Interfaces” on page 74.

To display the Today page, click **Security Manager Control Center** in the Navigation pane of the Control Center. For more information about using the Security Manager Today page and getting started with Security Manager, see the *User Guide for NetIQ Security Manager* or the Help.

Appendix A

Setting Permissions on Computer Groups

Security Manager uses Windows global groups to control access to Security Manager user interfaces and computer groups.

You can add Windows global groups to the OnePointOp groups to control access to certain Security Manager features and consoles. OnePointOp groups are Windows local groups that Security Manager creates. For more information about OnePointOp groups, see “Understanding Security Manager Requirements and Permissions” on page 79.

For an additional layer of security, you can configure **security filtering**. Security filtering allows you to grant or deny Windows global group permissions on a computer group. For example, you can use computer groups to organize computers by region, and then set permissions on the computer group so only members of a certain Windows global group have access to monitor data for that region.

Understanding Security Filtering

Security filtering allows you to set permissions on computer groups. Setting permissions on computer groups controls the computers that members of Windows global groups can see or modify for the following objects in the Control Center or Web Console:

- Views
- Forensic Analysis reports
- Incident packages

Notes

- Security filtering limits access only to data received from members of a filtered computer group. Security filtering does not limit access to views, reports, queries, or incident packages themselves. Users can open, modify, or delete any normally accessible objects in the Control Center or Web Console, even if Security Manager filters the data contained in those objects.
- In the Web Console, security permission settings do not apply to members of the OnePointOp ConfigAdms group. Members of this group have full access in the Web Console.
- Security filtering does not control what users can see for Trend Analysis reports.
- Avoid setting permissions on built-in Windows computer groups. Use custom Windows computer groups instead.
- You cannot create custom UNIX and iSeries computer groups. Security Manager provides default UNIX and iSeries computer groups to control what users can see in reports and views. All UNIX computers and iSeries servers are added to the computer groups for reports by default. Add computers to UNIX and iSeries computer groups for views with the Configuration Wizard.

Create custom computer groups to organize computers by the users who monitor them. For more information about creating computer groups, see the *Programming Guide for NetIQ Security Manager*.

For example, if you want to allow only database administrators to monitor database computers, you can create a computer group to contain all database computers and create a Windows global group to contain all database administrators. Then you can set permissions on the computer group so only the database administrators group has access to it. For more information about setting computer group permissions, see “Setting Permissions on Computers” on page 152.

Understanding Permission Settings

By default, members of the OnePointOp groups are granted **Write** and **Read** permissions on all computer groups, including custom computer groups. This is similar to granting the Windows Everyone group Full Control access to an object.

With the Control Center, you explicitly grant permissions to Windows global groups, and then remove the OnePointOp group permissions afterwards. Removing the OnePointOp group permissions denies access for anyone who is not a member of the Windows group. Although removing permissions effectively denies access, this behavior is different than setting a **Deny** permission, which overrides all other permission settings.

The following table defines the permissions and their override behavior.

| Permission | Definition |
|-------------------|--|
| Read | Users can see the computer group data, but cannot modify it. |
| Write (and Read) | Users can see and modify the computer group data. This setting overrides Read permissions. |
| Deny | Users cannot see or modify the computer group data. This setting overrides Write and Read permissions. |

Setting Permissions on Computers

Set permissions on computer groups containing computers to which you want to control access. Create custom computer groups to contain Windows computers. Use the built-in UNIX and iSeries computer groups to contain UNIX computers and iSeries servers. You cannot create custom UNIX and iSeries computer groups.

Add computers to UNIX and iSeries computer groups with the Configuration Wizard. Add Windows computers to custom computer groups with the Development Console.

Note

Ensure you explicitly grant permissions to all appropriate Windows global groups before removing the OnePointOp group permissions. OnePointOp groups provide access to product functionality. If you forget to set permissions for a OnePointOp group member and remove the OnePointOp group permissions, that member will no longer have access to Security Manager user interfaces. For more information about OnePointOp groups, see “Understanding Security Manager Requirements and Permissions” on page 58.

The following steps guide you through the process of assigning permissions to Windows computers in a configuration group. If you are assigning permissions to UNIX computers or iSeries servers, use the built-in computer groups instead.

| <input checked="" type="checkbox"/> | Steps |
|-------------------------------------|---|
| <input type="checkbox"/> | 1. Organize users by the permissions you want to grant them into Windows global groups. Ensure the Windows global groups contain members that are also included in the appropriate OnePointOp groups. For more information about OnePointOp groups, see “Understanding Security Manager Requirements and Permissions” on page 79. |
| <input type="checkbox"/> | 2. Create custom computer groups containing the Windows computers to which you want to limit or grant access. For more information about custom computer groups, see the <i>Programming Guide for NetIQ Security Manager</i> . |
| <input type="checkbox"/> | 3. Set permissions on the custom computer groups. For more information about setting permissions on computer groups, see “Configuring Security Filtering” on page 153. |

| | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | Steps |
| <input type="checkbox"/> | 4. Repeat Steps 1 through 3 for each computer group on which you want to set permissions. |
| <input type="checkbox"/> | 5. After you have set permissions on all custom computer groups, remove the permission settings assigned to the OnePointOp groups from all computer groups, including built-in computer groups. Removing OnePointOp group permissions from all computer groups is required before your changes can take effect. Ensure you have configured all permissions settings before performing this step. For more information about removing permissions, see “Removing OnePointOp Group Permissions” on page 155. |

Configuring Security Filtering

You can add, remove, and modify permissions to computer groups by configuring security filtering.

Notes

- Avoid setting permissions on built-in computer groups that contain Windows computers. A Windows computer can be in multiple built-in computer groups. Setting permissions on a built-in computer group can override permissions set on other computer groups. Instead, set permissions on custom computer groups for Windows computers.
- However, because you cannot create custom UNIX or iSeries computer groups, use the built-in UNIX or iSeries computer groups to configure security filtering for UNIX computers or iSeries servers.
- Ensure you do not modify account permissions for the OnePointOp System group. In order to run Forensic Analysis queries on all computers in your configuration group, the OnePointOp System group must have Read permissions for all computer groups.

To configure security filtering:

1. Log onto the Control Center computer as a member of the OnePointOp ConfigAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Configuration Groups**.
4. On the Configuration Groups window, select the configuration group with computer groups on which you want to set permissions.
5. On the Tasks menu, click **Configuration Groups Tasks > Set Security Permissions**.
6. In the left pane, select the computer group for which you want to set permissions.
7. Configure permissions for the computer group. For more information about fields on a window, see the Help.
 - To add a Windows global group, click **Add**.
 - To remove a Windows global group, click **Delete**.
 - To modify permissions for a Windows global group, select or clear the appropriate permission setting.
 - To restore the permission settings for OnePointOp groups, click **Restore Defaults**.
8. Repeat Steps 6 through 7 for each computer group on which you want to set permissions.
9. After you have finished setting permissions, click **OK**. Changes take place immediately for all Control Center users. However, if any computer groups have OnePointOp group permissions assigned to them, these permissions may override your changes until you remove the OnePointOp group permissions. For more information about removing permissions, see “Removing OnePointOp Group Permissions” on page 155.

Removing OnePointOp Group Permissions

All OnePointOp groups are granted **Write** and **Read** access on all computer groups, even custom computer groups. Because **Write** and **Read** permissions override **Read** permissions, remove the OnePointOp permissions from all computer groups after you have completely finished setting permissions on all custom computer groups. Removing OnePointOp group permissions from all computer groups is required before your changes can completely take effect.

Notes

- Do not delete the OnePointOp groups, which are required to provide access to user interfaces.
- Ensure you explicitly grant permissions to all Windows global groups before removing the OnePointOp group permissions. OnePointOp groups provide access to product functionality. If you forget to set permissions for a OnePointOp group member and remove the OnePointOp group permissions, that member will no longer have access to Security Manager user interfaces.
- Ensure you do not modify account permissions for the OnePointOp System group. In order to run Forensic Analysis queries on all computers in your configuration group, the OnePointOp System group must have **Read** permissions for all computer groups.

To remove OnePointOp group permissions:

1. Log onto the Control Center computer as a member of the OnePointOp ConfigAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Configuration Groups**.
4. On the Configuration Groups window, select the configuration group from which you want to remove OnePointOp group permissions.

5. *If you want to remove OnePointOp group permissions for a computer group,* complete the following steps:
 - a. On the Tasks menu, click **Configuration Groups Tasks > Set Security Permissions**.
 - b. In the left pane, select the computer group from which you want to remove OnePointOp group permissions.
 - c. In the right pane, select the OnePointOp group permissions settings you want to remove.
 - d. Click **Delete**, and then click **Yes**.
 - e. Click **OK**.
6. *If you want to remove all OnePointOp group permissions from all computer groups in the configuration group,* on the Tasks menu, click **Configuration Groups Tasks > Delete All OnePointOp Group Permissions**.

Restoring OnePointOp Group Permissions

You may find that you need to continually remove and restore OnePointOp group permissions until you have configured security filtering appropriately.

To restore OnePointop group permissions:

1. Log onto the Control Center computer as a member of the OnePointOp ConfgAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Configuration Groups**.
4. On the Configuration Groups window, select the configuration group to which you want to restore OnePointOp group permissions.

5. *If you want to restore OnePointOp group permissions for a computer group*, complete the following steps:
 - a. On the Tasks menu, click **Configuration Groups Tasks > Set Security Permissions**.
 - b. In the left pane, select the computer group to which you want to restore OnePointOp group permissions.
 - c. Click **Restore Defaults**.
 - d. Click **OK**.
6. *If you want to restore all OnePointOp group permissions to all computer groups in the configuration group*, on the Tasks menu, click **Configuration Groups Tasks > Restore All Default OnePointOp Group Permissions**.

Exporting Security Permissions

After you have defined permissions, you can export them as a simple text file for use in other configuration groups.

You can also export the permissions settings to back them up. Then if your security settings become corrupted, you can restore the permissions settings to a known, good configuration.

To export security permissions:

1. Log onto the Control Center computer as a member of the OnePointOp ConfigAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Configuration Groups**.
4. On the Configuration Groups window, select the configuration group with the permission settings you want to export.

5. On the Tasks menu, click **Configuration Groups Tasks > Export Security Permissions**, specify a name and location for the file, and then click **Save**. The export process may take a few moments.
6. Click **OK** on the window indicating the process has completed successfully.

Importing Security Permissions

After you have defined permissions and exported them, you can import them for use in other configuration groups. You can also import permission settings to restore them.

If you are importing permissions settings into other configuration groups, the configuration groups must have the same Windows global group names and computer group names. The file contains Windows global groups and computer groups as names, not as SIDs.

If there are any differences in computer group and Windows global group names between the two configuration groups, you can manually edit the file to correct the differences. The following is a sample of an exported file:

```
WindowsGroupName      G      ComputerGroupName      1      n
```

The parameters are defined as follows:

| Parameter | Description |
|--------------------------|---|
| <i>WindowsGroupName</i> | Name of the Windows global group to which you want to grant or limit access. |
| G | Identifier for a Windows global group object. |
| <i>ComputerGroupName</i> | Name of the computer group on which you want to set permissions. |
| 1 | Identifier for a computer group object. |
| <i>n</i> | Numeric identifier for the permission setting defined as follows: 1 = Read permissions 2 = Deny permissions 5 = Write (and Read) permissions |

To import security permissions:

1. Log onto the Control Center computer as a member of the OnePointOp ConfigAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Configuration Groups**.
4. On the Configuration Groups window, select the configuration group to which you want to import security permissions.
5. On the Tasks menu, click **Configuration Groups Tasks > Import Security Permissions**, browse to the file, and then click **Open**.

6. Specify the appropriate import option:
 - To completely replace the security settings, click **Replace all existing security permissions**.
 - To merge security settings that are already applied to the configuration group with those specified in the file, click **Merge with existing security permissions**.
7. Click **OK**. The import process may take a few moments.
8. Click **OK** on the window indicating the process has completed successfully.

Appendix B

Installing and Configuring Security Manager in Firewall Environments

To allow Security Manager to monitor computers in a firewall environment, ensure you open the appropriate ports to allow communication between Security Manager components and monitored computers and within Security Manager itself.

The following sections provide information necessary for installing and configuring Security Manager to work properly with firewalls. For more information about configuring firewalls and Security Manager, contact NetIQ Technical Support.

Supported Environments

NetIQ Corporation does not support managed agents separated from the central computer by a firewall or other device or configuration that can impede RPC or NetBIOS functionality.

When monitoring computers behind a firewall, NetIQ Corporation recommends manually installing unmanaged agents on your remote computers. For more information about manually installing unmanaged Windows agents, see “Understanding Unmanaged Windows Agent Installation” on page 120.

Note

In addition, NetIQ does not support using proxy agents to monitor agentless computers where a firewall or other device separates the proxy agent from the monitored computer.

To install Security Manager in a firewall environment, you must configure all firewalls to allow the domains in which you want to install Security Manager components to trust one another. For more information about configuring a firewall to allow trust, see Microsoft Knowledge Base Article 179442 on the Microsoft support site at support.microsoft.com.

