User Guide

NetIQ Agent Manager™

May 2013

NetIQ Agent 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.

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

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

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

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

Contents

About This Book and the Library 7
About NetIQ Corporation 9

1 Introduction 11

1.1 What Is Agent Manager? 11
1.2 How Agent Manager Works 11
1.2.1 Understanding Product Components 11
1.2.2 Understanding the Architecture 12
1.2.3 Understanding Windows Component Communication 13
1.2.4 Understanding Windows Agent Communication Security 14
1.2.5 Understanding Self-Scaling Windows Operations 14
1.2.6 Understanding Supported Windows Platforms 15
1.2.7 Understanding Supported Data Formats 15
1.2.8 Managing UNIX and iSeries Agents 15
1.3 Understanding Requirements and Permissions 16
1.3.1 Agent Manager Groups 16

2 Understanding the Agent Manager Console 17

2.1 Agent Manager Console Permissions Requirements. 17
2.2 Agent Manager Console 17
2.2.1 Data Collection Policy Window 18
2.2.2 Search Results Window. 18
2.3 Configuration Window 18

3 Understanding Data Collection Policies 19

3.1 Data Collection Policy Example 19
3.2 Data Collection Policy Security Knowledge 19

4 Managing and Analyzing Logs 21

4.1 What Are Data Collection Rules?. 21
4.2 Understanding Data Collection Rules 22
4.3 Understanding Data Providers 22
4.3.1 Windows Event Logs 22
4.3.2 Application Logs 23
4.4 Working with Data Providers 23
4.4.1 Creating a Data Provider 23
4.4.2 Creating a Data Provider for a Generic Single-line Text Log 24
4.5 Working with Data Collection Rules 24
4.5.1 Finding a Data Collection Rule 24
4.5.2 Reviewing Previous Rule Search Results 25
4.5.3 Forcing Data Collection Rule Changes 25

5 Monitoring Workstations 27

6 Administering Agents 29

6.1 Understanding Managed and Unmanaged Windows Agents 29
6.2 Understanding Discovery and Managed Windows Agent Deployment 30
6.2.1 Deploying a Managed Windows Agent 30
6.2.2 Deploying Multiple Managed Windows Agents 31
6.3 Understanding Unmanaged Windows Agent Installation 33
6.4 Scanning Managed Computers 33
6.5 Scanning a Single Managed Computer 34
6.6 Configuring Central Computer Properties 34
6.7 Configuring Agent Properties 35
6.8 Handling Pending Installations 35
6.8.1 Approving Pending Installations 36
6.8.2 Disapproving Pending Installations 37
6.8.3 Verifying Windows Agent Installation 38
6.9 Viewing Agents 38
6.9.1 Viewing All Agents 39
6.9.2 Viewing the Computers Assigned to a central computer 39
6.9.3 Changing Which central computer Manages an Agent 39
6.9.4 Changing the Name or Domain of a Monitored Computer 40
6.10 Disabling Communication from Computers 41
6.11 Viewing Hidden Computers 41
6.12 Uninstalling Windows Agents 41
6.12.1 Uninstalling Managed Windows Agents Using the Agent Administrator 42
6.12.2 Uninstalling Unmanaged Windows Agents 42
6.13 Configuring iSeries Agent Deployment 43
6.14 Configuring UNIX Agent Deployment 44

7 Understanding Device Groups 45

7.1 Built-in Device Groups 45
7.2 Device Group Membership 45
7.3 Understanding Device Grouping Criteria 46
7.4 Working with Device Groups 46
7.4.1 Associating a Device Group with a Data Collection Policy 46
7.5 Understanding Device Attribute Definitions 47
7.5.1 Predefined Device Attribute Definitions 47
7.5.2 Custom Device Attribute Definitions 47

8 Configuring Agent Manager 49

8.1 Using the Configuration Wizard 49
8.2 Configuring Message Buffering 49
8.3 Configuring Global Settings 50
8.3.1 Configuring Communication Ports 50
8.3.2 Configuring General Agent Settings 51
8.4 Configuring Primary and Backup central computers 52
8.5 Changing Service Account Passwords 53
8.6 Modifying Agent Manager OnePointOp Group Membership 53

A Understanding Text String Pattern Matching 55

A.1 Wildcard Characters 55
A.2 Regular Expressions 56

A.3 Boolean Regular Expressions 57

B Configuring Authenticated Communication 59

B.1 Understanding Default Agent Manager Communication 59
B.2 Understanding Authenticated Communication 60
B.3 Implementing Authenticated Communication 60
B.3.1 Certificate Requirements 61
B.3.2 Issuing and Installing Agent Authentication Certificates 62
B.3.3 Issuing and Installing central computer Authentication Certificates 63
B.3.4 Enabling Agent Authentication 64
B.3.5 Enabling central computer Authentication 64
B.3.6 Customizing Certificate Usage 65
B.3.7 Verifying Authenticated Communication 67
B.3.8 Troubleshooting Authentication Problems 68
B.4 Using Agent Manager with FIPS-Compliant Security Algorithms Enabled 70

About This Book and the Library

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

Intended Audience

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

Other Information in the Library

The library provides the following information resources:

Installation Guide

Provides detailed planning and installation information.

Plug-in Documentation

Provides information to help you configure specific products to monitor with Agent Manager.

Help

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

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

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

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, 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, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also 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, visit http://community.netiq.com.

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
- Complying with government regulations and audits

Agent Manager allows you to meet these objectives by:

- 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.

1.1 What Is Agent Manager?

Agent Manager is a component of NetIQ Sentinel, an automated security information and event management (SIEM) solution that addresses security management challenges.

Agent Manager provides host based data collection for Sentinel. Event sources from the Windows Event Log and Log files are supported.

1.2 How Agent Manager Works

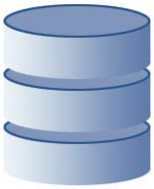
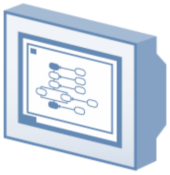
Agent Manager provides data collection rules that allow Sentinel to provide real-time data collection.

1.2.1 Understanding Product Components

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

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

Software Component	Purpose
Windows, UNIX, Linux, and iSeries Agents 	Services running on Windows, UNIX, Linux, or iSeries computers to monitor operating systems, devices, or applications, such as antivirus products.
Windows Central Computer Components 	Software running on central computers that receive data from agents and send log data to Sentinel. **Central computers** also install, uninstall, and configure Windows agents, distribute rules to Windows agent computers, and control data flow between all agents and the Sentinel servers.
Databases 	Databases located on the database server store configuration data. Agent Manager includes the AgentManager database, AgentManagerEx database, and AgentManagerCommon database, in a Microsoft SQL Server repository.
Agent Manager Consoles 	The **Agent Manager Console** customizes data collection rules, and other Agent Manager components for your environment.

1.2.2 Understanding the Architecture

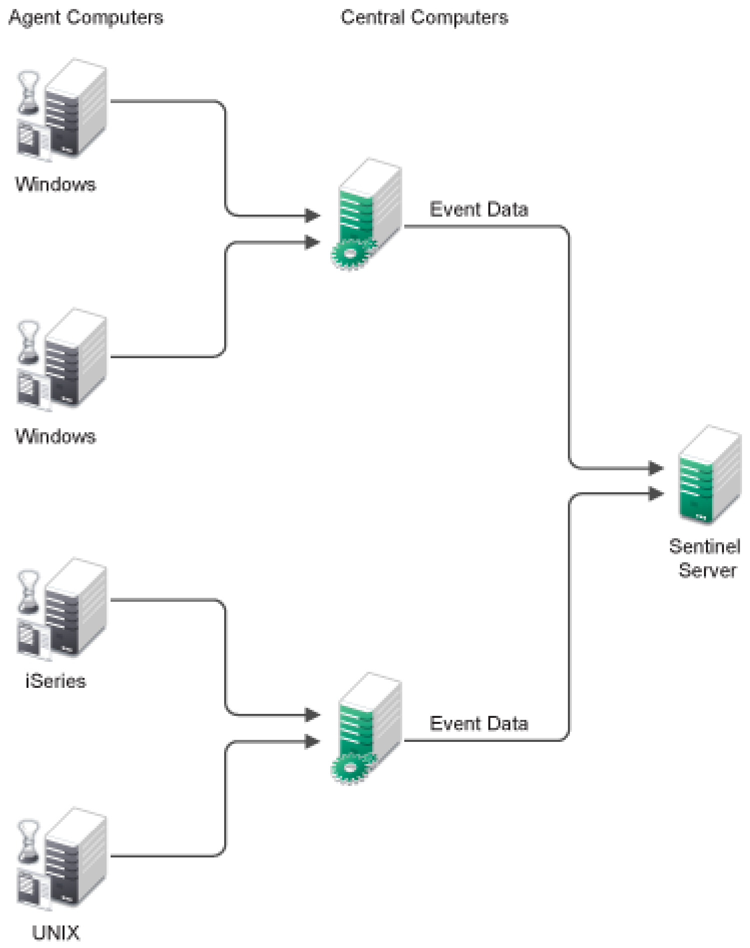
Because of the inherent adaptability of Agent Manager, there is no "one-size-fits-all" solution for installing Agent Manager. When you install Agent Manager, you can decide where to install the product components based on your environment and requirements for load balancing, failover, and performance.