Understanding Security Manager Ports

The ports listed in the following table are the default ports used for communication between Security Manager components.

| Component | To Component (if applicable) | Port Number | Purpose |
|------------------|------------------------------|-------------|--|
| Central computer | Database server | TCP 1433 | By default, the central computer uses this port to connect to the OnePoint database on the database server. This port is the default port for Microsoft SQL Server. Instances use alternate ports configured during installation. |
| | | UDP 1434 | If using a SQL Server instance, the browser service uses UDP 1434 to identify the port for the named instance. |

| Component | To Component (if applicable) | Port Number | Purpose |
|-----------|------------------------------|--------------|---|
| | Database server | TCP 135 | The database server uses this port to discover the Microsoft Distributed Transaction Coordinator (MSDTC) listening port on the central computer. |
| | | TCP (random) | <p>MSDTC on the database server computer uses RPC dynamic port allocation to randomly select a port number ranging from 1024 to 65535 for communication with the central computer.</p> <p>If you use a firewall to separate the database server from the central computer, the database server cannot communicate with the central computer unless you restrict RPC port usage to a specific number of ports higher than 1024 and then open those ports.</p> <p>For more information about configuring MSDTC and RPC port usage, see Microsoft Knowledge Base Articles 250367, Q300083, and 826852 on the Microsoft support site at support.microsoft.com.</p> |

| Component | To Component (if applicable) | Port Number | Purpose |
|-----------|------------------------------|--------------------------|--|
| | Log archive server | TCP 8989 | By default, the central computer uses this port to communicate with the log archive on the log archive server. You can configure this port using the Configuration Wizard. For more information about modifying log archive server settings, see the <i>User Guide for NetIQ Security Manager</i> . |
| | | TCP 1801 | The central computer uses this port to push data from the central computer to the log archive server using Microsoft Message Queuing (MSMQ). |
| | Central computer | TCP 8270 (Bidirectional) | The central computer uses this port for correlation with other central computers. |
| | | TCP 1625 (Bidirectional) | The central computer uses this port to communicate with the Configuration Wizard. |
| | SMTP | TCP 25 | The central computer uses this port to send email notifications. |
| | NetIQ AutoSync Server | HTTP 80 | The central computer uses this port to check the NetIQ AutoSync Server for new or updated modules. |

| Component | To Component (if applicable) | Port Number | Purpose |
|--------------------|------------------------------|---------------------------|--|
| | Windows agents | TCP 445 (SMB over TCP) | The central computer uses the Server Message Block protocol (SMB) over TCP port 445 to manage managed agents on Windows computers. |
| | UNIX agent | TCP 1622 | The central computer uses this port for a VigilEnt protocol connection to UNIX agents. |
| | iSeries agent computer | TCP 1622 | The central computer uses this port for a VigilEnt protocol connection to iSeries agents. |
| Log archive server | Reporting server | TCP 1433 | By default, the log archive server uses this port to connect to the Reporting server databases. This port is the default port for Microsoft SQL Server. Instances use alternate ports configured during installation. |
| | Reporting server | UDP 1434 | If using a SQL Server instance, the browser service uses UDP 1434 to identify the port for the named instance. |
| | Sentinel server | TCP 8443 | If using Novell Sentinel to search data stored in the log archive, the log archive server listens for requests from Sentinel on TCP 8443 by default. |

| Component | To Component (if applicable) | Port Number | Purpose |
|---------------------------|-------------------------------------|--------------------|---|
| Reporting server | Database server | TCP 1433 | By default, the reporting server uses this port to connect to the database server. This port is the default port for Microsoft SQL Server. Instances use alternate ports configured during installation. |
| | | UDP 1434 | If using a SQL Server instance, the browser service uses UDP 1434 to identify the port for the named instance. |
| Windows agent (unmanaged) | Central computer | TCP 8270 | The new Windows agent, version 6.5 and later, uses this port to connect to the central computer. |
| | | TCP 1270 | The legacy Windows agent, version 6.0 and earlier, uses this port to connect to the central computer. The legacy Windows agent can coexist with the new Windows agent. |
| UNIX agent | Central computer | TCP 1636 | The UNIX agent uses this port to communicate with the central computer. |
| | UNIX Agent Manager | TCP 2620 | The UNIX agent uses this port to communicate with the UNIX Agent Manager computer. |
| iSeries agent computer | Central computer | TCP 1636 | The iSeries agent uses this port to communicate with the central computer. |

| Component | To Component (if applicable) | Port Number | Purpose |
|---------------------------------|------------------------------|--------------|---|
| Security Manager Control Center | Central computer | TCP 8737 | The Control Center uses this port to connect to the NetIQ Security Manager Core service on the central computer. |
| | | TCP 135 | The Control Center wizards (Configuration Wizard, Agent Administrator, Module Importer, and Correlation Wizard) use this port to discover the Windows Distributed Component Object Model (DCOM) listening port on the central computer. |
| | | TCP (random) | <p>Windows DCOM on the Control Center computer uses RPC dynamic port allocation to randomly select a port number ranging from 1024 to 65535 for communication with the central computer.</p> <p>If you use a firewall to separate the Control Center computer from the central computer, the Control Center wizards cannot communicate with the central computer unless you restrict RPC port usage to a specific number of ports higher than 1024 and then open those ports.</p> <p>For more information about configuring RPC port usage, see Microsoft Knowledge Base Articles Q300083 and 826852 on the Microsoft support site at support.microsoft.com.</p> |

| Component | To Component (if applicable) | Port Number | Purpose |
|-----------|------------------------------|-----------------------------|--|
| | | TCP 1625 (Bidirectional) | The Configuration Wizard uses this port to communicate with the central computer when the user interfaces are installed on a remote computer. |
| | Database server | TCP 1433 | By default, the Control Center uses this port to connect to the OnePoint database on the database server. This port is the default port for Microsoft SQL Server. Instances use alternate ports configured during installation. |
| | | UDP 1434 | If using a SQL Server instance, the browser service uses UDP 1434 to identify the port for the named instance. |
| | Reporting server | TCP 2383 | The Control Center uses this port to connect to SQL Server Analysis Services on the reporting server. |
| | | TCP 2382 | The Control Center uses this port to connect to the SQL Server Analysis Services Browser when resolving instance names. |
| | | TCP 2725 | The Control Center uses Microsoft Office Web Components to display reporting server data in Trend Analysis report format. Microsoft Office Web Components uses this port to communicate with the reporting server. |

| Component | To Component (if applicable) | Port Number | Purpose |
|---------------------|------------------------------|--------------------------|---|
| Development Console | Central computer | TCP 135 | The Development Console uses this port to discover the Windows Distributed Component Object Model (DCOM) listening port on the central computer. |
| | | TCP (random) | <p>Windows DCOM on the Development Console computer uses RPC dynamic port allocation to randomly select a port number ranging from 1024 to 65535 for communication with the central computer.</p> <p>If you use a firewall to separate the Development Console from the central computer, the Development Console cannot communicate with the central computer unless you restrict RPC port usage to a specific number of ports higher than 1024 and then open those ports.</p> <p>For more information about configuring RPC port usage, see Microsoft Knowledge Base Articles Q300083 and 826852 on the Microsoft support site at support.microsoft.com.</p> |
| | | TCP 1625 (Bidirectional) | The Configuration Wizard uses this port to communicate with the central computer when the user interfaces are installed on a remote computer. |

| Component | To Component (if applicable) | Port Number | Purpose |
|-------------------------|---------------------------------------|-------------|--|
| | Database server | TCP 1433 | <p>By default, the Development Console uses this port to connect to the OnePoint database on the database server.</p> <p>This port is the default port for Microsoft SQL Server. Instances use alternate ports configured during installation.</p> |
| | | UDP 1434 | If using a SQL Server instance, the browser service uses UDP 1434 to identify the port for the named instance. |
| Web Console | Central computer (Web Console server) | HTTP 1271 | <ul style="list-style-type: none"> When secure HTTP is enabled on IIS, use the following URL to access the Web Console: <code>https://<i>WebConsoleServerName</i>:1271.</code> When secure HTTP is not enabled on IIS, use the following URL to access the Web Console: <code>http://<i>WebConsoleServerName</i>:1271.</code> |
| Report Manager Web site | Reporting server | HTTP 80 | The Report Manager Web site uses this port to connect to the Reporting server. |

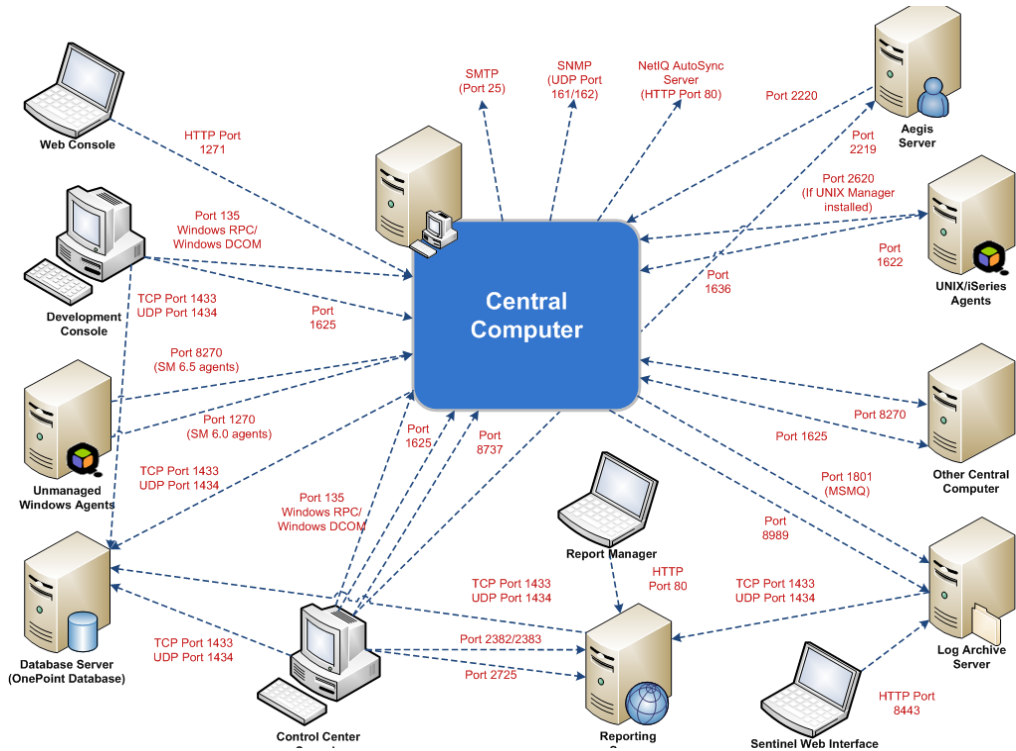
| Component | To Component (if applicable) | Port Number | Purpose |
|--------------|------------------------------|-------------|--|
| Aegis server | Central computer | TCP 2220 | If you have configured Aegis to retrieve data from your central computer, you must open this port on your central computer to allow the Aegis server to communicate. |

Notes

- The Security Manager reporting server uses several Microsoft products, including SQL Server, SQL Server Analysis Services, SQL Server Reporting Services, and SQL Server Integration Services, that require various ports.
- All SQL ports listed are the default ports. If you want to use named instances for any Security Manager SQL Server databases or services, configure named instances before installing Security Manager and specify the named instances during installation.
- If you want to use a non-default port and have stopped the SQL Server Browser service, you must open the non-default port and create an alias for the port on all central computers and user interface computers.
- Security Manager does not support using SQL aliases when installing the database server.

For more information about Microsoft SQL Server and ports, see the Microsoft product documentation.

The following graphic displays the various Security Manager components and the ports they use to communicate.



Troubleshooting Firewall-Related Issues

If you encounter issues with Security Manager components communicating through a firewall, you may need to verify that you have configured Microsoft Distributed Transaction Coordinator (MSDTC) correctly on all central computers and database servers.

For more information about the MSDTC settings required to install database servers, see “Planning to Install Your Database Server” on page 44. For more information about the MSDTC settings required to install central computers, see “Planning to Install Your Central Computers” on page 52.

You can also use the `DTCping` tool to verify connectivity between Security Manager computers. `DTCping` tests name resolution, RPC communication, and MSDTC communication between two computers that have the tool installed and displays MSDTC settings.

For more information about troubleshooting MSDTC-related issues and using `DTCping`, see Microsoft Knowledge Base Articles 250367, 306843, and 918331 on the Microsoft support site at support.microsoft.com.

Appendix C

Installing Reporting Components in Clustered Environments

You can install the Security Manager reporting server on clustered instances of Microsoft SQL Server. However, because the reporting server setup program must install Security Manager-specific files on each node in a cluster, you must perform additional steps before and during the installation process.

Supported Environments

Security Manager supports clustered instances of the Standard and Enterprise versions of Microsoft SQL Server. Security Manager supports both failover (active/passive) and multi-instance (active/active) SQL Server clustering.

Note

Do not configure SQL Server Integration Services as part of your shared cluster resources. Instead, install SQL Server Integration Services on all nodes of your cluster.

For more information about configuring SSIS in a cluster, search for the Microsoft TechNet article “Configuring Integration Services in a Clustered Environment” at technet.microsoft.com.

For more information about installing Microsoft SQL Server, see “Installing Microsoft SQL Server” on page 33, the Microsoft SQL Server documentation, and the Microsoft SQL Server Web site at www.microsoft.com/sql.

Installing Reporting Components in a Clustered Environment

If you want to install reporting server components on a SQL Server cluster, you must first install reporting server components on the SQL Server cluster node that owns the shared cluster resources. After installing reporting server components on a first cluster node, run the setup program on all subsequent nodes in the cluster you want to be able to use the shared cluster resources.

The following procedure guides you through the process of installing a reporting server in a clustered environment.

To install the reporting server on a SQL Server cluster:

1. Log on to the cluster node computer that owns the shared cluster resources using an account that is a member of the local Administrators group. Also ensure your logon account is a member of the Microsoft SQL Server `sysadmin` role on the database server and reporting server.

Note

You do not need an Administrator account or SQL Server `sysadmin` account to run most Security Manager consoles or utilities *after* installation.

You must use an account that is a member of the Microsoft SQL Server `sysadmin` role on the database server to use the Access Configuration utility.

2. Close all open applications.
3. Run the setup program from the Security Manager installation kit.
4. Click the Production Setup tab and click **Begin Reporting Setup**.
5. Follow the instructions in the setup program until you reach the Finished window.

6. Click **Finish**.
7. Log on to another cluster node computer you want to enable to share Security Manager reporting server components using an account that is a member of the local Administrators group. Also ensure your logon account is a member of the Microsoft SQL Server `sysadmin` role on the database server and reporting server.
8. Close all open applications.
9. Run the setup program from the Security Manager installation kit.
10. Click the Production Setup tab and click **Begin Reporting Setup**.
11. On the Specify Reporting Server Database Instances window, specify the SQL Server Analysis Services, cube depot, and SQL Server Integration Services instances you want to use.
12. Click **Next**.
13. Follow the instructions in the setup program until you reach the Finished window.
14. Click **Finish**.
15. Repeat Steps 7 through 14 for each additional log archive server you want to send data to the reporting server.

For more information about SQL server clustering, see the Microsoft SQL Server documentation and the Microsoft SQL Server Web site at www.microsoft.com/sql.

Configuring the Reporting Cube SQL Job in a Clustered Environment

After installing Security Manager reporting server components on a SQL cluster, you must configure the account Microsoft SQL Server uses to run the `NetIQ_SM_SSI` job. In a clustered environment, the SQL Server Agent cannot run the job without additional permissions or modifications to the standard service account the agent uses.

You have several options for configuring the SQL Server Agent to be able to run the NetIQ_SM_SSI S job:

Enable delegation

If possible in your environment, you can use Active Directory native tools to enable delegation for the SQL Server Agent service account.

Use the Local System account

You can use the SQL Server Configuration Manager to change the SQL Server Agent to log on as Local System.

Use the Security Manager service account

You can use the SQL Server Configuration Manager to change the SQL Server Agent to log on using the overall Security Manager service account.

If you want to configure the SQL Server Agent to use the Security Manager service account, you must also change the NetIQ_SM_SSI S job itself to run as the Security Manager service account.

Note

Since each computing environment varies, NetIQ does not recommend one option over any other.

Appendix D

Installing Security Manager Components Silently

You can silently install Security Manager components by running the installation program from the command line using the following basic syntax:

```
msiexec /i setup.msi /quiet /!*v LogFile.txt OPTIONS
```

This command instructs the installation program to run without showing a user interface. However, you still need to supply all of the necessary *OPTIONS* information on the command line when installing silently. For more information about possible silent installation options, see “Installation Program Options” on page 183.

Warning

NetIQ recommends only advanced users who have experience with Microsoft Installer (MSI)-based applications install Security Manager components silently.

The following procedures describe how to use the silent installation capability to install a Security Manager configuration group and unmanaged Windows agents.

Before installing Security Manager components silently, be aware of the following considerations:

- The installation program does not validate any of the information you enter on the command line. Ensure you have entered the required information correctly before executing the command.
- If the installation program cannot install Security Manager, the installation program notifies the user only by logging the failure in the installation log. The installation program does not display any errors or warnings during the process. When running the Security Manager installation program silently, ensure logging is enabled.

To enable logging, include the option `/l *v LogFile.txt` in the command line, where *LogFile.txt* is the name of the text file where you want the installation program to log installation progress and any errors.

- NetIQ recommends you do not silently install Security Manager database server components or reporting server components. Instead, you should install the necessary databases using the user interface-based setup program. However, you need to install databases only one time per configuration group.
- See the following steps for information on installing database server components. For more information about installing reporting server components, see “Installing the Reporting Server” on page 101.
- You can use the silent installation procedure to install Security Manager components or upgrade previously installed Security Manager components using the `INSTALL_TYPE` option. If you want to upgrade Security Manager, you must specify all components currently installed on the local computer using the `ADDLOCAL` option.

- Ensure the computers on which you install Security Manager components, including the database server, have all the necessary prerequisites already installed. For more information about Security Manager prerequisites, see “Planning to Install Security Manager” on page 23.
- If you want to silently install a central computer, you must run the installation program from the complete installation kit. The installation program requires several specific files located in a standard location in the installation kit.

Note

When you silently install Security Manager components on a computer with Windows Server 2008 or Windows Vista installed, you may need to run the setup program using the built-in administrator account.

To run `Setup.msi` as the administrator, open the command-line interface using the `runas` command:

```
runas /user:administrator cmd
```

In the command-line interface, follow the installation instructions to install the components silently.

To silently install Security Manager components:

1. Log on to the computer you want to use as your database server using an account that is a member of the local Administrators group. Also ensure your logon account is a member of the Microsoft SQL Server `sysadmin` role on the database server and reporting server.
2. Close all open applications.
3. Run the setup program from the Security Manager installation kit.
4. Click the Production Setup tab and click **Begin Production Setup**.
5. Click **Run**.
6. On the Select Security Manager Components window, select **Database Server**.
7. Follow the instructions in the setup program until you reach the Finished window.
8. Click **Finish**.

9. After the setup program finishes installing database server components, log on to the computer on which you want to install one or more Security Manager components using an account that is a member of the local Administrators group. Also ensure your logon account is a member of the Microsoft SQL Server `sysadmin` role on the database server and reporting server.
10. Close all open applications.
11. Open a command-line interface.
12. In the command-line interface, navigate to the location of the Security Manager installation kit.
13. In the Security Manager installation kit, open the `INTEL` folder.
14. Enter the following command, including all applicable options:

```
msiexec /i Setup.msi /quiet /I *v LogFile.txt
CONFIDGROUP_NAME="ConfigGroup" CONFIDGROUP_ID="ConfigID"
CONFIDGROUP_PASSWORD="Password"
IS_SQLSERVER_SERVER="DatabaseServer"
LAS_INITIAL_VOLUME="LogArchive" LAS_SERVERNAME="LogArchiveServer"
LAS_DATASTORE_LOCATION="C:\LogArchivePath\"
INSTALLDIR="C:\Installation\" INSTALL_TYPE="InstallationType"
ADDLOCAL="ComponentsToInstall"
IS_NET_API_LOGON_USERNAME="Domain\ServiceAccount"
IS_NET_API_LOGON_PASSWORD="ServiceAccountPassword"
```

where *LogFile.txt*, *ConfigGroup*, *ConfigID*, *Password*, *DatabaseServer*, *LogArchive*, *LogArchiveServer*, *LogArchivePath*, *InstallationType*, *ComponentsToInstall*, *Domain*, *ServiceAccount*, and *ServiceAccountPassword* are the appropriate values for your configuration group.

For more information about installation program options, see “Installation Program Options” on page 183.

15. After the installation program finishes, verify the installation program successfully installed the selected Security Manager components. For more information about verifying a silent installation, see “Verifying Silent Installation” on page 192.
16. Close the command-line interface.

Installation Program Options

The following table defines all possible command line options used with the Security Manager installation program:

| Option Name | Description | Components |
|----------------------|--|-----------------------------------|
| CONFIGGROUP_NAME | Specifies the name of the configuration group you created when you installed your database server. | Central computer |
| CONFIGGROUP_ID | Specifies the globally unique identifier (GUID) of the configuration group you created when you installed your database server. You can obtain your configuration group's GUID by running the following query in SQL Management Studio on your database server: Configurati onselectbydatana meandcategory config, id Execute the query on the OnePoint database. Use the DataValue column value returned by the query as the CONFIGGROUP_ID value. | Central computer |
| CONFIGGROUP_PASSWORD | Specifies the password for the configuration group you created when you installed your database server. | Central computer |
| IS_SQLSERVER_SERVER | Specifies the name of your database server computer. | Central computer, user interfaces |
| LAS_INITIAL_VOLUME | Specifies the name of the initial log archive volume on the log archive server. | Log archive server |

| Option Name | Description | Components |
|------------------------|---|---|
| LAS_RESTRICT_PERMS | <p>Specifies whether you want to set restrictive access permissions on the log archive so that only members of the OnePointOp ConfigAdms and OnePointOp System groups can access the log archive.</p> <p>A value of true restricts log archive access. Do not include this option to leave access unrestricted.</p> | Log archive server |
| LAS_SERVERNAME | <p>Specifies the name of the computer you want to use as your log archive server.</p> | Central computer |
| LAS_DATASTORE_LOCATION | <p>Specifies the path where you want to install the log archive.</p> <p>Note: You cannot specify a log archive installation path name that includes spaces or special characters.</p> | Log archive server |
| INSTALLDIR | <p>Specifies the folder where you want to install Security Manager. If the specified folder does not exist, the installation program creates a folder with the specified path and name.</p> <p>Note: You cannot specify C:\Program Files\NetIQ\ as your installation folder. Security Manager uses this path by default for specific Security Manager components.</p> | Central computer, user interfaces, log archive server |

| Option Name | Description | Components |
|--------------|---|----------------|
| INSTALL_TYPE | <p>Specifies the type of Security Manager installation you want to perform, whether a new installation or an upgrade of existing Security Manager components. Possible values are <code>install</code> or <code>upgrade</code>.</p> <p>Note: You need to specify the installation type only if you want to upgrade an existing Security Manager installation. The default value of this property is <code>install</code> unless you specify <code>upgrade</code>.</p> | All components |

| Option Name | Description | Components |
|-------------|--|---|
| ADDLOCAL | <p>Specifies the Security Manager components you want to install, in a comma-separated list.</p> <p>The following items are possible values for this option:</p> <ul style="list-style-type: none"> • SecurityManager • Central Computer • Agent • CommonFiles_CC_UI • CommonFiles_UI • LogArchive • Control Center • DevConsole • WebConsole <p>You must start the ADDLOCAL list with SecurityManager. Specify additional components depending on what you want to install.</p> <p>Notes: If you want to install user interface components, you must include both CommonFiles_CC_UI and CommonFiles_UI in the list of options.</p> <p>If you want to upgrade Security Manager, you must specify all components currently installed in the ADDLOCAL list.</p> | Central computer, user interfaces, log archive server |
| | <p><i>If you want to install Security Manager central computer components</i>, specify the following options:</p> <p>SecurityManager, Agent, Central Computer, CommonFiles_CC_UI</p> | Central computer |

| Option Name | Description | Components |
|-------------------------------|---|---|
| | <p>If you want to install the Control Center and Development Console, specify the following options: SecurityManager, CommonFiles_CC_UI, CommonFiles_UI, Control Center, DevConsole</p> | User interfaces |
| | <p>If you want to install the Web Console (requires central computer), specify the following options: SecurityManager, Agent, Central Computer, CommonFiles_CC_UI, WebConsole</p> | Central computer, user interfaces (Web Console) |
| | <p>If you want to install log archive server components, specify the following options: SecurityManager, LogArchive</p> | Log archive server |
| | <p>If you want to install only the Control Center, specify the following options: SecurityManager, CommonFiles_CC_UI, CommonFiles_UI, Control Center</p> | User interfaces (Control Center) |
| IS_NET_API_LOGON_USER NAME | Specifies the name of the service account you used when you installed your database server, using the format <i>Domain\User</i> . | Central computer, log archive server |
| IS_NET_API_LOGON_PASS WORD | Specifies the password for the service account you used when you installed your database server. | Central computer, log archive server |

The following command is an example of the command line text you would need to input in order to install a Security Manager central computer silently:

```
msiexec /i Setup.msi /quiet /I*v test.txt CONFIGGROUP_NAME="test"  
CONFIGGROUP_ID="4F0180D9-2D47-4BA7-924F-4599B9C1447A"  
CONFIGGROUP_PASSWORD="testtest" IS_SQLSERVER_SERVER="sql server002"  
INSTALLDIR="C:\silentinstall\  
ADDLOCAL="SecurityManager, Agent, WebConsole, CommonFiles_CC_UI, Central Computer" IS_NET_API_LOGON_USERNAME="domain\bobr"  
IS_NET_API_LOGON_PASSWORD="*****"
```

Installing or Upgrading Unmanaged Agents Silently

In addition to main Security Manager components, you can silently install unmanaged Security Manager agents using the following procedure. You can also silently apply service packs or hotfixes to unmanaged agents.

Notes

- If the installation program cannot install or upgrade the unmanaged agent, the installation program notifies the user only by logging the failure in the installation log. The installation program does not display any errors or warnings during the process. When running the Security Manager installation program silently, ensure logging is enabled.
- You can use the silent installation procedure to install or upgrade only Security Manager 6.5, Security Manager 6.5 Service Pack 1, Security Manager 6.5.2, Security Manager 6.5.3, or Security Manager 6.5.4 unmanaged agents. Do not attempt to silently install or upgrade Security Manager 6.0 or Security Manager 5.6 unmanaged agents.
- Ensure the computers on which you install unmanaged Security Manager agents have all the necessary prerequisites already installed. For more information about Security Manager prerequisites, see “Planning to Install Security Manager” on page 23.