The agent computers, central computer, and database server make up a product installation. You can control where to install various components of the configuration group, including where to install the database server and how many central computers to install.

A choice of configuration options is especially important in large distributed enterprises or when communicating over slower network links, such as WANs.

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

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



This model uses many agents that report to distributed central computers, and one Sentinel server configured to gather event data and store configuration information for Agent Manager.

1.2.3 Understanding Windows Component Communication

Agent Manager components installed on Windows computers communicate at specified intervals using agents to transfer data and receive data collection rules. **Data collection rules** define how Agent Manager collect 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 data collection 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. The product can take up to 15 minutes to automatically begin enforcing the rule on monitored Windows computers.

A **monitored computer** is a computer from which Agent Manager collects and processes information. Collected information can indicate critical security events occurring on the monitored computer.

1.2.4 Understanding Windows Agent Communication Security

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

Agent 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, Agent 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 Agent Manager core service components comply with the requirements of the FIPS 140-2 Inside logo program:

- central computer
- database server
- Agent Manager 7.1.0 Windows agents

1.2.5 Understanding Self-Scaling Windows Operations

Agent Manager automatically adds agents to Windows computers throughout your network. As you add Windows computers to your network, Agent 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, Agent Manager automatically changes with it. Agent Manager ensures that the right knowledge is applied to the right computers at the right time.

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

1.2.6 Understanding Supported Windows Platforms

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

- Windows Server 2012
- 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 Server 2003 (32- and 64-bit)
- Windows 8 (32- and 64-bit)
- Windows 7 (32- and 64-bit)
- Windows Vista (32- and 64-bit)
- Windows XP (32- and 64-bit)

1.2.7 Understanding Supported Data Formats

Agent 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 Agent Manager components on dual-stack computers, which are computers that have both IPv4 and IPv6 running at the same time.

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

NOTE: If you want to use your Agent 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.

1.2.8 Managing UNIX and iSeries Agents

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

Agent 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.

1.3 Understanding Requirements and Permissions

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

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

If you need to add an additional domain group, or if you did not specify a domain group at the end of installation, use the Access Configuration utility. For more information about using this utility to modify group memberships, see Section 8.6, "Modifying Agent Manager OnePointOp Group Membership," on page 53.

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

- Installing or upgrading Agent Manager
- Uninstalling Agent Manager
- Using the Access Configuration utility
- Using the Agent Manager Console

1.3.1 Agent Manager Groups

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

OnePointOp ConfgAdms

User accounts in the OnePointOp ConfgAdms group can modify the information that Security Manager collects and can configure all settings in the Agent Manager Console.

OnePointOp System

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

2 Understanding the Agent Manager Console

You can use the Agent Manager Console to customize the way Sentinel monitors computers and collects data.

Agent Manager allows Sentinel to monitor your enterprise right out of the box using built-in knowledge in the form of device groups and data collection policies. To extend and control Agent Manager, use the Agent Manager Console to perform the following types of customization:

- Define your own data collection policies.
- Update the Agent Manager configuration to include your changes.
- Identify additional sources of data in your enterprise that Agent Manager can use.

2.1 Agent Manager Console Permissions Requirements

The Agent Manager setup program installs the Agent Manager Console. To use the Agent Manager Console, log on with a user account that is a member of the OnePointOp ConfgAdms group. For more information about assigning permissions based on the group memberships, see the *Installation Guide for NetIQ Agent Manager.*

2.2 Agent Manager Console

The Agent Manager Console provides the following panes:

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

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

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

- Data Collection Policies
- Providers
- Search Results
- Configuration

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

2.2.1 Data Collection Policy Window

Data collection policies organize related data collection rules, such as all the rules to monitor a specific application.

Data collection rules define how Sentinel monitors your enterprise. For more information about data collection rules, see Chapter 4, "Managing and Analyzing Logs," on page 21.

When you create a data collection policy, Agent Manager automatically creates the subgroup Data Collection Rules.

You can search data collection policies for a specific data collection rule or for rules that match specified search criteria. When you perform a search, the right pane displays the rules that match the search criteria.

2.2.2 Search Results Window

You can search data collection policies based on keywords or wildcard characters. The Search Results window displays any data collection rules that match your search criteria. You may want to search for data collection rules to find all rules related to one topic or to locate data collection rules you want to customize. For more information about using the search feature, see Section 4.5.1, "Finding a Data Collection Rule," on page 24.

2.3 Configuration Window

The Agent Manager Console also provides the Configuration window.

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

The Configuration allows you to manage the following Agent Manager features:

Central Computers

Lists all Central Computers and lets you view details of each. You can also view and scan managed computers, view agent installation properties and specify the service account for agents installed by the selected Central Computer.

Global Settings

Lets you configure component settings that apply for all agents and central computers.

Pending Agents

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

For more information about using the Configuration snap-in, see the Help.

3 Understanding Data Collection Policies

Data collection policies are containers that let you categorize and organize your data collection rules by application or topic. When you want specific data collection rules to apply to a device group, you associate a data collection policy with a device group.

Agent Manager then applies data collection rules in data collection policies to computers in the associated device group. Data collection rules in data collection policies are not applied to any computers unless the data collection policy is associated with a device group. The Sentinel Web console allows you to manage this association.

3.1 Data Collection Policy Example

Since you associate data collection policies with specific device groups, you can think of data collection policies as groups of data collection rules that pertain to specific types of computers. For example, you could group all data collection rules you want to apply to computers running a specific application into a data collection policy.

When you select a data collection policy in the left pane, the Agent Manager Console displays details describing the contents of the data collection policy in the right pane.

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

- To print the data collection policy report pane, click **Print** in the upper right corner.
- To export information about the current data collection policy and all displayed rules to an HTML file, click **Export Group/Rule Information**.

3.2 Data Collection Policy Security Knowledge

When you select a data collection policy in the left pane, the Agent Manager Console displays the NetIQ Knowledge Base in the right pane. The NetIQ Knowledge Base provides information about the data collection policy, including a summary of features and configuration information.

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

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

4 Managing and Analyzing Logs

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

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

Agent Manager uses data collection rules to easily gather data from various logs across your enterprise network and store this data on the Sentinel server for archival and reporting.

4.1 What Are Data Collection Rules?

Data collection rules gather data from various logs across your enterprise network and store this data in a secure repository.

You can configure Agent Manager to collect almost any log data. Agent Manager collects logs using agents and settings you specify using the Configuration Wizard. Ensure you have installed and configured agents and then configured Agent Manager using the Configuration Wizard. Also ensure you have configured logging or auditing for some platforms. For more information about log collection, review the configuration wizard, Support for Operating Systems page.

Agent Manager stores data collection rules in data collection policies, and applies data collection rules to Windows computers in the device groups associated with the data collection policies. For more information about computer groups, see Chapter 7, “Understanding Device Groups,” on page 45.

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

Agent Manager supplies many built-in data collection rules, but you can also create or modify data collection rules.

4.2 Understanding Data Collection Rules

Sentinel uses the Data collection rules created in Agent Manager to collect and monitor events. Agent Manager allows you to group data collection rules by storing them in data collection policies. Using the Sentinel Web console, you associate data collection policies with the device groups you want to monitor.

To associate data collection rules with device groups, start the Sentinel Web console, click **Collection** on the top menu, and then select **Devices**. For more information about associating data collection rules and policies to device groups, see the *User Guide for NetIQ Sentinel*.

When you review a defined rule, Agent Manager displays the rule Properties window. For more information about displaying the Properties for a rule, see Section 4.5, "Working with Data Collection Rules," on page 24. The Properties tabs typically display the rule criteria that you supply when creating data collection rules. For more information about any entry on a tab, see the Help.

Depending on the data collection rule, the following tabs may be available:

General

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

Data Provider

Specifies the event or performance data provider name and type. For more information about data providers, see Section 4.3, "Understanding Data Providers," on page 22.

Knowledge Base

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

4.3 Understanding Data Providers

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

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

Sentinel collects information from a variety of sources called data providers. Data collection rules specify which provider includes the information you want to collect.

4.3.1 Windows Event Logs

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

Application

Records events from applications on the computer.

System

Records events from Windows system components.

Security

Records events based on specified Windows security options.

DNS Server

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

File Replication

Records events from the File Replication service on Windows.

Directory Service

Records events from the Active Directory service on Windows.

4.3.2 Application Logs

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

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

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

4.4 Working with Data Providers

The following topics provide information and instructions for data provider tasks.

4.4.1 Creating a Data Provider

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

To create a data provider:

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

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

You can create a data provider for a generic single-line text log based on the application log data provider. The application log data provider can collect data from only text logs encoded using the ASCII character encoding standard. The application log data provider cannot collect data encoded using the Unicode character-encoding standard.

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

1. Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see the *Installation Guide for NetIQ Agent Manager*.
2. Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.
3. In the left pane, click **Providers**.
4. On the Action menu, click **New > Provider**.
5. On the Select Data Provider Type window, click **Application Log** and then click **Next**.
6. On the Log Type window, select **Generic single-line log file,** and then click **Next**.
7. On the Directories window, click **Add**.
8. On the Directory Edit window, specify the command location, format, and file name, and then click **Next**. The file name provides Agent Manager with the file name convention for each generated log file. For example, an application may include a sequential number in its log file names, such as `error*.log`. For more information about window options, see the Help.
9. Click **Next**.
10. On the Name window, specify a provider name and then click **Finish**.

4.5 Working with Data Collection Rules

When you create a data collection rule, you specify a variety of information including the data source (data provider) and the response to take when a rule match occurs.

4.5.1 Finding a Data Collection Rule

Finding the data collection rule you want to modify or review can be a challenge if you do not know where it is stored in the data collection policy hierarchy. You can search data collection policies to locate the data collection rule you want.

Agent Manager allows you to specify detailed search criteria for each data collection rule type. The following examples demonstrate criteria you can specify for data collection rules:

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

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

To find a specific rule or set of data collection rules:

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

2 Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.

3 In the left pane, expand **Agent Manager Console > Data Collection Policies**.

4 Select any data collection rule folder.

5 On the Action menu, click **Find data collection rules**.

6 Specify the search criteria to locate the data collection rule you want. You can broaden or narrow the criteria to help you find the rules you want.

7 Click **Next** until you have finished specifying the search criteria.

8 Click **Finish**. Agent Manager displays the results of the rule search in a new window.

4.5.2 Reviewing Previous Rule Search Results

Agent Manager saves rule search results. Access previous search results using the Agent Manager Console.

To review results of a previous rule search:

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

2 Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.

3 In the left pane, expand **Agent Manager Console > Search Results > Data Collection Rule Search Results.**

4 Select a **Rule Search** results folder. Agent Manager displays the search results in the right pane.

4.5.3 Forcing Data Collection Rule Changes

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

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

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

To force data collection rule changes:

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

2 Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.

3 In the left pane, select **Agent Manager Console**.

4. On the Action menu, click **Force Configuration Changes Now**.
5. Select the central computer with agents you want to update, and then click **OK**.
6. *If Agent Manager displays a confirmation window*, click **Close**.

NOTE: Forcing configuration changes distributes data collection rules changes only to Windows computers with agents already installed. For more information about installing agents, see the Help.

5 Monitoring Workstations

Agent Manager can monitor Windows server and Windows workstation computers, collecting data from both. Because many environments can include many workstation computers, Agent Manager uses a scalability multiplier to enable central computers to monitor large numbers of agents installed on workstations.

Agents deployed on workstation computers may send relatively few events to the central computer. However, while an agent may need to send event data to the central computer infrequently, the agent must heartbeat within the configured heartbeat interval in order to remain active. Continually receiving heartbeats from multiple computers, even without event data, can affect the performance of the central computer.

If you want to enable a central computer to monitor a large number of low-volume workstation computers without becoming overburdened, you can configure the workstation scalability multiplier to increase the interval between agent communications. The agent then multiplies the default heartbeat interval and other agent communication settings by the multiplier value for all workstation computers.

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

If no computers belong to the Windows Workstations device group, changes to the workstation scalability multiplier setting do not affect your agent computers.

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

Using the Agent Manager Console, you can modify the default scalability multiplier setting. For more information about modifying global Windows agent settings in the Agent Manager Console, see Section 8.3.2, “Configuring General Agent Settings,” on page 51.

6 Administering Agents

Agent Manager monitors computers using host-based agents. An agent is a service that runs on a monitored computer to collect events and execute automatic responses.

6.1 Understanding Managed and Unmanaged Windows Agents

A **managed agent** is an agent the central computer can install and upgrade remotely. An **unmanaged agent** is an agent you manually install and update. The central computer cannot upgrade unmanaged agents.

Use an unmanaged agent in circumstances where a managed agent is not supported. Agent Manager cannot deploy managed Windows agents to remote Windows computers that are located outside a firewall. Consider installing an unmanaged agent to access the network over a WAN or a slow connection.

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

When monitoring computers behind a firewall, NetIQ Corporation recommends installing unmanaged agents on your remote computers.

For more information about installing agents in a firewall environment, see the *Installation Guide for NetIQ Agent Manager*.

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

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

- Installs and upgrades the managed agent
- Scans the managed agent
- Sends data collection rules and configuration information to the managed agent
- Receives events from the managed agent

For an unmanaged computer, a central computer sends rules and configuration information to the unmanaged agent. The central computer cannot install, upgrade, or scan an unmanaged agent.

All managed agents are authorized by the central computer by default. You can use either the Agent Administrator utility or Agent Manager Console to specifically authorize each unmanaged agent.

6.2 Understanding Discovery and Managed Windows Agent Deployment

Agent Manager can automatically deploy agents on computers that you identify. You can use the Agent Administrator to select these computers individually, or you can select multiple computers based on common characteristics using discovery rules.

Discovery rules are rules that identify computers. Agent Manager deploys a managed agent to a discovered computer and monitors it. Agent Manager evaluates discovery rules during a managed computer scan. Managed computer scans occur daily at 2:05 AM. You can manually run a managed computer scan.

Use discovery rules to identify multiple computers with similar characteristics. The central computer periodically scans all managed Windows computers assigned to it and uses device grouping rules to determine whether to place a computer in a device group. central computers then install or update managed agents on computers as necessary.

central computers install managed agents only when a computer matches the criteria for inclusion in a device group. You can configure central computers to automatically install agents or to wait for your approval.

To deploy managed agents, the service account used to run Agent Manager must be a member of the local Administrators group on the central computer and all agent computers that the central computer will manage in the domain. If you want the service account to have rights to install agents in other trusted domains, the service account must be a member of the local Administrators group on all agent computers that the central computer will manage in the trusted domain.

NOTE: Agent Manager uses NetBIOS to identify computers. Any computer on which you want to install a Windows agent must have a NetBIOS-compliant name.

For more information about configuring the heartbeat interval for agents, see Section 8.3.2, "Configuring General Agent Settings," on page 51.

Agent Manager cannot deploy managed agents on computers outside a firewall or on a non-Windows platform. For more information about manually installing unmanaged Windows agents, see Section 6.3, "Understanding Unmanaged Windows Agent Installation," on page 33.

When assigning agents to computers, ensure that you assign no more agents to the central computer than it can handle. If you want to rebalance the distribution of agents across central computers, use the Agent Administrator to assign an agent to a different central computer.

6.2.1 Deploying a Managed Windows Agent

Use this procedure to deploy managed agents on Windows computers you want to monitor.

After the central computer installs a managed agent, you may need to restart the computer before the managed agent can start. If the central computer logs an event with an event ID of `21116`, `21118`, or `21169`, you must restart the computer.

To immediately deploy a managed Windows agent:

1. Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group.
2. Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.
3. In the Navigation pane, click **Configuration**.

4 Select the appropriate configuration group in the Results window.

5 On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.

6 In the Agent Administrator window, click the Managed Agents tab.

7 In the right pane, click **Deploy Agents**.

8 Click **Add**.

9 Specify a computer you want to monitor, and then click **OK**.

10 Repeat Step 7 on page 31Step 9 on page 31 for each computer you want to monitor.

11 ***If you want to deploy the managed agents at the next scan,*** click **Finish**.

12 ***If you want to deploy the managed agents immediately or add them to the Pending Agents Installation list,*** complete the following steps:

12a In the Deploy Action column, click the row corresponding to an agent.

12b Select one of the following options:

- To deploy the managed agent immediately, select **Deploy now**.
- To add the computer to the Pending Agents Installation list, select **Add to pending list**. Depending on your settings, Agent Manager either approves and deploys agents during the next managed computer scan, or places them in the list pending your approval.

13 Click **Finish**.

For more information about deploying an agent at the next scan, see Section 6.4, “Scanning Managed Computers,” on page 33.

For more information about deploying agents added to the Pending Agents Installation list, see Section 6.8, “Handling Pending Installations,” on page 35.

6.2.2 Deploying Multiple Managed Windows Agents

You can create discovery rules to define which Windows agent computers you want to discover. Agent Manager applies the discovery rules every time it runs the daily managed computer scan.

You can use string matching or Active Directory Light Directory Access Protocol (LDAP) queries to discover multiple computers with common attributes. Because Agent Manager runs the discovery rules at every scan, Agent Manager discovers any new computers you have added to your network that fit the rule criteria.

Depending on your settings, Agent Manager installs managed agents on discovered computers, or adds them to the pending Agents Installation list to be approved or installed at the next managed computer scan. For more information about pending installations, see Section 6.8, “Handling Pending Installations,” on page 35.

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

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

After the central computer installs an agent on a Windows computer, you might need to restart the computer before the managed agent will start. If the central computer logs an event with an event ID of `21116`, `21118`, or `21169`, you need to restart the computer.