The `msiexec` command syntax for running a silent installation is as follows:

```
msiexec /i ManualAgent.msi /qn [/l LogFile.txt]
INSTALLDIR="C:\InstallDirectory\\"
SM_CENTRALCOMPUTER="Central Computer"
SM_CONFIGURATIONGROUP="ConfigGroup" [SM_SECUREPORT="PortNumber"]
```

The options are defined as follows:

| Option Name | Description |
|--|--|
| <i>/l LogFile.txt</i> | Specifies that the setup program log installation progress and any errors encountered during installation. If you use the <i>/l</i> option to enable logging, you must specify the path to the location where you want the setup program to save the log file as the value for the <i>LogFile</i> parameter. |
| <i>INSTALLDIR="InstallDirectory"</i> | Specifies the path and folder in which you want the setup program to install files. For 32-bit computers, the default is C:\Program Files\NetIQ Security Manager. For 64-bit computers, the default is C:\Program Files (x86)\NetIQ Security Manager. |
| <i>SM_CENTRALCOMPUTER="Central Computer"</i> | Specifies the name of the central computer to which you want the unmanaged Windows agent to connect. Note: If you are using the <i>/qn</i> option to silently run installation, this parameter is required. |
| <i>SM_CONFIGURATIONGROUP="ConfigGroup"</i> | Specifies the name of the configuration group to which the unmanaged Windows agent belongs. Note: If you are using the <i>/qn</i> option to silently run installation, this parameter is required. |
| <i>SM_SECUREPORT="PortNumber"</i> | Specifies the secured port through which you want the unmanaged Windows agent to communicate with the central computer. Default: 8270. |

To silently install an unmanaged agent to the \manual agent folder on the agent computer and assign the SMCCSERVER central computer in the Bi_g_Confi g configuration group to manage it, type:

```
msiexec /i ManualAgent.msi /qn INSTALLDIR="C:\manualagentdir"  
SM_CENTRALCOMPUTER="SMCCSERVER" SM_CONFIGURATINGGROUP="Big_Config"
```

If you are using the `/qn` option to silently run installation, you must specify values for the `SM_CENTRALCOMPUTER` and `SM_CONFIGURATINGGROUP` parameters. All other parameters are optional.

Note

When you silently install an unmanaged agent on a computer with Windows Server 2008 or Windows Vista installed, you may need to run the setup program using the built-in administrator account.

To run `ManualAgent.msi` as the administrator, open the command-line interface using the `runas` command:

```
runas /user:administrator cmd
```

In the command-line interface, follow the installation instructions to install the agent silently.

For more information about installing and configuring unmanaged agents, see “Installing and Configuring a Windows Agent Manually” on page 121.

To silently install or upgrade an unmanaged agent:

1. Log on to the unmanaged agent computer using an account that is a member of the local Administrators group.
2. Close all open applications.
3. Open a command-line interface.
4. *If you want to install an agent*, complete the following steps:
 - a. In the command-line interface, navigate to the location of the Security Manager installation kit.
 - b. In the Security Manager installation kit, navigate to the `Additional Setups/Manual Agent Installation` folder.
 - c. Enter the following command:

```
msiexec /i ManualAgent.msi /qn /l LogFile.txt  
INSTALLDIR="C:\InstallDirectory\  
SM_CENTRALCOMPUTER="Central Computer"  
SM_CONFIGURATINGGROUP="ConfigGroup"
```

where *LogFile.txt*, *InstallDirectory*, *Central Computer*, and *ConfigGroup* are the appropriate values for your configuration group.

5. **If you want to apply a service pack or hotfix to an existing agent**, complete the following steps:
 - a. In the command-line interface, navigate to the location of the Security Manager service pack or hotfix.
 - b. Enter the following command:

```
"Manual Agent SP1.msp" /quiet /l *v LogFile.txt
```

Where *LogFile.txt* is the name of the text file where you want the installation program to log installation progress and any errors.
6. After the installation program finishes, verify the installation program successfully installed the selected Security Manager components. For more information about verifying a silent installation, see "Verifying Silent Installation" on page 192.
7. Close the command-line interface.
8. Log on to the central computer as a member of the OnePointOp ConfigAdms group.
9. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
10. In the Tasks pane, click **Launch Agent Administrator**.
11. In the left pane, click **Unmanaged Agents**.
12. In the right pane, click **Authorize Unmanaged Agents**.
13. Select the unmanaged agent you want to authorize.
14. Click **OK**.
15. Select **Apply configuration changes now**.

16. Click **OK**.
17. Verify the selected central computer and click **OK**.
18. Click **Close**.

Verifying Silent Installation

Because the command-line installation process is silent, the installation program does not notify you of any errors encountered during the process. If you enter incorrect information for your installation environment and the installation program cannot install Security Manager, the installation program stops the process and does not display an error message.

If you want to verify that you successfully installed one or more Security Manager components, you can search for an event in the Application event log containing the status of the installation.

In addition, if you included the `/v` option when you ran the installer, you can navigate to the location of the log file and check that the installer completed successfully.

To verify silent installation of Security Manager components:

1. On the computer where you silently installed Security Manager components, open the Event Viewer located in the Control Panel.
2. Click **Application**.
3. Click the **Source** column to sort by event source.
4. Scroll down until you find one or more events with the source `msiexec` or `MsiInstaller`.
5. Right-click the first `msiexec` or `MsiInstaller` event and select **Properties**.
6. Use the down arrows to search through all `msiexec` or `MsiInstaller` events.
7. If you find an Information event with the Description `Successfully installed X`, the installation program installed Security Manager successfully.

If you find an Error event, the installation program could not install all Security Manager components.

8. Navigate to the log file created during the installation process.
9. Open the log file and search for logged failure messages that may indicate why the installation program could not successfully install Security Manager.

Appendix E

Upgrading Security Manager

The following procedures describe how to upgrade Security Manager to the current version. During this upgrade process, you will install new Security Manager components, as well as upgrade existing components. Ensure you review the planning information indicated in the procedures because Security Manager contains new components and new requirements for existing components.

This section documents how to upgrade a **production** installation of Security Manager.

You cannot upgrade a trial installation to a production installation. If you currently have a trial installation and want to move to a production installation, you must first uninstall the trial installation, then install the production installation. For more information about uninstalling Security Manager, see “Uninstalling Security Manager” on page 245. For more information about installing Security Manager, see “Installing Security Manager” on page 85.

When upgrading Security Manager, it is important to upgrade configuration groups and components in the proper order. Follow the steps in this section to upgrade each Security Manager component in a configuration group based on the number and type of configuration groups in your production implementation.

If you upgrade components out of order or do not upgrade all components, Security Manager may generate errors when upgraded components attempt to connect to previous version components.

You can use these procedures to upgrade any production installation of the following Security Manager versions to the latest version:

- Security Manager 6.0 Service Pack 4 (*agents only*)
- Security Manager 6.5
- Security Manager 6.5 Service Pack 1
- Security Manager 6.5.2
- Security Manager 6.5.3

Notes

- When you upgrade Security Manager components, the setup program automatically deletes any unused or obsolete files currently located on the local computer. However, the setup program updates but does not delete any Security Manager configuration files.
 - If you have customized your SQL environment prior to upgrading Security Manager components, the setup program may overwrite your customizations.
-

Upgrading Security Manager Overview

You can upgrade your Security Manager implementation by completing the following checklist:

| <input checked="" type="checkbox"/> | Steps | See Section | Page |
|-------------------------------------|---|--|-----------|
| <input type="checkbox"/> | 1. Review planning and system requirements. | "Planning to Roll Out Your Configuration Groups" "Installing and Configuring Security Manager in Firewall Environments" | 26 161 |
| <input type="checkbox"/> | 2. Prepare to upgrade existing components. | "Preparing to Upgrade" | 198 |

| <input checked="" type="checkbox"/> | Steps | See Section | Page |
|-------------------------------------|---|---|-------------------|
| <input type="checkbox"/> | 3. Upgrade each log archive server in the configuration group. | "Upgrading Log Archive Servers" | 199 |
| <input type="checkbox"/> | 4. Upgrade each central computer in the configuration group. Security Manager automatically upgrades your database server when you upgrade the first central computer in the configuration group. | "Upgrading Central Computers and the Database Server" | 201 |
| <input type="checkbox"/> | 5. Upgrade each user interface computer in the configuration group. | "Upgrading User Interface Computers" | 205 |
| <input type="checkbox"/> | 6. Upgrade agents. | "Upgrading Managed Windows Agents" "Upgrading Unmanaged Windows Agents" "Upgrading UNIX and iSeries Agents" | 206 210 211 |
| <input type="checkbox"/> | 7. Upgrade the reporting server for the configuration group. | "Upgrading the Reporting Server" | 212 |
| <input type="checkbox"/> | 8. After upgrading components, run the Configuration Wizard in each configuration group and ensure all applicable settings are correct. | "Configuring Security Manager" | 109 |
| <input type="checkbox"/> | 9. Upgrade saved Forensic Analysis query schedules and completed Forensic Analysis reports, if necessary. | "Upgrading Completed Forensic Analysis Reports and Query Schedules" | 213 |

| <input checked="" type="checkbox"/> | Steps | See Section | Page |
|-------------------------------------|--|--|------|
| <input type="checkbox"/> | 10. Configure redundancy, if necessary. | "Managing Central Computer Redundancy" | 215 |
| <input type="checkbox"/> | 11. After upgrading all components, upgrade installed modules on the central computer closest to the database server on the network. | "Upgrading Modules" | 216 |
| <input type="checkbox"/> | 12. Repeat Steps 2 through 11 for each configuration group. | | |
| <input type="checkbox"/> | 13. Verify upgrade success. | "Verifying Upgrade Success" | 217 |

Preparing to Upgrade

Before upgrading, you must properly configure your computer and stop certain services. The following procedure describes how to configure your computer and stop services locally.

Notes

- You should have at least 40% free log and data space available in your OnePoint database before upgrading.
 - You should have at least 700 MB of free space on your local computer before upgrading.
 - Instead of upgrading an agent on a database server, uninstall and then reinstall the agent.
-

To prepare for an upgrade:

1. Log on to the Development Console computer with a user account that is a member of the OnePointOp ConfigAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Development Console** from the NetIQ Security Manager program folder.
3. Expand **Security Manager Development Console > Configuration** in the left pane.
4. Ensure pending agent installation is configured by completing the following steps:
 - a. In the left pane, click **Central Computers**.
 - b. On the Action menu, click **Properties**.
 - c. On the Agent Installation tab, select the following:
 - **Do not install agents automatically. Add computers to the Pending Agents Installation list with a disapproved status.**
 - **Do not uninstall agents automatically. Add computers to the Pending Agents Uninstallation list with a disapproved status.**
 - d. Click **OK**.
5. Close the Development Console.
6. Log on to the database server using an account that is a member of the local Administrators group.
7. Back up the databases using your backup procedure.

Upgrading Log Archive Servers

When upgrading Security Manager, you should upgrade all log archive servers in the configuration group before upgrading all central computers.

To upgrade log archive servers:

1. Ensure you have your service account information and configuration group password available. You are prompted to provide this information during setup.
2. Log on to the log archive server you are upgrading using an account that is a member of the local Administrators group.
3. Close all open applications.
4. Run the setup program from the Security Manager installation kit.
5. Click the Production Setup tab and click **Verify Prerequisites**. Follow the instructions until you have installed all the necessary prerequisites. You can install some of the prerequisites using the Verify Prerequisites tool.
6. After you have finished verifying prerequisites, click **Finish**.
7. Click the Production Setup tab and click **Begin Production Setup**.
8. Click **Run**.
9. If you receive a second security warning, click **Run** again.
10. Click **Next**.
11. On the **License Agreement** window, select **I accept the terms in the license agreement** and click **Next**.
12. Follow the instructions in the setup program until you finish upgrading the log archive server.
13. Click **Finish**.
14. Repeat Steps 2 through 13 on each log archive server.
15. When you finish upgrading all log archive servers, ensure each log archive server is configured properly. For more information about configuring log archive server settings, see the *User Guide for NetIQ Security Manager*.

Upgrading Central Computers and the Database Server

Select your first central computer to upgrade. For the first central computer you upgrade, Security Manager will automatically update the following components:

- Database server
- Central computer
- User interfaces installed on the central computer

You cannot upgrade your database server directly. To upgrade the database server for a configuration group, upgrade a central computer, and Security Manager automatically upgrades the database server.

For additional central computers, Security Manager automatically updates the following components:

- Database server
- Central computer
- User interfaces installed on the central computer

Notes

- NetIQ recommends you upgrade the central computer closest on the network to the database server first, before upgrading central computers on more remote network subnets or that communicate with the database server using a connection with significant latency.
 - NetIQ recommends you back up all existing databases on your database server before upgrading.
 - NetIQ recommends you wait to upgrade modules on your central computers until you finish upgrading all Security Manager components, including user interface computers and log archive servers.
 - If you have customized your SQL environment prior to upgrading your Security Manager database server, the setup program may overwrite your customizations.
-

To upgrade central computers and the database server:

1. Ensure you have your service account information and configuration group password available. The setup program prompts you to provide this information.
2. Log on to the central computer you are upgrading using an account that is a member of the local Administrators group.
3. Close all open applications, including the Performance Monitoring tool.
4. Run the setup program from the Security Manager installation kit.
5. Click the Production Setup tab and click **Verify Prerequisites**.
6. Click **Run**.
7. *If you receive a second security warning*, click **Run** again.

8. Click **Next**.
9. Follow the instructions until you have verified all the necessary prerequisites for the Security Manager components you want to upgrade. You can install some of the required software using the Verify Prerequisites tool.
10. After you have finished verifying prerequisites, click **Finish**.
11. Click the Production Setup tab and click **Begin Production Setup**.
12. Click **Run**.
13. *If you receive a second security warning*, click **Run** again.
14. Click **Next**.
15. On the **License Agreement** window, select **I accept the terms in the license agreement** and click **Next**.
16. Follow the instructions in the setup program until you finish upgrading the central computer.

Note

Agent computers may display error messages and record error events to their event logs while you are upgrading the database server and central computers.

17. *If you want to add global domain groups to Security Manager OnePointOp groups*, log on with an account that is a member of the local Administrators group on the central computer and a member of the OnePointOp ConfigAdms group, and then complete the following steps:
 - a. Click **Launch Access Configuration**.
 - b. Add global domain groups to OnePointOp groups.
 - c. Click **Close**.

18. *If you want to upgrade all completed Forensic Analysis reports and query schedules*, complete the following steps:

- a. Click **Migrate Forensic Data**.
- b. Click **OK**.
- c. After the Forensic Analysis Migrator Tool finishes migrating your data, click **Summary Report** to review the status of your existing completed reports and schedules.
- d. When you finish reviewing the migration status, close the Summary Report window.
- e. In the Forensic Analysis Migrator Tool, click **OK**.

Notes

- You need to upgrade completed Forensic Analysis reports and query schedules on only the first central computer you upgrade in a particular configuration group.
 - You must upgrade your existing completed Forensic Analysis reports to be able to view the reports in the Security Manager Control Center. You must also upgrade existing Forensic Analysis query schedules to be able to run queries on their configured schedules.
 - If you upgrade a Forensic Analysis query schedule with an interval shorter than five minutes, the setup program automatically upgrades the query schedule to the minimum five-minute interval allowed.
 - The Forensic Analysis report and schedule upgrade process can take a significant amount of time. If you do not want to upgrade all reports and schedules when upgrading your central computer, you can also use the Forensic Analysis Migrator tool to upgrade at a later time. For more information about using the Migrator tool to upgrade completed Forensic Analysis reports and Forensic Analysis query schedules after upgrading Security Manager, see “Upgrading Completed Forensic Analysis Reports and Query Schedules” on page 213.
-

19. Click **Finish**.

20. Repeat Steps 2 through 19 on each central computer.
21. Log off of the central computer.

Upgrading User Interface Computers

After upgrading the core Security Manager components and agents, upgrade user interface computers, including user interface computers with agents. User interface computers have user interfaces installed, but are not central computers.

To upgrade user interface computers:

1. Log on to the user interface computer you are upgrading using an account that is a member of the local Administrators group.
2. Close all open applications.
3. Run the setup program from the Security Manager installation kit.
4. Click the Production Setup tab and click **Verify Prerequisites**.
5. Click **Run**.
6. *If you receive a second security warning*, click **Run** again.
7. Click **Next**.
8. Follow the instructions until you have verified all the necessary prerequisites for the Security Manager components you want to upgrade. You can install some of the required software using the Verify Prerequisites tool.
9. After you have finished verifying prerequisites, click **Finish**.
10. Click the Production Setup tab and click **Begin Production Setup**.
11. Click **Run**.
12. *If you receive a second security warning*, click **Run** again.
13. Click **Next**.

14. On the **License Agreement** window, select **I accept the terms in the license agreement** and click **Next**.
15. Follow the instructions in the setup program until you finish upgrading the user interface computer.
16. Click **Finish**.
17. Repeat Steps 2 through 16 on each user interface computer.

Note

If you upgrade a user interface computer that also has a Windows agent installed, the setup program automatically upgrades both the user interface components and the agent.

Upgrading Managed Windows Agents

Security Manager does not immediately upgrade managed agents on Windows computers. The central computer periodically scans the managed agent computers assigned to it. The first time it scans, the central computer identifies agents to upgrade.

If you approve the pending upgrades, the central computer upgrades managed agents the next time it performs a managed computer scan. By default, the central computer scans every day at 2:05 AM. However, you can also force Security Manager to immediately upgrade managed agents.

Notes

- If the managed agent computer is running the Compaq Insight Manager SNMP extension agent, stop the SNMP service and any dependent services before upgrading agents.
- Upgrading Windows agents may require you to restart the Windows agent computer.
- When you upgrade your managed agents, Security Manager retains all data those agents send to the central computer. Security Manager automatically migrates agent data from the existing message queues into its upgraded message queue structure.
- Windows agents in this version of Security Manager communicate with the central computer using more secure methods of authentication and encryption than previous (legacy) versions of the agent. Legacy and current agents are assigned different default ports, so that a Security Manager central computer can communicate with both types of agents if desired. For more information about default ports, see “Installing and Configuring Security Manager in Firewall Environments” on page 161.
- When you upgrade Security Manager, legacy agent communication is disabled by default unless you have one or more existing managed or unmanaged legacy agents deployed in your environment.
- If you do not upgrade all managed agents, any legacy agents in the configuration group continue to communicate with their respective central computers. However, if you configure a central computer to use FIPS-compliant algorithms for encryption, that central computer cannot communicate with legacy Windows agents (version 6.0 or earlier), UNIX agents, or iSeries agents.

For more information about configuring agent communication, see “Configuring Authenticated Communication” on page 141.

To upgrade automatically managed Windows agents immediately:

1. *If an agent computer is running any of the Security Manager user interfaces*, close all user interfaces running on the agent computer.
2. *If an agent computer is running the Performance Monitoring tool*, close the tool on the agent computer.
3. Log on to the central computer with a Windows account in the OnePointOp ConfigAdms group.
4. Start the **Development Console** from the NetIQ Security Manager program folder.
5. In the left pane, expand **Security Manager Development Console > Configuration**.
6. Scan managed computers by completing the following steps:
 - a. Click **Central Computers**.
 - b. On the Action menu, click **Scan All Managed Computers**.
 - c. Click **OK**.
 - d. On the Action menu, click **Refresh**.
7. Approve pending actions by completing the following steps:
 - a. In the left pane, expand **Pending Agents > Installation**.
 - b. On the Action menu, click **Refresh**.
 - c. On the Action menu, click **Approve all Pending Installations**.
 - d. *If Security Manager displays the Restart Warning window*, click **OK** to restart the managed agent computer.
8. Process approved actions by completing the following steps:
 - a. In the left pane, expand **Pending Agents > Installation**.
 - b. Select **Installation**.
 - c. On the Action menu, click **Install All Approved Agents Now**.

- d. Click **OK**.
 - e. On the Action menu, click **Refresh** until Security Manager finishes upgrading all agents.
9. Close the Development Console.

Upgrading Unmanaged Windows Agents

If you have manually installed unmanaged agents on Windows computers, run the setup program in the `Manual Agent Installation` folder of the Security Manager installation kit on the unmanaged agent computers. Run the setup program after you have upgraded the central computers and database server.

Notes

- NetIQ recommends upgrading all unmanaged agents to the latest version of Security Manager after you upgrade your other Security Manager components.
- You can upgrade unmanaged agents directly from Security Manager 6.0 Service Pack 4 to the latest version of Security Manager.
- Security Manager does not support authenticated communication between central computers and legacy agents or communication between central computers and legacy agents when FIPS-compliant security algorithms are enabled. Legacy agents are agents with Security Manager 6.0 installed. For more information about enabling authenticated communication or FIPS-compliant algorithms, see the *User Guide for NetIQ Security Manager*.
- When you upgrade Security Manager, legacy agent communication is disabled by default unless you have one or more existing managed or unmanaged legacy agents deployed in your environment.
- When you upgrade your unmanaged agents, Security Manager retains all data those agents send to the central computer. Security Manager automatically migrates agent data from the existing message queues into its upgraded message queue structure.
- When you upgrade an unmanaged agent on a computer with Windows Server 2008 or Windows Vista installed, you may need to run the setup program using the built-in administrator account.

To run `Manual Agent.msi` as the administrator, open the command-line interface using the `runas` command:

```
runas /user:administrator cmd
```

In the command-line interface, follow the installation instructions to upgrade the agent.

To upgrade an unmanaged agent:

1. Log on with an administrator account to the unmanaged agent computer.
2. Close all open applications, including the Performance Monitoring tool.
3. Run the `Manual Agent.msi` setup program from the `Additional Setups\Manual Agent Installation` folder of the installation kit.
4. Read the Welcome window, and then click **Next**.

Note

During the upgrade, the setup program allows you to maintain multiple configuration groups monitoring the unmanaged agent.

5. Follow the instructions in the `Manual Agent.msi` setup program until you have finished upgrading the unmanaged agent.

Upgrading UNIX and iSeries Agents

You must manually upgrade UNIX and iSeries agents. For more information about upgrading a UNIX agent, see the NetIQ UNIX Agent documentation, located in the NetIQ UNIX Agent installation kit. For more information about upgrading an iSeries agent, see the NetIQ Security Solutions for iSeries documentation, located in the NetIQ Security Solutions for iSeries installation kit.

Upgrading the Reporting Server

When upgrading Security Manager, upgrade the reporting server in the configuration group, if applicable, after upgrading all central computers and log archive servers. If your configuration group does not include a reporting server, do not complete the following task.

Notes

- Before running the setup program to upgrade your reporting server, note where the current reporting server components are installed.

Security Manager does not cache the location of the installed reporting components. When you upgrade, you must specify the locations of the reporting server components, as you would for a new installation. If you specify the existing server or instance for a component, the setup program proceeds with the upgrade.

However, if you specify a server or instance *other* than the existing component server or instance, the setup program installs a new version of the reporting component on that new server or instance.

- If you have customized your SQL environment prior to upgrading your Security Manager reporting server, the setup program may overwrite your customizations.
 - After upgrading the reporting server, NetIQ recommends you install any updated report modules available through AutoSync. For more information about installing modules using AutoSync, see the *User Guide for NetIQ Security Manager*.
-

To upgrade the reporting server:

1. Ensure you have your service account information and configuration group password available. The setup program prompts you to provide this information.
2. Log on to the reporting server you are upgrading using an account that is a member of the local Administrators group.
3. Close all open applications.
4. Run the setup program from the Security Manager installation kit.
5. Click the Production Setup tab and click **Begin Reporting Setup**.

6. Click **Run**.
7. *If you receive a second security warning*, click **Run** again.
8. Click **Next**.
9. On the **License Agreement** window, select **I accept the terms in the license agreement** and click **Next**.
10. Follow the instructions in the setup program until you finish upgrading the reporting server.
11. Click **Finish**.

Upgrading Completed Forensic Analysis Reports and Query Schedules

After upgrading to the current version of Security Manager, you must upgrade any completed Forensic Analysis reports and existing Forensic Analysis query schedules to continue to be able to view the reports in the Control Center or run queries on their configured schedules.

You can automatically upgrade all Forensic Analysis reports and schedules as part of the upgrade process by clicking **Migrate Forensic Data** when you finish upgrading the first central computer and associated database server in your configuration group. For more information about upgrading reports and schedules immediately after upgrading, see “Upgrading Central Computers and the Database Server” on page 201.

However, because the upgrade process can take a significant amount of time, depending on the number of completed reports and schedules, you may not want to upgrade immediately.

If you want to upgrade your completed Forensic Analysis reports and query schedules at a later date, you can run the Forensic Analysis Migrator tool to migrate the report data whenever you want. As the tool upgrades reports and schedules, you can review the status of the upgrade process using the `ForensicAnalysisMigrationStatus.xml` summary report the tool automatically creates.

To manually upgrade Forensic Analysis reports and query schedules after upgrading Security Manager:

1. Log on to the central computer where you want to upgrade reports and schedules using an account that is a member of the OnePointOp ConfigAdms group or the local Administrators group.

Note

You need to upgrade completed Forensic Analysis reports and query schedules on only the first central computer you upgrade in a particular configuration group.

2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **Forensic Analysis > Completed Reports**. Security Manager does not display any reports completed prior to upgrading Security Manager.
4. In the Navigation pane, click **Forensic Analysis > Scheduled Queries**. Security Manager does not display any scheduled queries created prior to upgrading Security Manager.
5. Navigate to *installation folder*\NetIQ Security Manager\NetIQ Security Manager Core, where *installation folder* is the location where you installed Security Manager.
6. Run NetIQ.SM.ForensicMigrationTool.exe.
7. Click **OK**.
8. After the Forensic Analysis Migrator Tool finishes migrating your data, click **Summary Report** to review the status of your existing completed reports and schedules.
9. When you finish reviewing the migration status, close the Summary Report window.
10. In the Forensic Analysis Migrator Tool, click **OK**.
11. In the Control Center, click **Refresh** on the View menu to view upgraded reports and scheduled queries.

12. *If you want to verify you have successfully upgraded completed reports and query schedules*, complete the following steps:
 - a. Navigate to Documents and Settings\All Users\Application Data\NetIQ\Security Manager\Log Files.
 - b. Open ForensicMigrationStatus.xml.
 - c. Review information on any reports or schedules the Migrator tool could not upgrade.
 - d. When finished reviewing the summary, close the ForensicMigrationStatus.xml window.
13. Close the Control Center.

Note

If you upgrade a Forensic Analysis query schedule with an interval shorter than five minutes, the setup program automatically upgrades the query schedule to the minimum five-minute interval allowed.

Managing Central Computer Redundancy

By default, Security Manager manages redundancy when a central computer fails. A check box on the Central Computers Global Settings Redundancy Policy tab determines whether this function is enabled. However, after completing an upgrade from a Security Manager installation that used multiple service accounts on central computers, this setting is turned off. In this case, you must manually configure redundancy. For more information about manually configuring central computer redundancy, see “Specifying Central Computers for Failover” on page 110.