To discover and deploy Windows agents:

1. Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see Section 1.3, "Understanding Requirements and Permissions," on page 16.
2. Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.
3. In the Navigation pane, click **Configuration**.
4. Select the appropriate configuration group in the Results window.
5. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.
6. In the Agent Administrator window, click the Managed Agents tab.
7. In the right pane, click **Configure Agent Discovery Rules**.
8. Click **Add**.
9. Select **Include Computers**, and then click **Next**.
10. Complete the rules creation wizard, specifying parameters that select the computers you want to discover. For more information about fields on a window, see the Help.
11. Select the check box and row corresponding to the rule you created.
12. Click **Next**.
    - To discover computers at the next managed computer scan, click **No**.
    - To immediately discover computers, click **Yes**.
13. *If you clicked Yes,* select the central computers that will manage the computers you discover.
14. Click **Next**.
15. ***If you want to deploy agents immediately,*** click **Yes**.
16. ***If you want to add agents to the list of computers pending deployment,*** click **No**.
17. Click **Next**.
18. ***If you want to approve deployment,*** select **Approved** for each discovered computer to which you want to deploy a managed agent, and then click **Next**.
19. ***If you do not want to approve deployment at this time,*** clear **Approved** for each discovered computer you want to place in the Pending Agent Installation list, and then click **Next**.

    NOTE: If you do not approve deployment to a computer, Agent Manager places the computer in the Pending Agent Installations list until you approve deployment.
20. Specify whether to immediately deploy agents to approved computers or to deploy the agents at the next managed computer scan.
21. Click **Finish**.

NOTE: If you discover agents using a discovery rule, modify an existing rule or create a new discovery rule, and run the modified or new discovery rule, the Agent Administrator may display previously-discovered computers in both the Discovered Computers list and Agent Summary View.

If you want to only display computers discovered by a modified or new discovery rule, remove any previously-discovered computers from both the Manage Pending Actions list and Agent Summary View before using the discovery rule.

For more information about deploying an agent at the next managed computer scan, see Section 6.4, “Scanning Managed Computers,” on page 33.

6.3 Understanding Unmanaged Windows Agent Installation

The unmanaged Windows agent setup program, `manualagent.msi`, installs an unmanaged agent on the local Windows computer and guides you through Windows agent configuration. You can also use a transform file to specify setup options and silently run the setup program. Additionally, you can specify that multiple configuration groups monitor the unmanaged agent. For more information about unmanaged agent installation, see the *Installation Guide for NetIQ Agent Manager*.

6.4 Scanning Managed Computers

Agent Manager does not immediately install agents on remote computers. The central computer periodically scans computers assigned to it. The first time it scans, the central computer identifies computers on which to install agents. If you approve the computers the central computer identifies, the central computer installs agents the next time it performs a managed computer scan. By default, the central computer scans every day at 2:05 AM.

You can also scan on demand. Scanning finds computers that match the discovery rules, collects device attribute definitions older than 24 hours, and identifies computers requiring an agent installation or upgrade. By default, Agent Manager lists these computers in the Pending Agents Installation window of the Configuration snap-in, where you can choose to approve or disapprove pending installations.

To scan managed computers:

1. Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see Section 1.3, “Understanding Requirements and Permissions,” on page 16.

   NOTE: The Agent Manager service account must be a member of the local Administrators group on the managed agent computer and must be in a trusted domain or in the same domain as the database server.

2. Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.
3. In the left pane, expand **Agent Manager Agent Manager Console**, and then expand **Configuration**.
4. In the left pane, click **Global Settings**.
5. In the right pane, click **central computers**.
6. On the Action menu, click **Properties**.
7. ***If you want to change the time and frequency that central computers automatically scan managed computers,*** specify the appropriate values on the Managed Computer Scan tab.
8. ***If you want the central computer to perform a managed computer scan now,*** click **Scan managed computers now** on the Managed Computer Scan tab.
9. Click **OK**.

NOTE: Ensure the Remote Registry Service is started on the managed agent and central computer before attempting to scan agents. You can review services using the Component Services Administrative Tool, located in the Control Panel.

10 In the left pane, expand **Pending Agents > Installation** to see the results of the managed computer scan.

6.5 Scanning a Single Managed Computer

If you change the configuration of a Windows agent computer, you can prompt the central computer to scan only that computer instead of all managed computers. Scanning only the affected computer takes less time than scanning all managed computers, and allows the central computer to update the affected computer immediately, instead of waiting until the scheduled scan.

6.6 Configuring Central Computer Properties

Using the Agent Manager Console, you can modify the properties for a central computer. For example, you can specify whether the central computer automatically installs agents, or places them into the Pending Agents Installation list to await your approval.

You can also modify the Global Settings used by all central computers to deploy agents. For more information about modifying Global Settings, see Section 8.3, "Configuring Global Settings," on page 50.

NOTE: If you modify settings in the Advanced tab of the central computer settings, you must right-click **Agent Manager Agent Manager Console** in the left pane of the Agent Manager Console, select **Force Configuration Changes Now**, then manually restart the `Agent Manager` service on all affected central computers for the change to take effect.

To configure a central computer:

1. Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see Section 1.3, "Understanding Requirements and Permissions," on page 16.
2. Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.
3. In the left pane, expand the **Agent Manager Agent Manager Console**, and then expand **Configuration**.
4. Click **central computers**.
5. In the right pane, click the central computer you want to configure.
6. On the Action menu, click **Properties**.
7. Specify the appropriate values on the Properties tabs. For more information about the fields on a window, click **Help**.
8. Click **OK**.

6.7 Configuring Agent Properties

You can configure individual Windows agent properties if necessary, including buffering, service checking, event collection, communication failure handling, and response handling parameters, among others.

You can also modify the Global Settings used by all Windows agents in your configuration group. For more information about modifying Global Settings, see Section 8.3, “Configuring Global Settings,” on page 50.

NOTE: If you modify settings in the Communications, Buffering, Temporary Storage, Response Handling, or Advanced tabs, Agent Manager automatically restarts the `Agent Manager` service on all affected agent computers.

To configure individual Windows agent properties:

1 Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see Section 1.3, “Understanding Requirements and Permissions,” on page 16.

2 Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.

3 In the left pane, expand **Agent Manager Agent Manager Console**, and then expand **Configuration**.

4 Click **central computers**.

5 In the right pane, click the central computer for the agent you want to configure.

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

7 On the Managed Computers tab, click the computer with the agent you want to configure.

8 Click **Settings**.

9 Specify the appropriate values on the Properties tabs. For more information about the fields on a window, click **Help**.

10 Click **OK**.

6.8 Handling Pending Installations

Discovery rules and the settings you specify using the Agent Administrator and in the Configuration snap-in determine when an agent needs to be installed on a Windows computer. After a managed computer scan, the Pending Agents Installation window lists computers requiring agent installations and upgrades. You can approve or disapprove all pending installations or each individual pending installation.

NOTE: If a computer on the approved installation list is running the Windows Event Viewer or any Agent Manager console, ensure you close the Windows Event Viewer and the console before starting the managed computer scan. If these products are running during a managed computer scan, you may need to restart the computer before the Agent Manager agent will start.

6.8.1 Approving Pending Installations

By default, Agent Manager requires you to manually approve deployment of managed agents. If you did not choose to immediately deploy managed agents or approve them for deployment at the next scan, Agent Manager adds them to a Pending Agents Installation list, where the managed agents wait until you approve them for deployment either immediately or at the next scan.

Approving Pending Installations Using the Agent Administrator

You can use the Agent Administrator to approve pending installations of managed agents.

To approve pending installations using the Agent Administrator:

1. Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see Section 1.3, "Understanding Requirements and Permissions," on page 16.
2. Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.
3. In the Navigation pane, click **Configuration**.
4. Select the appropriate configuration group in the Results window.
5. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.
6. In the Agent Administrator window, click the Managed Agents tab.
7. In the left pane, click **Managed Agents**.
8. In the right pane, click **Manage Pending Actions**.
9. Select computers to approve for installation, and then click **Next**. For more information about the fields on a window, see the Help.
10. *If you want to install the agent immediately,* click **Yes**.
11. *If you want to schedule the approved agent installation for the next managed computer scan,* click **No**.
12. Click **Finish**.

Approving Pending Installations Using the Agent Manager Console

By default, Agent Manager adds Windows computers requiring agent installations or upgrades to the Pending Agents Installation list to wait for approval. You can approve all pending installations or upgrades or each individual pending installation or upgrade using the Agent Manager Console.

To approve pending installations or upgrades using the Agent Manager Console:

1. Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see Section 1.3, "Understanding Requirements and Permissions," on page 16.
2. Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.
3. In the left pane, expand **Agent Manager Agent Manager Console**, and then expand **Configuration > Pending Agents > Installation**.
4. *If you want to approve all pending installations or upgrades,* on the Action menu, click **Approve All Pending Installations**.

5 ***If you want to approve individual pending installations or upgrades,*** complete the following steps for each computer you want to approve:

   5a In the right pane, click the computer you want to approve.

   5b On the Action menu, click **Approve**.

6 ***If you want to install all approved installations and upgrades now***, on the Action menu, click **Install All Approved Agents Now**. The time required for installation depends on your network configuration.

6.8.2 Disapproving Pending Installations

In some circumstances, you may not want to automatically deploy managed agents to computers that you want to monitor. If you have already approved an agent for deployment at the next scan but want to delay that deployment, you can disapprove deployment indefinitely.

Disapproving Pending Installations Using the Agent Administrator

You can use the Agent Administrator to disapprove pending installations.