Upgrading Modules

After upgrading all Security Manager components, NetIQ recommends you upgrade all installed modules.

Notes

- NetIQ recommends you update modules on the central computer closest on the network to the database server first.
 - The speed of the connection between the central computer on which you update modules and the database server can impact the amount of time required to update modules.
 - Many modules contain views. When you import an updated module, the Module Installer replaces the module views in the database. The Module Installer does not retain changes made to module views.
-

To upgrade Security Manager modules:

1. Log on to the central computer closest to the database server on the network using an account that is a member of the OnePointOp ConfigAdms or OnePointOp Operators groups.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Tasks pane, click **Global Tasks > Launch Module Installer**.
4. Select the modules that you want to update.
5. Click **Install**.
6. Confirm the modules you want to update and click **Continue**.
7. Click **Finish**.
8. Click **Close**.
9. Close the Security Manager Control Center.
10. Start the **Development Console** from the NetIQ Security Manager program folder.

11. In the left pane, expand **Security Manager Development Console > Configuration**.
12. Click **Central Computers**.
13. On the Action menu, click **Scan All Managed Computers**.
14. Click **OK**.
15. Close the Development Console.

Verifying Upgrade Success

After upgrading Security Manager central computers, user interface computers, and agents, you can verify the success of your upgrade by viewing the status of your central computers and agents in the Control Center.

To view the status of central computers and agents in the Control Center:

1. Log on to the Control Center computer using an account that is a member of the OnePointOp ConfigAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.
4. In the Navigation pane, expand **Infrastructure Components > Agents**.
5. Confirm that the status of all agent computers is **Running**.
6. Confirm that the version of all agent computers is the correct version of Security Manager.
7. Click **Central Computers**, and then confirm that the agent status of all central computers is **Running**.

8. *If agents or central computers are not running*, complete the following steps:
 - a. In the Navigation pane, expand **Security Views > Security Manager Self-monitoring > All Windows Events**.
 - b. Review the events written during the upgrade process.
9. Close the Control Center.

Obtaining New Modules and Module Updates

You can periodically check the NetIQ AutoSync Server for updated or new modules using the Module Installer. The **NetIQ AutoSync Server** is a Web server from which the Module Installer can download new and updated modules published between Security Manager product releases.

Note

You can run the Module Installer on a central computer or on a user interfaces computer. However, if you run the Module Installer from the installation kit, you must be on a central computer.

To run the Module Installer:

1. Log on to the central computer as a member of the OnePointOp ConfigAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Tasks pane, click **Global Tasks > Launch Module Installer**.
4. Specify whether to install modules from the NetIQ AutoSync Server or a location on your network. For more information about fields on a window, see the Help.

After you install or upgrade a module, ensure you configure it. For more information about configuring modules, see the module documentation.

Appendix F

Upgrading SQL Server Computers

Security Manager requires Microsoft SQL Server 2005 with Service Pack 3, Microsoft SQL Server 2008, or Microsoft SQL Server 2008 R2. However, if your database server or reporting server computers currently use SQL Server 2005, NetIQ recommends you upgrade your computers to use SQL Server 2008 or SQL Server 2008 R2.

You can upgrade Security Manager SQL databases by either upgrading SQL Server 2005 directly to SQL Server 2008 or SQL Server 2008 R2 on your existing servers or by installing SQL Server 2008 or SQL Server 2008 R2 on new servers and migrating all databases to the new computers.

Notes

- You can upgrade or migrate a database or reporting server at any time.
- You must have Security Manager 6.5.3 installed in order to install database and reporting server components on SQL Server 2008 computers. Upgrade to Security Manager 6.5.3 before upgrading or migrating databases.
- When migrating a database or reporting server, ensure the new SQL Server 2008 computer uses the same version of Security Manager as the existing SQL Server 2005 computer.

For more information about upgrading SQL Server, see the SQL Server documentation and the Microsoft support site at support.microsoft.com.

Upgrading the Database Server to SQL Server 2008

If you want to upgrade SQL Server 2005 to SQL Server 2008 or SQL Server 2008 R2 on your current database server, see the SQL Server documentation available at technet.microsoft.com for detailed steps and planning information.

Migrating Database Server Databases to a SQL Server 2008 Database Server

Instead of upgrading SQL Server 2005 on your existing database server, you can migrate your existing SQL Server 2005 databases to a computer with SQL Server 2008 or SQL Server 2008 R2 installed. Install SQL Server 2008 or SQL Server 2008 R2 on the new database server computer, then migrate your existing databases.

For more information about installing SQL Server, see “Installing Microsoft SQL Server” on page 33, the SQL Server documentation, and the SQL Server Web site at www.microsoft.com/sql.

You need to migrate the OnePoint, LogManagerConfiguration, and SecurityManagerCommon databases from the SQL Server 2005 database server to the new SQL Server 2008 or SQL Server 2008 R2 database server in order for Security Manager to function properly.

Notes

- If you want to upgrade to SQL Server 2008 or SQL Server 2008 R2 and have reporting server components installed in your environment, you must upgrade your database server first, followed by the reporting server.
 - Complete the steps in the following sections in one continuous process and in order. Make proper preparations ahead of time to have all account, passwords, data paths, and software available.
 - If you want to migrate your database server data as part of the Security Manager upgrade process, ensure you upgrade all Security Manager components *before* migrating databases.
 - NetIQ recommends creating Global groups in advance and mapping these Global groups to the local OnePointOp groups during the installation.
 - The new database server computer must be located in the same domain as the central computer.
-

Preparing the SQL Server 2008 Database Server

Before migrating any data to a new SQL Server 2008 computer, first install Security Manager database server components on the SQL Server 2008 computer.

To install Security Manager database components on a SQL Server 2008 server:

1. Log on to the SQL Server 2008 computer on which you want to install the Security Manager database components using an account that is a member of the local Administrators group. Also ensure your logon account is a member of the Microsoft SQL Server `sysadmin` role on the new database server.

Note

You do not need an Administrator account or SQL Server `sysadmin` account to run most Security Manager consoles or utilities *after* installation.

2. Ensure SQL Server 2008 is installed on the new database server computer.
3. Close all open applications.
4. Run the setup program from the Security Manager installation kit.
5. Click the Production Setup tab and click **Begin Production Setup**.
6. Click **Run**.
7. *If you receive a second security warning*, click **Run** again.
8. Click **Next**.
9. On the **License Agreement** window, select **I accept the terms in the license agreement** and click **Next**.
10. On the **Select Security Manager Components** window, click **Database Server** and select **This feature will be installed on local hard drive**.
11. Install all required prerequisites and click **Next**.
12. In the **Database Server Name** field, specify the name of the SQL Server 2008 computer as the database server name and click **Next**.
13. Follow the instructions in the setup program until you reach the Finished window.

Note

Ensure you specify the configuration group information you currently use for the existing database server.

14. Close the setup program.
15. Start **SQL Server Management Studio** in the Microsoft SQL Server 2008 program group.
16. In the Connect to Server window, select **Database Engine** as the server type.
17. Ensure the **Server name** field specifies the SQL Server 2008 server.
18. Click **Connect**.
19. Expand **Databases**.
20. Right-click **OnePoint** and select **Tasks > Detach**.
21. Click **OK**.
22. Right-click **LogManagerConfiguration** and select **Tasks > Detach**.
23. Click **OK**.
24. Right-click **SecurityManagerCommon** and select **Tasks > Detach**.
25. Click **OK**.
26. Log off of the new database server.

Detaching Security Manager Databases from the SQL Server 2005 Database Server

To migrate Security Manager databases to the new SQL Server 2008 database server, close all connections to the existing database server and then detach the OnePoint, LogManagerConfiguration, and SecurityManagerCommon databases.

To detach Security Manager databases from an existing SQL Server 2005 database server:

1. Close all open Security Manager user interfaces.
2. Log on to the central computer using an account that is a member of the local Administrators group.

3. Start **Services** in the Administrative Tools program group.
4. Right-click the **NetIQ Security Manager Core** service and select **Stop**.
5. Right-click the **NetIQ Security Manager** service and select **Stop**.
6. Close the Services tool.
7. Start **Component Services** in the Administrative Tools program group.
8. Expand **Component Services > Computers > My Computer > COM+ Applications**.
9. Right-click **OnePointActiveOpsDas** and select **Shut down**.
10. Close the Component Services tool.
11. Repeat steps Steps 2 through 10 on each central computer in the configuration group.
12. Log on to your SQL Server 2005 database server using an account that is a member of the SQL Server **sysadmin** role. For more information about SQL permissions, see the SQL Server Help.
13. Start **SQL Server Management Studio** in the Microsoft SQL Server 2005 program group.
14. In the Connect to Server window, select **Database Engine** as the server type.
15. Ensure the **Server name** field specifies the SQL Server 2005 database server.
16. Click **Connect**.
17. Expand **Databases**.
18. Right-click **OnePoint** and select **Properties**.
19. Click **Files**.
20. In the Database files window, note the locations of the **Eea_Data.mdf** and **Eea_Data.ldf** files for the OnePoint database.
21. Click **OK**.

22. Right-click **OnePoint** and select **Tasks > Detach**.
23. Click **OK**.
24. Right-click **LogManagerConfiguration** and select **Properties**.
25. Click **Files**.
26. In the Database files window, note the locations of the **LogManagerConfiguration.mdf** and **LogManagerConfiguration.ldf** files for the **LogManagerConfiguration** database.
27. Click **OK**.
28. Right-click **LogManagerConfiguration** and select **Tasks > Detach**.
29. Click **OK**.
30. Right-click **SecurityManagerCommon** and select **Properties**.
31. Click **Files**.
32. In the Database files window, note the locations of the **SecurityManagerCommon.mdf** and **SecurityManagerCommon.ldf** files for the **SecurityManagerCommon** database.
33. Click **OK**.
34. Right-click **SecurityManagerCommon** and select **Tasks > Detach**.
35. Click **OK**.
36. Close SQL Server Management Studio.
37. Navigate to the location of the your data (.mdf) and transaction log (.ldf) files.

38. From the current database server, connect to your new database server using an account that is a member of the SQL Server `sysadmin` role. For more information about SQL permissions, see the SQL Server Help.
39. Move or copy the following files to the new database server:
 - `EeaData.mdf`
 - `EeaLog.ldf`
 - `LogManagerConfiguration.mdf`
 - `LogManagerConfiguration.ldf`
 - `SecurityManagerCommon.mdf`
 - `SecurityManagerCommon.ldf`

Notes

- NetIQ recommends you copy the data and transaction files to the corresponding drive and folder on the new database server.
 - Delete the existing `.mdf` and `.ldf` files listed above on the new database server before copying the corresponding files from the SQL Server 2005 database server.
 - Because `.mdf` and `.ldf` files can be extremely large, transferring database files from one server to another can take a significant amount of time.
-

Attaching Security Manager Databases to the SQL Server 2008 Database Server

On the new SQL Server 2008 database server, attach the migrated databases using SQL Server Management Studio. After attaching each database, remove and re-add the existing Security Manager service account, providing `db_owner` permissions to the account.

To attach Security Manager databases to a new SQL Server 2008 database server:

1. Log on to your SQL Server 2008 database server using an account that is a member of the SQL Server `sysadmin` role. For more information about SQL permissions, see the SQL Server Help.
2. On the new database server, start **SQL Server Management Studio** in the Microsoft SQL Server 2008 program group.
3. In the Connect to Server window, select **Database Engine** as the server type.
4. Ensure the **Server name** field specifies the SQL Server 2008 server.
5. Click **Connect**.
6. In the Object Explorer, expand **Security > Logins**.
7. *If SQL Server Management Studio already lists the Security Manager service account*, complete the following steps:
 - a. Right-click the existing service account login and select **Delete**.
 - b. Click **OK**, then click **OK** to confirm.
8. Right-click **Logins** and select **New Login**.
9. Specify the Security Manager service account, either by entering the account information or clicking **Search**.
10. Click **Server Roles**.
11. Ensure the service account is a member of *only* the `public` server role.
12. Click **OK**.
13. In the Object Explorer, expand **Databases**.
14. Right-click **Databases** and select **Attach**.
15. Click **Add**.
16. Browse to the `Eea_Data.mdf` file you copied from the previous database server.
17. Select `Eea_Data.mdf` and click **OK**.

18. Verify the file names and file paths are correct for both the . mdf and . l df files.

Note

If you copied the . mdf and . l df files to a location on the new database server that differs from the original location on the SQL Server 2005 database server, you can modify the file path to reflect the correct location on the new server.

To modify the file path, click the ... button next to the file path for each file, select the location of the file on the new database server, and click **OK**.

19. Click **OK**, then click **OK** again.
20. On the View menu, click **Refresh**.
21. In the Object Explorer, expand **OnePoint > Security > Users**.
22. *If SQL Server Management Studio displays the Security Manager service account*, complete the following steps:
 - a. Right-click the existing service account and select **Delete**.
 - b. *If SQL Server Management Studio displays a warning*, click **Yes** to confirm.
 - c. Click **OK**.
23. Right-click **Users** and select **New User**.
24. In the **Login name** field, click the browse button.
25. Click **Browse**, select the Security Manager service account, and click **OK**.
26. Click **OK**.
27. Specify a user name for the service account.
28. In the **Database role membership** list, select **db_owner**.
29. Click **OK**.
30. Repeat Steps 14 through 29 for the LogManagerConfiguration and SecurityManagerCommon databases on the database server.