To disapprove pending installations using the Agent Administrator:

1 Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see Section 1.3, "Understanding Requirements and Permissions," on page 16.

2 Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.

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

4 Select the appropriate configuration group in the Results window.

5 On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.

6 In the Agent Administrator window, click the Managed Agents tab.

7 In the right pane, click **Manage Pending Actions**.

8 Clear the check boxes of approved agents you want to disapprove, and then click **Next**. For more information about the fields on a window, click **Help**.

9 Click **No**.

10 Click **Finish**.

Disapproving Pending Installations Using the Agent Manager Console

By default, Agent Manager adds Windows computers requiring agent installations or upgrades to the Pending Agents Installation list to wait for approval. You can disapprove all pending installations or upgrades or each individual pending installation or upgrade using the Agent Manager Console. The central computer waits for approval before installing or upgrading agents on Windows computers.

To disapprove all pending installations using the Agent Manager Console:

1 Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see Section 1.3, "Understanding Requirements and Permissions," on page 16.

2 Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.

3 In the left pane, expand **Agent Manager Agent Manager Console > Configuration > Pending Agents > Installation**.

4 *If you want to disapprove all pending installations or upgrades,* on the Action menu, click **Disapprove All Pending Installations**.

5 *If you want to disapprove individual pending installations or upgrades,* complete the following steps on each computer you want to disapprove:

5a In the right pane, click the computer you want to disapprove.

5b On the Action menu, click **Disapprove**.

6 Close the Agent Manager Console.

6.8.3 Verifying Windows Agent Installation

If a computer on the approved installation list is running the Windows Event Viewer or any Agent Manager console, ensure you close the Windows Event Viewer and the console before starting the managed computer scan. If these products are running during a managed computer scan, you may need to restart the computer before the Agent Manager agent will start.

If the central computer logs an event with an event ID of `21116`, `21118`, or `21169`, you need to restart the computer. Monitor these events in the Agent Manager Console to verify correct agent installation.

To verify that Windows agents are online:

1 Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp Users group. For more information about groups and permissions, see Section 1.3, “Understanding Requirements and Permissions,” on page 16.

2 Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.

3 In the Navigation pane, click **Infrastructure Components**.

4 In the Navigation pane, click **Agents**.

5 In the Results window, check the **Agent Status** column. If the agent is working, the status is **Running**.

NOTE: After you deploy one or more new agents, you may not immediately see the new agents in the Agents view. Until the new agents receive configuration information from the central computer and respond, the agent computers do not belong to any device group. The Agents view does not display computers that do not belong to at least one device group.

To view newly deployed agents before Agent Manager configures the agent computers, click **Ungrouped Computers** in the Navigation pane, instead of Agents.

6.9 Viewing Agents

From the **Agent Summary View** in the Agent Administrator, you can view the status of agents on all computers monitored by your configuration group. From this window, you can also perform maintenance and troubleshooting tasks to keep your agent environment in good working order.

6.9.1 Viewing All Agents

You can view information about all agents in a configuration group. The information available from the Agent Administrator includes:

- The domain of an agent computer
- Whether a computer has a managed, unmanaged, UNIX, or iSeries agent
- Whether a computer is authorized in the database
- Whether a computer has an agent installation or upgrade pending
- Whether a computer is a proxy agent or an agentless monitored computer

6.9.2 Viewing the Computers Assigned to a central computer

The central computer finds computers that match the discovery rules, collects device attribute definitions older than 24 hours, and installs an agent as appropriate.

To view the agents assigned to a central computer:

1. Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group.
2. Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.
3. In the left pane, expand **Agent Manager Agent Manager Console**, and then expand **Configuration**.
4. Click **central computers**.
5. In the right pane, click the central computer with agents you want to view.
6. On the Action menu, click **View Managed Computers**. For more information about the fields on a window, click **Help**.

6.9.3 Changing Which central computer Manages an Agent

You can change the central computer to which a managed or unmanaged agent is assigned. You can specify any central computer in the same configuration group. For more information about the relationship between an agent and a central computer, see Section 6.1, "Understanding Managed and Unmanaged Windows Agents," on page 29.

NOTE: If you reassign an agent to a central computer that uses a different service account, ensure the service account is a member of the local Administrators group on all agents it will manage.

You may want to assign a new central computer to an agent in the following circumstances:

- To remove the central computer from the configuration group. When you permanently stop using a central computer, assign a new central computer to the managed and unmanaged agents managed by that computer.
- To take a central computer offline temporarily.
- To reassign agents to different central computers to balance the agent load. No central computer should manage too many agents. Monitor central computer performance to determine whether you need to rebalance the agent load.

To change the central computer to which an agent is assigned:

1. Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see Section 1.3, "Understanding Requirements and Permissions," on page 16.
2. Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.
3. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.
4. In the left pane, click **Agent Summary**.
5. In the right pane, click **Agent Summary View**.
6. Select an agent you want to reassign to another central computer.
7. Click **Reassign**.
8. Select a different central computer, and then click **OK**. For more information about the fields on a window, see the Help.
9. Click **Yes** to confirm the change.
10. Click Apply.
11. Click **Close**.
12. Select **Apply configuration changes now**.
13. Click **OK**.
14. Verify the selected central computer and click **OK**.
15. Click **Close**.

6.9.4 Changing the Name or Domain of a Monitored Computer

If you change the name of the domain in which a monitored computer is located, move the computer to a different domain, or want the agent to monitor a different computer, update the agent using the Agent Administrator. If you are changing the domain of an agent computer, perform this task after you change the domain of the computer.

To change the name or domain of a monitored computer:

1. Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see Section 1.3, "Understanding Requirements and Permissions," on page 16.
2. Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.
3. On the Tasks menu, click **Global Tasks > Launch Agent Administrator**.
4. In the Agent Administrator window, click the Agent Summary tab.
5. Click **Agent Summary View**.
6. Select the agent you want to associate with a different domain.
7. Click **Change**. For more information about the fields on a window, see the Help.
8. ***If you want to change which computer the agent monitors,*** complete the following steps:

   8a Select **Computer**.

   8b In the **New Computer** field, type the name of the computer you want the agent to monitor and click **OK**.

9. ***If you want to update the domain to which a monitored computer belongs,*** complete the following steps:
   - **9a** Select **Domain**.
   - **9b** Select the domain to which the monitored computer now belongs, and then click **OK**.
10. Click **Apply**.

6.10 Disabling Communication from Computers

Instances may occur in which you want to disable communication from an agent without uninstalling the agent software or removing the agent from the Agent Manager database. For example, if an agent begins to send garbled data, you may want to prevent the agent from communicating with the central computer until you resolve the problem with the agent.

NOTE: If you plan to keep the agent in an unauthorized state for an extended period of time, stop the `Agent Manager` service on the agent computer. If the service is not stopped, the agent will continue evaluating rules and attempting to contact the central computer.

By default, each agent is authorized to communicate with the central computer. The following procedure suspends this authorization.

6.11 Viewing Hidden Computers

When you uninstall an agent from a Windows computer, Agent Manager automatically hides that computer from some views. You can still view any collected events.

Agent Manager automatically hides the computer from the Sentinel console.

You can also show hidden computers if at a later date you want to view old agent information about them. However, showing a hidden computer does not cause Agent Manager to resume monitoring that computer.

6.12 Uninstalling Windows Agents

You may decide that an agent already installed on a computer is not required.

To uninstall managed Windows agents from Windows computers, you can use the Agent Administrator.

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.

NOTE

- A central computer cannot uninstall unmanaged Windows agents. For more information, see the *Installation Guide for NetIQ Agent 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.

6.12.1 Uninstalling Managed Windows Agents Using the Agent Administrator

The following procedure uninstalls agent software from a managed computer.

To uninstall a Windows agent using the Agent Administrator:

1. Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see Section 1.3, "Understanding Requirements and Permissions," on page 16.
2. Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.
3. In the Navigation pane, click **Configuration**.
4. Select the appropriate configuration group in the Results window.
5. In the right pane, click **Agent Administrator**.
6. In the Agent Administrator window, click the Agent Summary tab.
7. Click **Agent Summary**.
8. Click **Agent Summary View**.
9. Select the row of the computer you want to uninstall.
10. Click **Uninstall**.
11. Select when you want to uninstall the managed agent:
    - To uninstall the agent immediately, click **Uninstall Now**.
    - To uninstall the agent at the next managed computer scan, click **Pending**.

    NOTE: By default, Agent Manager automatically approves pending agent uninstallation procedures. If you changed this Global setting, clicking **Pending** places the agent uninstall procedure in the Pending Agent Installations list until you approve it.
12. Click **Finish**.
13. ***If you are uninstalling a proxy agent that monitors an agentless monitored computer,*** Agent Manager stops monitoring the agentless monitored computer but does not hide it from views. If you want to hide it, use the Agent Summary view in the Agent Administrator. If you want to assign another proxy agent to monitor the agentless monitored computer, run the Agentless Monitored Computers wizard in the Agent Administrator.

6.12.2 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.

The following procedure uninstalls an unmanaged Windows agent for all configuration groups.

To uninstall an unmanaged agent:

1. Log on to an unmanaged agent computer as a local administrator.
2. Close all open applications.
3. Run **Add or Remove Programs** from the Control Panel.
4. Select **NetIQ Agent Manager Agent**.
5. Click **Remove**.
6. Click **Yes**.

7. Follow the instructions until the unmanaged agent is removed.
8. Close the Add or Remove Programs window.
9. Log off of the unmanaged agent computer.
10. Log on to a central computer that monitors the unmanaged agent as a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see Section 1.3, “Understanding Requirements and Permissions,” on page 16.
11. Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.
12. In the left pane, click **Agent Summary**.
13. In the right pane, click **Agent Summary View**.
14. Select the unmanaged agent you want to remove.
15. Click **Uninstall > Pending**.
16. Click **Yes**.
17. Click **Apply**.
18. Click **Close**.
19. Select **Apply configuration changes now**.
20. Click **OK**.
21. Verify the selected central computer and click **OK**.
22. In the left pane, click **Managed Agents**.
23. In the right pane, click **Manage Pending Actions**.
24. Select **Approved** for the unmanaged agent you want to remove.
25. Click **Finish**.
26. In the left pane, click Agent Summary.
27. In the right pane, click Agent Summary View.
28. Select Show Hidden Computers.
29. Select the removed unmanaged agent.
30. Click **Delete**.
31. Click **Yes**.
32. Click **Close**.
33. Select **Apply configuration changes now**.
34. Click **OK**.
35. Verify the selected central computer and click **OK**.
36. Click **Close**.

6.13 Configuring iSeries Agent Deployment

Agent Manager can monitor iSeries servers using an iSeries agent and can monitor, analyze, and consolidate events from log files on monitored iSeries servers.

6.14 Configuring UNIX Agent Deployment

Agent Manager can monitor UNIX computers using a UNIX agent. For more information about deploying and configuring UNIX agents, see the NetIQ UNIX Agent documentation. For more information about configuring the UNIX agent for Agent Manager, see the NetIQ UNIX Agent documentation.

7 Understanding Device Groups

Device groups are groups of computers that have some attribute in common, such as all computers with McAfee VirusScan installed. You can create device groups, and you can add Windows computers to built-in device groups in the Sentinel console.

Device groups use membership criteria to define the types of computers to include. Organizing Windows computers into device groups allows Agent Manager to apply certain data collection policies to computers which serve a similar purpose. For more information about data collection policies, see Chapter 3, "Understanding Data Collection Policies," on page 19.

7.1 Built-in Device Groups

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

If you are creating custom data collection rules, the built-in device groups might not contain the computers to which you want to deploy the custom data collection rules. You can create a device groups to contain the computers. You can identify the computers to place in the device group using membership criteria, such as explicit inclusion or computer attributes. For more information about device grouping criteria, see Section 7.3, "Understanding Device Grouping Criteria," on page 46.

7.2 Device Group Membership

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

Agent Manager places Windows computers in the appropriate device groups if the following two conditions are met:

- An agent is installed or to be installed on the Windows computer. For more information about installing agents on Windows computers or other platforms, see the Help and the *Installation Guide for NetIQ Agent Manager*.
- The computer matches the criteria defined in the device group properties. For more information about device group properties, see Section 7.3, "Understanding Device Grouping Criteria," on page 46.

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

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

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

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

NOTE: If the device group is associated with a data collection policy, the central computer also periodically updates the Windows agent with data collection rules contained in the data collection policy. For more information about associating device groups with rule groups, see Section 7.4.1, "Associating a Device Group with a Data Collection Policy," on page 46.

7.3 Understanding Device Grouping Criteria

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

7.4 Working with Device Groups

Agent Manager provides tremendous flexibility with device groups. You can create new device grouping rules to define new sets of Windows computers for Agent Manager to manage and monitor.

7.4.1 Associating a Device Group with a Data Collection Policy

If you create a device group, associate it with the data collection policy containing the data collection rules you want applied to the computers in the device group. You can associate device groups and data collection policies in the Sentinel Web Console. Built-in data collection policies are already associated with built-in device groups.

Data collection rules are updated periodically on agents. You can expedite this process. For more information about updating Data Collection rules, see Section 4.5.3, "Forcing Data Collection Rule Changes," on page 25.

7.5 Understanding Device Attribute Definitions

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

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

The central computer sends computer attribute definitions to Windows agents whenever it installs a Windows agent or the definitions change. The Windows agents send their computer attributes to the central computer when it first installs the Windows agents, every 24 hours since the Windows agents last sent their computer attributes, or during a managed computer scan if the computer attributes are older than 24 hours. For more information about device group attributes, see Section 7.2, “Device Group Membership,” on page 45.

7.5.1 Predefined Device Attribute Definitions

Sentinel Agent Manager provides predefined computer attributes that define built-in device groups. Predefined computer attributes are located in the Sentinel Web Console.

7.5.2 Custom Device Attribute Definitions

You can create custom computer attributes that you can use and reuse to create device groups.

When you create or modify a computer attribute, the central computer sends the computer attribute definition to the Windows agents at the next heartbeat. Then the Windows agents collect their computer attributes and send them to the central computer at the following heartbeat. After the central computer receives computer attributes, it places computers in the appropriate device groups. For more information about device groups, see Section 7.2, “Device Group Membership,” on page 45.

8 Configuring Agent Manager

You typically deploy agents and configure Agent Manager immediately after installation. However, sometimes you must reconfigure Agent Manager to fine-tune your implementation. This chapter covers configuration tasks and customization tasks to refine Agent Manager for your environment. For more information about the initial configuration of Agent Manager, see the *Installation Guide for NetIQ Agent Manager*.

This chapter does not cover configuration tasks relating to agents, such as adding and deleting agents or modifying their properties. For more information about configuring agents, see Chapter 6, "Administering Agents," on page 29.

You can also customize Agent Manager by modifying existing data collection rules or creating new rules specifically suited for your environment.

8.1 Using the Configuration Wizard

You can customize Agent Manager using the Configuration Wizard.Typically, you use this wizard immediately after installation to register UNIX and iSeries agents to be monitored by Agent Manager. You can run the Configuration Wizard at any time to reconfigure these settings.

8.2 Configuring Message Buffering

Agent Manager uses persistent storage to protect against data loss, storing data locally on the agent level. Windows agents temporarily store data on the agent computer to safeguard against communication interruptions between the agent and the monitoring central computer. If a communication failure occurs, the agent stores any collected event or log data until the agent can re-establish a connection with the central computer and then sends all collected data.

Agent Manager categorizes pending agent messages as normal priority, invalid, or high priority, with buffer disk space allocated for messages of each category. The following table lists the default buffer sizes for each message category:

Message Category Name	Default Buffer Size (in KB)
Normal Priority	1000000
Invalid	10000

Using the Agent Manager Console, you can configure temporary storage settings globally, for all agents, or for specific agents in a configuration group. You can increase or decrease the default message buffer sizes, as necessary.

A Windows agent that cannot communicate with a central computer stores data until one of the following events occurs:

- The agent can send the data.
- The stored data grow to the size of the configured message buffering settings.
- The stored data grow to fill the hard disk of the agent computer.

After the agent reaches either the agent's message buffering settings or the hard disk space limit of the computer, the agent stops processing collected data. Event data remains in the native event logs until the agent can begin processing again.

To configure temporary storage settings:

1. Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see Section 1.3, "Understanding Requirements and Permissions," on page 16.
2. Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.
3. In the left pane, expand **Agent Manager Console**, and then expand **Configuration**.
4. ***If you want to configure global temporary storage settings,*** complete the following steps:

   4a Click **Global Settings**.

   4b On the Action menu, click **Edit Agent Settings**.
5. ***If you want to configure temporary storage settings for a specific agent computer,*** complete the following steps:

   5a Click **central computers**.

   5b In the right pane, select the central computer that monitors the agent you want to configure.

   5c On the Action menu, click **View Managed Computers**.

   5d Select the agent computer you want to configure and click **Settings**.
6. Click the Temporary Storage tab.
7. Specify the appropriate settings. For more information about the fields on a window, click **Help**.
8. Click **OK**.

8.3 Configuring Global Settings

These tasks provide step-by-step guidance for configuring Global Settings, such as component communications.

8.3.1 Configuring Communication Ports

You can change the default TCP/IP port for communications between Windows agents and central computers in a configuration group. For more information about default ports, see the *Installation Guide for NetIQ Agent Manager*.

NOTE: NetIQ does not recommend changing the default port after you initially configure your environment. Changing the port can cause significant interruptions in communications between central computers and agents. If you change the port and then restart the `NetIQ Agent Manager` service on your central computers, your agents cannot communicate with your central computers until you restart the service on all agents, as well.

To change the TCP/IP port:

1. Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see Section 1.3, "Understanding Requirements and Permissions," on page 16.
2. Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.
3. In the left pane, expand **Agent Manager Console**, and then expand **Configuration**.
4. Click **Global Settings**.
5. In the right pane, click **Communications**.
6. On the Action menu, click **Properties**.
7. ***If you want to modify the port for standard Windows agents,*** specify the port number you want your Windows agents to use to communicate with your central computer. For more information about the fields on a window, click **Help**.
8. In the left pane, click **central computers**.
9. On the Action menu, click **Scan All Managed Computers**.
10. When the central computer finishes scanning all managed agents, stop and restart the `NetIQ Agent Manager` service on all central computers in your configuration group.
11. After you restart the service on all central computers, log on to each agent computer and manually stop and restart the `NetIQ Agent Manager` service.