Configuring Migrated Databases on a SQL Server 2008 Server

After migrating databases from SQL Server 2005 to SQL Server 2008, configure the new database server to communicate with all central computers in the configuration group.

To configure migrated Security Manager databases on a new SQL Server 2008 server:

1. In the Object Explorer, expand **Databases > OnePoint > Tables**.
2. *If you want to rename your new database server to use the name of your existing database server*, skip to “Configuring Security Manager to Use the SQL Server 2008 Database Server” on page 230.
3. Right-click **dbo.Configuration** and select **Edit Top 200 Rows**.
4. Find the **DataName** entry **AlertURLBase** and replace the SQL Server computer name in the corresponding **DataValue** entry with the name of the new database server computer.

For example, if the current database server name is **HTSSM1**, the **DataValue** entry is **PropertySheet.asp?database=HTSSM1&target=%1&t=alert**. If the new database server name is **HTSERV2**, update the **DataValue** entry to **PropertySheet.asp?database=HTSERV2&target=%1&t=alert**.

5. Find the **DataName** entry **EventURLBase** and replace the SQL Server computer name in the corresponding **DataValue** entry with the name of the new database server computer.

For example, if the current database server name is **HTSSM1**, the **DataValue** entry is **PropertySheet.asp?database=HTSSM1&target=%1&t=event**. If the new database server name is **HTSERV2**, update the **DataValue** entry to **PropertySheet.asp?database=HTSERV2&target=%1&t=event**.

6. Close the **dbo.Configuration** table.
7. Right-click **dbo.Configuration** and select **Edit Top 200 Rows** a second time, then verify that SQL Server Management Studio saved all changes.
8. Close the **dbo.Configuration** table again.

9. *If the SQL Server Agent is not running*, complete the following steps:
 - a. Right-click **SQL Server Agent** and select **Start**.
 - b. Click **Yes** to confirm.
10. Log off of the new database server.

Configuring Security Manager to Use the SQL Server 2008 Database Server

After you migrate the databases and configure the SQL Server 2008 database server, configure all central computers and user interface computers in your environment to communicate with the new database server.

Warning

Configuring Security Manager to use the SQL Server 2008 database server requires you to edit several entries in the Windows Registry.

Be careful when editing your Windows Registry. If there is an error in your Registry, your computer may become nonfunctional. If an error occurs, you can restore the Registry to its state when you last successfully started your computer. For more information about editing the Registry, see the Help for the Windows Registry Editor.

To configure Security Manager components to use the SQL Server 2008 database server:

1. Log on to your central computer using an account that is a member of the local Administrators group and the OnePointOp ConfigAdms group.
2. Update the following registry entries using the Registry Editor:

```
HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\Security  
Manager\DasServer\Datasource = NewDatabaseServer
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\Security  
Manager\Configurations\Default\McsApplications\Operations  
Gui\Databases\Default = NewDatabaseServer
```

Where *NewDatabaseServer* is the name of the new database server computer.

3. *If the following registry entries exist on the central computer*, update the following entries using the Registry Editor:

```
HKEY_LOCAL_MACHINE\Software\NetIQ\Security  
Manager\Configurations\ConfigurationGroupName\Operations\Database  
= NewDatabaseServer
```

```
HKEY_LOCAL_MACHINE\Software\NetIQ\Security  
Manager\Databases\NewDatabaseServer
```

Where *NewDatabaseServer* is the name of the new database server computer and *ConfigurationGroupName* is the name of your configuration group.

4. *If you use a named instance for the database server*, update the following entry using the Registry Editor:

```
HKEY_LOCAL_MACHINE\Software\NetIQ\Security  
Manager\Databases\NewDatabaseServer\InstanceName
```

Where *NewDatabaseServer* is the name of the new database server computer and *InstanceName* is the name of your database instance.

5. Find and open the SMServi ceHost. exe. confi g file.
6. Update the following section of the SMServi ceHost. exe. confi g file:

```
<connecti onStri ngs>  
  <add name="OnePoi nt"  
    connecti onStri ng="Database=OnePoi nt; SERVER=<NewDatabaseServer>;  
    I ntegrated Securi ty=SSPI ;" provi derName="System. Data. Sql Cl i ent"  
    />  
  <add name="NetI QSMBBusi nessServi ces"  
    connecti onStri ng="Database=Securi tyManagerCommon; SERVER=<NewDat  
abaseServer>; I ntegrated Securi ty=SSPI ;"  
    provi derName="System. Data. Sql Cl i ent" />  
</connecti onStri ngs>
```

Where *<NewDatabaseServer>* is the name of the new database server computer.

7. Close the SMServi ceHost. exe. confi g file.
8. Log on to your SQL Server 2005 database server.
9. Start **SQL Server Configuration Manager** in the Microsoft SQL Server 2005 > Configuration Tools program group.

10. Use the SQL Server Configuration Manager tool to stop all SQL Server services.
11. Log on to your central computer.
12. Restart all Security Manager services on the central computer.
13. *If the following registry entry exists on the central computer*, delete the following entry using the Registry Editor:

```
HKEY_LOCAL_MACHINE\Software\NetIQ\Security  
Manager\Databases\PreviousDatabaseServer
```

Where *PreviousDatabaseServer* is the name of the SQL Server 2005 database server.

14. Start **Access Configuration** in the NetIQ Security Manager > Configuration program group.
15. In the left pane, click the OnePointOp System group.
16. Select any Member Name with a corresponding Valid value of No.
17. Click **Repair**.
18. Repeat Steps 15 through 17 for each OnePointOp group.
19. Log off of the central computer.
20. Repeat Steps 1 through 19 on each central computer in the configuration group.
21. Update the following registry entries on all existing user interface computers using the Registry Editor:

```
HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\Security  
Manager\DasServer\Datasource = NewDatabaseServer
```

```
HKEY_LOCAL_MACHINE\Software\NetIQ\Security  
Manager\Configurations\Default\McsApplications\Operations  
Gui\Databases\Default = NewDatabaseServer
```

Where *NewDatabaseServer* is the name of the new database server computer.

22. *If the following registry entry exists on one or more user interface computers*, delete the following entry using the Registry Editor:

```
HKEY_LOCAL_MACHINE\Software\NetIQ\Security  
Manager\Databases\PreviousDatabaseServer
```

Where *PreviousDatabaseServer* is the name of the SQL Server 2005 database server.

Migrating Reporting Data to a SQL Server 2008 Reporting Server

Rather than upgrading an existing reporting server to SQL Server 2008 or SQL Server 2008 R2, NetIQ recommends you install SQL Server 2008 or SQL Server 2008 R2 on a new computer, install the latest version of the Security Manager reporting components, and migrate all databases from the existing reporting server to the new SQL Server 2008 computer.

You need to migrate the SMCubeDepot database and SMReporting OLAP cube from the SQL Server 2005 reporting server to the new reporting server in order for Security Manager to function properly.

Notes

- If you want to upgrade to SQL Server 2008 or SQL Server 2008 R2 and have reporting server components installed in your environment, you must upgrade your database server first, followed by the reporting server.
 - Complete the steps in the following sections in one continuous process and in order. Make proper preparations ahead of time to have all account, passwords, data paths, and software available.
 - If you want to migrate your reporting server data as part of the Security Manager upgrade process, ensure you upgrade all Security Manager components *before* migrating the reporting databases.
 - NetIQ recommends creating Global groups in advance and mapping these Global groups to the local OnePointOp groups during the installation.
 - The new reporting server computer must be located in the same domain as the central computer.
-

For more information about installing SQL Server, see “Installing Microsoft SQL Server” on page 33, the SQL Server documentation, and the SQL Server Web site at www.microsoft.com/sql.

Preparing Security Manager to Migrate Reporting Components to the SQL Server 2008 Reporting Server

To migrate Security Manager reporting components to a new SQL Server 2008 or SQL Server 2008 R2 reporting server, first stop the log archive server from uploading more data to the cube depot.

To prepare Security Manager for migrating reporting components:

1. Before upgrading your reporting server, first upgrade your database server to use SQL Server 2008 or SQL Server 2008 R2 or migrate your database server databases to a server using SQL Server 2008 or SQL Server 2008 R2.

For more information about upgrading your database server, see “Upgrading the Database Server to SQL Server 2008” on page 220. For more information about migrating your databases, see “Migrating Database Server Databases to a SQL Server 2008 Database Server” on page 220.

2. On a server with SQL Server 2008 installed, install Security Manager reporting components. When prompted by the setup program, specify the name of the upgraded database server. Specify the new reporting server for the SQL Server Analysis Services instance, SQL Server Integration Services instance, and Cube Depot. For more information about installing the reporting server, see “Installing the Reporting Server” on page 101.
3. Log off of the new reporting server.
4. Log on to the log archive server using an account that is a member of the OnePointOp ConfigAdms group.
5. Start **Log Archive Configuration** in the NetIQ Security Manager > Configuration program group.
6. Click **Log Archive Server Settings**.
7. In the **Enable Summarized Data Upload** field, specify **False**.

8. Click **Apply**.
9. Click **Yes**.
10. Click **Close**.
11. Click **Yes** on the confirmation message to restart the NetIQ Security Manager Log Archive service.

Note

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

12. Click **Yes** to exit the wizard.
13. Log off of the log archive server.

Backing Up the SQL Server 2005 Reporting Cube

After preparing Security Manager, back up the existing SQL Server 2005 reporting cube and copy the cube backup file to the new reporting server computer.

To back up the reporting cube on an existing SQL Server 2005 reporting server:

1. Log on to your SQL Server 2005 reporting server using an account that is a member of the SQL Server `sysadmin` role. For more information about SQL permissions, see the SQL Server Help.
2. *If you previously stopped all SQL Server services on the reporting server*, use the SQL Server Configuration Manager to start all services.
3. Start **SQL Server Management Studio** in the Microsoft SQL Server 2005 program group.
4. In the Connect to Server window, select **Database Engine** as the server type.
5. Ensure the **Server name** field specifies the SQL Server 2005 reporting server.
6. Click **Connect**.
7. Expand **SQL Server Agent > Jobs**.

8. Right-click `NetIQ_SM_SIS` and select **Disable**.
9. Click **Close**.
10. Click **Connect > Analysis Services**.
11. Ensure the **Server name** field specifies the SQL Server 2005 reporting server.
12. Click **Connect**.
13. Expand **Databases**.
14. Right-click **SMReporting** and select **Back Up**.
15. Click **Browse** and note the location where SQL Server Management Studio stores the backup file.
16. *If you want to store backup files in the default location*, click **Cancel**.
17. *If you want to store backup files in a different location*, specify the full path to the new location in the **Selected path** field, then click **OK**.
18. Click **OK**.
19. From the SQL Server 2005 reporting server, connect to the SQL Server 2008 reporting server using an account that is a member of the SQL Server `sysadmin` role. For more information about SQL permissions, see the SQL Server Help.
20. Move or copy the `SMReporting.abf` file to the new reporting server.

Restoring the Reporting Cube on the SQL Server 2008 Reporting Server

To migrate the reporting cube to the SQL Server 2008 reporting server, restore the SQL Server 2005 cube using SQL Server Management Studio. After restoring the cube, browse the cube data and note the number of events in the cube.

To restore the reporting cube on a new SQL Server 2008 reporting server:

1. Log on to your SQL Server 2008 reporting server using an account that is a member of the SQL Server `sysadmin` role. For more information about SQL permissions, see the SQL Server Help.
2. On the new reporting server, start **SQL Server Management Studio** in the Microsoft SQL Server 2008 program group.
3. In the Connect to Server window, select **Analysis Services** as the server type.
4. Ensure the **Server name** field specifies the SQL Server 2008 server.
5. Click **Connect**.
6. Right-click **Databases** and select **Restore**.
7. In the **Backup file** field, click **Browse**.
8. Navigate to the location of the backup file and select `SMReporting.abf`.
9. Click **OK**.
10. Click the **Restore database** field and select **SMReporting**.
11. Select **Allow database overwrite**.
12. Click **OK**.
13. Expand **Databases > SMReporting > Cubes > LogArchive**.
14. Right-click **LogArchive** and select **Browse**.
15. In the Measure Group pane, expand **Measures > Measures**.
16. Drag and drop **Count** to the **Drop Totals or Detail Fields Here** pane.
17. Note the number of events in the reporting cube.

Configuring Roles for the SQL Server 2008 Reporting Cube

After restoring the reporting cube, configure the `CubeAdmin` role on the SQL Server 2008 reporting server.

To configure the **CubeAdmin** role:

1. In the Object Explorer, expand **SMReporting > Roles**.
2. Right-click **CubeAdmin** and select **Properties**.
3. Click **Membership**.
4. In the **Specify the users and groups for this role** window, select the existing SID and click **Remove**.
5. Click **Add**.
6. Click **Advanced**.
7. Click **Object Types** and select **Groups**, then click **OK**.
8. Click **Find Now**.
9. Select **SMReportingDBAdmin** and click **OK**.
10. Click **OK**, then click **OK** again.

Backing Up the SQL Server 2005 Cube Depot

After backing up and restoring the reporting cube, back up the **SMCubeDepot** database on the SQL Server 2005 reporting server and copy the cube depot backup file to the new reporting server computer.

To back up the **SMCubeDepot** database on an existing SQL Server 2005 reporting server:

1. Log back on to the SQL Server 2005 reporting server.
2. In SQL Server Management Studio, click **Connect > Database Engine**.
3. Ensure the **Server name** field specifies the SQL Server 2005 server.
4. Click **Connect**.
5. Expand **Databases**.
6. Right-click **SMCubeDepot** and select **Tasks > Back Up**.

7. In the **Destination** field, note the location where SQL Server Management Studio stores the backup file.
8. Click **OK**, then click **OK** again.
9. From the SQL Server 2005 reporting server, connect to the SQL Server 2008 reporting server using an account that is a member of the SQL Server `sysadmin` role. For more information about SQL permissions, see the SQL Server Help.
10. Move or copy the `SMCubeDepot.bak` file to the new reporting server.

Restoring the Cube Depot on the SQL Server 2008 Reporting Server

To migrate the `SMCubeDepot` database to the SQL Server 2008 reporting server, restore the SQL Server 2005 database using SQL Server Management Studio.

To restore the `SMCubeDepot` database on a new SQL Server 2008 reporting server:

1. Log back on to the SQL Server 2008 reporting server.
2. In SQL Server Management Studio, click **Connect > Database Engine**.
3. Ensure the **Server name** field specifies the SQL Server 2008 server.
4. Click **Connect**.
5. Right-click **Databases** and select **Restore Database**.
6. Click the **To database** field and select `SMCubeDepot`.
7. Select **From device**.
8. Click the browse button and click **Add**.
9. Navigate to the location of the backup file and select `SMCubeDepot.bak`.
10. Click **OK**, then click **OK** again.
11. Under **Select the backup sets to restore**, select **Restore** for the `SMCubeDepot` backup set.

12. Click **Options** and select **Overwrite the existing database (WITH REPLACE)**.
13. Click **OK**.
14. Click **OK** when finished.

Note

If SQL Server Management Studio displays an error when you restore the SMCubeDepot database, click **OK**, then click **Cancel**. Use SQL Server Management Studio to detach and then re-attach the existing SMCubeDepot database and then try to restore the backed-up SQL Server 2005 database.

Configuring the SQL Server 2008 Cube Depot

After restoring the SMCubeDepot database to the SQL Server 2008 reporting server, configure the cube depot to receive and process uploaded log archive data.

To configure the cube depot to receive and process data:

1. In the Object Explorer, expand **Databases > SMCubeDepot**.
2. Right-click **SMCubeDepot** and select **Properties**.
3. Click **Options**.
4. Click **Compatibility level** and select **SQL Server 2008 (100)**.
5. Click **OK**.
6. Under the SQL Server Analysis Services instance, expand **Databases > SMReporting > Data Sources**.
7. Right-click **SMCubeDepot** and select **Properties**.
8. Click **Connection String**.
9. Click the browse button.
10. In the **Server name** field, select or specify the name of the new server where you migrated the SMCubeDepot database.
11. Click **OK**, then click **OK** again.

Configuring Security Manager to Use the SQL Server 2008 Reporting Server

After you migrate the reporting cube and cube depot and configure the SQL Server 2008 reporting server, configure all log archives you want to send data to the reporting server and restart the NetIQ Security Manager Log Archive service.

To configure all log archives to send data to the SQL Server 2008 reporting server:

1. Log back on to the log archive server using an account that is a member of the OnePointOp CnfgAdms group.
2. Start **Log Archive Configuration** in the NetIQ Security Manager > Configuration program group.
3. Click **Log Archive Server Settings**.
4. In the **Reporting Server Name** field, specify the name of the SQL Server 2008 server where you migrated the SMCubeDepot database.
5. In the **Enable Summarized Data Upload** field, specify **True**.
6. Click **Apply**.
7. Click **Yes**.
8. Click **Close**.
9. Click **Yes** on the confirmation message to restart the NetIQ Security Manager Log Archive service.

Note

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

10. Click **Yes** to exit the wizard.
11. Log off of the log archive server.
12. Repeat Steps 1 through 19 on each log archive server you want to send data to the SQL Server 2008 reporting server.

Verifying the Status of the SQL Server 2008 Reporting Server

When you finish migrating the reporting cube and cube depot and configuring both the reporting server and log archives, run the `NetIQ_SM_SSI` S job and browse the reporting cube to ensure the cube depot is processing data.

To verify the status of the migrated cube and cube depot on a SQL Server 2008 reporting server.

1. Log back on to the SQL Server 2008 reporting server.
2. Connect to the Database Engine.
3. *If the SQL Server Agent is not running*, complete the following steps:
 - a. Right-click **SQL Server Agent** and select **Start**.
 - b. Click **Yes** to confirm.
4. Expand **SQL Server Agent > Jobs**.
5. *If the NetIQ_SM_SSI job is disabled*, complete the following steps:
 - a. Right-click **NetIQ_SM_SSI** and select **Enable**.
 - b. Click **Close**.
6. Right-click **NetIQ_SM_SSI** and select **Start Job at Step**.
7. When the job finishes processing data, click **Close**.
8. Connect to the SQL Server Analysis Services instance.
9. Expand **Databases > SMReporting > Cubes > LogArchive**.
10. Right-click **LogArchive** and select **Browse**.
11. In the Measure Group pane, expand **Measures > Measures**.

12. Drag and drop **Count** to the **Drop Totals or Detail Fields Here** pane.

Note

In most environments, the number of events in the cube is now higher than when previously checked. If the number of events increases, the reporting server is successfully receiving and processing log archive data.

13. Close SQL Server Management Studio.

Appendix G

Uninstalling Security Manager

If necessary, you can uninstall Security Manager by completing the procedures in the following sections. These procedures completely remove a Security Manager configuration group from your enterprise, and ensure you do not leave Windows agents on monitored computers. Leaving Windows agents on monitored computers may require you to manually delete the Windows agents from those computers.

Uninstalling Security Manager Overview

You can uninstall your Security Manager implementation by completing the following checklist:

| <input checked="" type="checkbox"/> | Steps | See Section |
|-------------------------------------|---|--|
| <input type="checkbox"/> | 1. Remove all agents on monitored computers. | <ul style="list-style-type: none">• For more information about uninstalling Windows agents, see “Uninstall Windows Agents” on page 247.• For more information about uninstalling UNIX agents, see the NetIQ UNIX Agent documentation.• For more information about uninstalling iSeries agents, see the NetIQ Security Solutions for iSeries documentation. |
| <input type="checkbox"/> | 2. Remove Security Manager components from your computers. | “Uninstall Security Manager Components” on page 251 |
| <input type="checkbox"/> | 3. Remove Security Manager reporting server components from your computers. | “Uninstall Reporting Server Components” on page 252 |
| <input type="checkbox"/> | 4. Remove the Security Manager databases. | “Uninstall the Databases” on page 253 |
| <input type="checkbox"/> | 5. Remove the log archives. | “Uninstall the Log Archives” on page 253 |

Uninstall Windows Agents

To ensure you remove Security Manager agents from the monitored Windows computers in your enterprise, uninstall all managed and unmanaged agents from computers assigned to each central computer.

The steps in this section refer to uninstalling agents only from Windows computers. For information about uninstalling agents from UNIX computers, see the NetIQ UNIX Agent documentation, available in the NetIQ UNIX Agent installation kit. For information about uninstalling agents from iSeries servers, see the NetIQ Security Solutions for iSeries documentation.

Notes

- When you uninstall Security Manager components from a central computer, you automatically uninstall the managed agent installed on the central computer. You do not need to uninstall the managed agent on the central computer itself prior to uninstalling Security Manager components.
 - If you remove agents, Security Manager no longer collects data, evaluates rules, or stores information in the databases for those computers.
 - If you want to remove a single agent from your configuration, and do not want to uninstall all Security Manager components from your environment, see the *User Guide for NetIQ Security Manager*.
 - If you want to uninstall an agent, ensure you close all Microsoft Management Consoles and snap-ins, including Event Viewer, on the agent computer before uninstalling.
-

Uninstalling Managed Agents

Perform the following procedure to remove all managed agents from Windows computers in a configuration group, prior to removing Security Manager and its databases.

Warning

If multiple configuration groups monitor an agent and you delete the agent when removing one of the configuration groups, the agent will no longer be available to the other configuration groups.

To uninstall all managed agents in a configuration group:

1. Log on to a central computer as a member of the OnePointOp ConfigAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.
4. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.
5. In the left pane, click **Agent Summary**.
6. In the right pane, click **Agent Summary View**.
7. Select all managed agents.
8. Click **Uninstall > Uninstall Now**.
9. Click **Yes**.
10. Click **Delete**.
11. Click **Yes**.
12. Click **Apply**.
13. Click **Close**.

14. Select **Apply configuration changes now**.
15. Click **OK**.
16. Verify the selected central computer and click **OK**.
17. Click **Close**.
18. Repeat Steps 1 through 17 on each central computer.

Uninstalling Unmanaged Agents from All Configuration Groups

The following procedure removes all unmanaged Windows agents associated with a configuration group from your enterprise, prior to removing Security Manager and its databases.

Warning

If multiple configuration groups monitor an unmanaged agent you uninstall, the unmanaged agent will no longer be available to the other configuration groups. To keep the unmanaged agent available to other configuration groups, do not uninstall the unmanaged agent. Remove the configuration group instead. For more information about removing a configuration group, see “Removing a Configuration Group that Monitors an Unmanaged Agent” on page 251.

To uninstall all unmanaged agents in all configuration groups:

1. Log on to an unmanaged agent computer as a local administrator.
2. Close all open applications.
3. Run **Add or Remove Programs** from the Control Panel.
4. Select **NetIQ Security Manager Agent**.
5. Click **Remove**.
6. Click **Yes**.
7. Follow the instructions until the unmanaged agent is removed.
8. Close the Add or Remove Programs window.

9. Log off of the unmanaged agent computer.
10. Repeat Steps 1 through 9 for each unmanaged agent you want to uninstall.
11. Log on to a central computer as a member of the OnePointOp ConfigAdms group. For more information about groups and permissions, see “Understanding Requirements and Permissions” on page 24.
12. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
13. In the Navigation pane, click **All Folders**.
14. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.
15. In the left pane, click **Agent Summary**.
16. In the right pane, click **Agent Summary View**.
17. Select all unmanaged agents.
18. Click **Uninstall > Pending**.
19. Click **Yes**.
20. Click **Apply**.
21. Click **Close**.
22. Select **Apply configuration changes now**.
23. Click **OK**.
24. Verify the selected central computer and click **OK**.
25. In the left pane, click **Agent Summary**.
26. In the right pane, click **Agent Summary View**.
27. Select **Show Hidden Computers**.
28. Select all unmanaged agents listed.
29. Click **Delete**.

30. Click **Yes**.
31. Click **Close**.
32. Select **Apply configuration changes now**.
33. Click **OK**.
34. Verify the selected central computer and click **OK**.
35. Click **Close**.

Removing a Configuration Group that Monitors an Unmanaged Agent

If you want a configuration group to stop monitoring an unmanaged agent that is monitored by multiple configuration groups, you can remove the configuration group.

To remove a configuration group:

1. Log on to an unmanaged agent computer as a local administrator.
2. Start the **Configure Multiple Configuration Groups** utility in the NetIQ Security Manager > Configuration Utilities program group.
3. Select **Remove this agent from a configuration group**.
4. Select the configuration group name you want to remove.
5. Click **OK**, and then click **OK**.

Uninstall Security Manager Components

After uninstalling all agents from your monitored computers, you can remove Security Manager components from your enterprise. This procedure must be performed on every computer where a Security Manager component was installed, typically the database server, log archive server, reporting server, central computer, and user interface computers.

To uninstall Security Manager components on each computer with Security Manager components installed:

1. Log on with an administrator account to a computer where you installed a component.
2. Close all open applications.
3. *If the Alert Sentry is running*, right-click the Alert Sentry icon in the system tray, select **Exit** on the menu, and then click **OK**.
4. Open the Control Panel and select **Add or Remove Programs**.
5. Select **NetIQ Security Manager**.
6. Click **Remove**.
7. Restart the computer.

Uninstall Reporting Server Components

After uninstalling all Security Manager components, you can remove reporting server components from your reporting server computer.

To uninstall reporting server components on the reporting server computer:

1. Log on with an administrator account to a computer where you installed reporting server.
2. Close all open applications.
3. *If the Alert Sentry is running*, right-click the Alert Sentry icon in the system tray, select **Exit** on the menu, and then click **OK**.
4. Open the Control Panel and select **Add or Remove Programs**.
5. Select **NetIQ Security Manager Reporting**.

6. Click **Remove**.
7. Restart the computer.

Note

If you installed your Security Manager reporting server on a Microsoft SQL Server cluster, you must uninstall reporting server components from each cluster node computer.

Uninstall the Databases

Completely removing Security Manager from your enterprise requires removing the Security Manager databases and OnePoint jobs from the database server and any reporting servers.

The setup program does not automatically remove the databases or OnePoint jobs. Use the Microsoft SQL Server administrator tools to remove the databases and jobs from the database server and reporting server. For more information about removing databases, see the Microsoft SQL Server documentation.

Warning

If you uninstall Security Manager and want to keep the data in the databases, disable or delete the OnePoint grooming jobs. If you do not disable or delete the OnePoint jobs, they will continue to groom data from the databases.

Uninstall the Log Archives

Completely removing Security Manager from your enterprise requires removing the Security Manager log archives from any log archive servers.

The setup program does not automatically remove the log archive data. If you want to remove the log archive data, you can delete the following folders from your log archive servers:

- C: \NetIQSMLogArchive
- *installation folder*\NetIQ Security Manager\NetIQ Log Archive, where *installation folder* is the location where you installed Security Manager