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

8.3.2 Configuring General Agent Settings

Using the Agent Manager Console, you can configure settings for managed and unmanaged Windows agents in the configuration group, either globally or for each specific agent computer. These settings include buffering, service checking, event collection, communication failure handling, among others.

NOTE

- You can only modify certain agent settings globally, like scalability and heartbeat settings.
- If you modify settings in the Communications, Scalability, Buffering, Temporary Storage, or Advanced tabs, Agent Manager automatically restarts the `NetIQ Agent Manager` service on all affected agent computers.

To configure global Windows agent settings:

1. Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see Section 1.3, "Understanding Requirements and Permissions," on page 16.
2. Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.
3. In the left pane, expand **Agent Manager Console**, and then expand **Configuration**.
4. ***If you want to configure global Windows agent settings,*** complete the following steps:

   4a Click **Global Settings**.

   4b On the Action menu, click **Edit Agent Settings**.

5 *If you want to configure settings for a specific agent computer,* complete the following steps:

5a Click **central computers**.

5b In the right pane, select the central computer that monitors the agent you want to configure.

5c On the Action menu, click **View Managed Computers**.

5d Select the agent computer you want to configure and click **Settings**.

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

7 Click **OK**.

8.4 Configuring Primary and Backup central computers

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

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

When failover to another central computer occurs, the backup central computer provides many of the functions the primary central computer provided until the primary central computer is again accessible. Following failover, agents send events to the backup central computer. The backup central computer can pass rules and configuration to the agent and can scan the agent.

Each central computer can have more than one backup computer. When Agent Manager initiates failover, the inaccessible central computer fails to the first designated backup central computer. If the backup central computer is also unavailable, Agent Manager continues down the list until it identifies an available computer.

NOTE: If you are permanently removing a primary central computer, do not rely on failover to provide agent coverage. Instead, reassign the agent to a different central computer. For more information about changing the central computer to which an agent is assigned, see Section 6.9.3, “Changing Which central computer Manages an Agent,” on page 39.

To manually specify central computers for failover:

1 *If the central computers use different service accounts,* ensure the service account used by each backup central computer is a member of the local Administrators group on all agents managed by the primary central computer and that each is also either in a trusted domain or the same domain as the database server.

2 Log on to the Agent Manager Console computer using an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see Section 1.3, “Understanding Requirements and Permissions,” on page 16.

3 Start the **Agent Manager Console** in the NetIQ Sentinel Agent Manager program group.

4 *If you want to disable automatic failover,* complete the following steps.

4a In the left pane, expand **Agent Manager Agent Manager Console > Configuration > Global Settings**.

4b In the right pane, click **central computers**.

4c On the Action menu, click **Properties**.

4d Click **Redundancy Policy**.

4e Clear **System controlled**.

4f Click **OK**.

5 In the left pane, click **central computers**.

6 In the right pane, select a central computer for which you want to specify failover computers.

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

8 Click **Redundant central computers**.

9 In Available central computers, select a computer.

10 Click >>.

11 Repeat Step 9 on page 53Step 10 on page 53 for each central computer that you want to designate as a failover computer.

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

13 Click **OK**.

8.5 Changing Service Account Passwords

To change the password for the service account, follow the instructions in the NetIQ Technical Support Knowledge Base.

To access the NetIQ Technical Support Knowledge Base:

1 Access the Web site at `www.netiq.com/support`.

2 Click **Support & Services > Technical Support**.

3 In the **Search Knowledgebase** field, type `How do I change the service account password?`

4 In **Choose a Product** select **NetIQ Security Manager**.

5 Click **Search**.

6 Scroll down to see a list of related topics.

7 Click the title of the most appropriate topic.

8.6 Modifying Agent Manager OnePointOp Group Membership

Agent Manager uses OnePointOp groups and database roles to restrict access to product functionality. For more information about OnePointOp groups and database roles, see Section 1.3, "Understanding Requirements and Permissions," on page 16.

The Access Configuration utility allows you to add global domain groups to the OnePointOp groups. The utility also creates database logins for the global domain groups, and then adds the database logins to the appropriate database roles on the database server. You can also use the Access Configuration utility to repair invalid accounts.

If you added an account with a user interface other than the Access Configuration utility, the account is invalid. For a user account to be valid it must be a member of a global domain group that you added to a OnePointOp group with the Access Configuration utility. The Access Configuration utility must also create a database login for the global domain group.

If a global domain group contains an invalid user account, you can use the Access Configuration utility to repair the user account. The Access Configuration utility repairs the user account by resetting the database login. However, the Access Configuration utility cannot make a user account valid if the account does not belong to a global domain group already a member of one or more OnePointOp groups.

To add a user account to a OnePointOp group and database role, add the user account to a global domain group that is a member of the OnePointOp group.

NOTE: The Access Configuration utility does not manage membership of the global domain groups. Use Active Directory Users and Computers to manage account memberships of the global domain groups.

To modify memberships in OnePointOp Groups and database roles:

1. Log on to a central computer with an account that is a member of the local Administrators group and a member of the Microsoft SQL Server sysadmin role on the database server.
2. Start **Access Configuration** in the Configuration program group.
3. In the left pane, click the OnePointOp group with memberships you want to modify. Complete one of the following steps:
   - To add a member, click **Add**.
   - To remove a member, click **Remove**.
   - To repair a member, select an invalid group member, and then click **Repair**.
4. Repeat Step 3 on page 54 for each OnePointOp group you want to modify.
5. Click **OK**. For more information about fields on a window, see the Help.
6. Repeat Step 1 on page 54 Step 5 on page 54 on each central computer.

A Understanding Text String Pattern Matching

In many Agent Manager fields, you can enter or select wildcard characters, regular expressions, or Boolean regular expressions. Wildcard characters and regular expressions allow you to specify or match many items using one expression or character-string formula.

NOTE: Agent Administrator does not support using regular expressions or Boolean regular expressions. Regular or Boolean regular expressions are only used in defining or finding rules in the Agent Manager Console.

You can select wildcard characters, regular expressions, or Boolean regular expressions from some drop-down menus, or you can enter them directly in the appropriate field, depending on the interface. Wildcard menu items and their associated characters are defined in tables in the following sections.

A.1 Wildcard Characters

You can use wildcard characters in some areas where you cannot use regular expressions. Wildcard pattern matching is not case-sensitive. Some fields support the following wildcard characters.

Menu Item	Character	Definition
Any Character	Question mark (?)	Matches exactly one character.
Any Digit	Number sign (#)	Matches one digit. **NOTE:** This wildcard is used only when defining rules or views and cannot be used for Forensic Analysis queries.
Any Character, 0 or More Matches	Asterisk (*)	Matches zero or more characters.

The following table provides examples of wildcard character specifications and example matches. The escape character (\ ) that precedes a character changes the character from a wildcard to its text meaning. For example, Agent Manager reads the Any Character wildcard in `houston\?` as a question mark.

Example	Matches	Does Not Match
den???	Denton and Dennis	Denison
`el ????o`	El Campo and El Indio	El Paso
`houston\?`	Houston?	Houstons

Example	Matches	Does Not Match
houston, tx #####	Houston, TX 77024	Houston, TX USOFA
5555 lovers ln \###	5555 Lovers Ln #32	5555 Lovers Ln 320
*TX	Houston, TX and TX	Houston, TX 77024
San *	San Antonio and San Angelo	Santa Fe
b*ville	Brownsville and Beeville	Somerville

A.2 Regular Expressions

You can perform advanced text pattern matching using **regular expressions**. Regular expressions provide more flexibility than simple wildcard characters in defining rules or views. To match an exact regular expression character, precede the character with a backslash (\).

The following table lists regular expression operators and their definitions:

Menu Item	Character	Definition
Any Character	.	Matches any single character.
Character in Range	[ ]	Matches any single character from within the bracketed list. Within square brackets, most characters are interpreted literally.
Character Not in Range	[^]	Specifies a set of characters not to be matched.
Beginning of Line	^	Matches the beginning of a line.
End of Line	$	Matches the end of a line.
Or	|	Matches either the regular expression preceding it or the regular expression following it.
Group	( )	Groups one or more regular expressions to establish a logical regular expression consisting of sub-regular expressions. Used to override the standard precedence of specific operators.
0 or 1 Matches	?	Specifies that the preceding regular expression is matched 0 or 1 time.
0 or More Matches	*	Specifies that the preceding regular expression is matched 0 or more times.
1 or More Matches	+	Specifies that the preceding regular expression is matched 1 or more times.
Exactly N Matches	{n}	Specifies that the preceding regular expression is matched exactly n number of times.
At Least N Matches	{n,}	Specifies that the preceding regular expression is matched n or more times.
At Most N Matches	{,n}	Specifies that the preceding regular expression is matched n or fewer times.

Menu Item	Character	Definition
N to M Matches	{n,m}	Specifies that the preceding regular expression is matched a maximum of m times and a minimum of n times.
New Line Character	\n	Matches a new line.
Tab Character	\t	Matches a tab character.

The following table provides examples of regular expressions and matches.

Example	Matches	Does Not Match
`st.n`	Austin and Houston	Webster
`st[io]n`	Austin and Houston	Stanton
`st[^io]n`	Stanton	Houston or Austin
`^houston`	Houston	South Houston or Fort Sam Houston
`ston$`	Houston and Galveston	Stonewall
`dall|hart`	Dallas and Dalhart and Lockhart	Dale
`dal(l|h)art`	Dalhart	Dallas or Lockhart
`il?e$`	Etoile and Wylie	Beeville
`il*e$`	Etoile and Wylie and Beeville	Bellaire
`il+e$`	Etoile and Beeville	Wylie
`ad{2}`	Addison and Caddo	Adkins
`(la.*){2,}`	Highland Village and Lake Dallas	Laredo
`il{,1}e$`	Bowie and Etoile	Brownsville
`(a.*){2,3}`	Alamo Heights and La Blanca	Austin or Arkansas Pass
`not ville`	Houston and Dallas	Brownsville

A.3 Boolean Regular Expressions

Boolean regular expressions allow you to combine regular expressions using the Boolean `and`, `or`, and `not` operators.

Menu Item	Operator	Definition
Boolean And	and	Specifies that the preceding and following regular expressions must both match.
Boolean Or	or	Specifies that one of the preceding and following regular expressions must match.
Boolean Not	not	Specifies that the regular expression following the Not must not match.

Regular and Boolean regular expression operators are available from some drop-down menus, or you can enter them directly in the appropriate field. The following table shows examples of Boolean regular expressions:

Example	Matches	Does Not Match
`la and ia`	La Vernia and Lelia Lake	Lake Jackson
`ville$ or town$`	Brownsville and Baytown	Lubbock
`ille$ and not ^[n-z]`	Brownsville and Kerrville	Pflugerville

B Configuring Authenticated Communication

Agent Manager provides two types of secure communication on Windows platforms. The default is encrypted communication, used to preserve the privacy and integrity of data passed between the central computer and agents.

Additionally, you can choose to authenticate communication. Certificate-based authentication adds a level of security by enabling the central computer to verify the data it collects comes only from valid agent computers. Authentication also enables the agent computers to verify the central computer itself is valid.

WARNING: Changing from encrypted communication mode to encrypted and authenticated mode is an operation that requires significant planning and consideration.

Ensure you install all appropriate certificates before enabling agent authentication or central computer authentication. If you enable authentication without correctly installing all certificates, your central computers and agents cannot communicate.

B.1 Understanding Default Agent Manager Communication

Agent Manager uses the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocols included in the Microsoft Secure Channel (SChannel) security package to send data from Windows agents to the central computer.

Out of the box, Agent Manager uses a default self-signed certificate, installed on the central computer, for communication between the central computer and monitored Windows agents.

If you want to enable authenticated communication, you can implement your own Public Key Infrastructure (PKI) and deploy custom certificates on central computers and agents, replacing the default central computer certificate. For more information about authenticated communication, see Section B.2, “Understanding Authenticated Communication,” on page 60.

Agents on UNIX and iSeries computers also communicate with the central computer using the SSL protocol. UNIX and iSeries agents authenticate any central computer that requests data collection.

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

B.2 Understanding Authenticated Communication

Agent Manager uses the self-signed certificate created during installation of the central computer to enable secure communication between the central computer and agents. By default, agent computers do not provide their own agent certificates to the central computer.

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

To enable authenticated communication, use your PKI to deploy and install trusted certificates on the central computer, agent computers, or both, depending on your environment. You can configure authenticated communication for any of the following scenarios:

- You can enable agent authentication, so the central computer that monitors your agents communicates only with agent computers presenting valid, trusted certificates.
- You can enable central computer authentication, so monitored agents communicate only with a central computer presenting a valid, trusted certificate.
- You can enable mutual authentication, so agents communicate only with central computers presenting valid, trusted certificates, and central computers communicate only with agent computers presenting valid, authenticated certificates.

After generating and installing trusted certificates on both agent computers and the central computer, as necessary, modify the registry on all affected computers to configure central computer Authentication and Agent Authentication settings. For more information about modifying the registry to enable authentication, see Section B.3.4, “Enabling Agent Authentication,” on page 64 and Section B.3.5, “Enabling central computer Authentication,” on page 64.

For authentication changes to take effect, you must restart the `NetIQ Agent Manager` service on the central computer and all affected agents.

If you enable authentication between a central computer and an agent but do not correctly install or configure certificates for both components, the following situations occur:

- The agent is unable to send a heartbeat to the central computer.
- The central computer is unable to update the agent configuration.

B.3 Implementing Authenticated Communication

You can configure authenticated communication in your Agent Manager environment by completing the following checklist:

☑	Steps	See Section
□	*If you want to configure authenticated communication with your agent computers*, issue and install agent computer certificates.	Section B.3.1, “Certificate Requirements,” on page 61 Section B.3.2, “Issuing and Installing Agent Authentication Certificates,” on page 62
□	1. *If you want to configure authenticated communication with your central computers*, issue and install central computer certificates.	Section B.3.1, “Certificate Requirements,” on page 61 Section B.3.3, “Issuing and Installing central computer Authentication Certificates,” on page 63

☑	Steps	See Section
□	2. *If you want to configure authenticated communication with your agent computers,* enable agent authentication.	Section B.3.4, “Enabling Agent Authentication,” on page 64
□	3. *If you want to configure authenticated communication with your central computers,* enable central computer authentication.	Section B.3.5, “Enabling central computer Authentication,” on page 64
□	4. *If you want to customize additional authentication settings,* modify the appropriate registry keys.	Section B.3.6, “Customizing Certificate Usage,” on page 65
□	5. Verify that authenticated agents and central computers can communicate.	Section B.3.7, “Verifying Authenticated Communication,” on page 67
□	6. Troubleshoot any authentication-related issues.	Section B.3.8, “Troubleshooting Authentication Problems,” on page 68

NOTE

- You can create and deploy authentication certificates for your agents and central computers either before or after installing Agent Manager.
- You can enable authentication at any time after installing Agent Manager. However, ensure you issue and install all necessary certificates on agent and central computers before enabling authentication.

B.3.1 Certificate Requirements

When you issue agent or central computer certificates for authentication, ensure all certificates meet the following requirements:

- The certificate is an X.509 certificate.
- The certificate has an Client Authentication (`1.3.6.1.5.5.7.3.2`), a Server Authentication (`1.3.6.1.5.5.7.3.1`) Enhanced Key Usage (EKU), or both.
- The certificate has a private key.
- The certificate has the EXCHANGE key specification, including a public/private key pair used to encrypt session keys so they can be safely stored and exchanged with other users.

NOTE: For added security, NetIQ also recommends you ensure the certificate was issued by one of the certification authorities listed in the `TrustedIssuerSubjectNames` configuration property.

B.3.2 Issuing and Installing Agent Authentication Certificates

If you want to configure authentication for Agent Manager agent computers, each agent needs to present a trusted certificate to the central computer that monitors the agent. You must install agent certificates in the `NetIQ Agent Manager` container of the `Local Computer` certificate store on each agent computer.

Agent certificates should include the Client Authentication EKU, object identifier (OID) `1.3.6.1.5.5.7.3.2`, and must be trusted by the central computer. You can establish trust by placing all issuer certificates from the certificate chain of the agent certificate in the `Trusted Root Certification Authorities` container of the `Local Computer` certificate store on the central computer.

NOTE

- You can install the agent authentication certificate by logging directly into the agent computer using an account that is a member of the local Administrators group or by remotely deploying the certificate to one or more agent computers, depending on your environment and PKI.
- If you have multiple certificates with the Client Authentication EKU stored in the `NetIQ Agent Manager` container in the `Local Computer` certificate store, Agent Manager uses the first valid certificate and ignores any additional certificates.
- You can configure agent computers to search other certificate stores and locations for certificates, if required by your PKI. For more information about configuring certificate stores, see Section B.3.6, "Customizing Certificate Usage," on page 65.
- If the agent is configured to use an authentication certificate and is unable to access the associated private key, the agent service fails to start and the agent computer generates an event 21334 in the Application event log.

To issue and install agent authentication certificates:

1. ***If you have not configured a certificate authority for your environment,*** establish a certificate authority (CA) to issue agent authentication certificates. Ensure your certificate authority can issue agent computer certificates that meet all authentication requirements. For more information about certificate requirements, see Section B.3.1, "Certificate Requirements," on page 61.

   NOTE

   - If all agents and central computers are internal to your company, NetIQ recommends you use a local CA. If any Agent Manager computers are hosted externally, you should purchase a commercial certificate.
   - You can use Microsoft Certificate Services or another CA to issue certificates, as configured in your environment.

2. Use your certificate authority to issue one or more agent computer certificates.
3. Install the agent computer certificate in the `NetIQ Security Manager` container of the `Local Computer` certificate store on the agent computer.
4. ***If the issuer certificate for the agent certificate is not already installed on the agent,*** install the issuer certificate in the `Trusted Root Certification Authorities` container of the `Local Computer` certificate store.

5 Repeat Step 3 on page 62Step 4 on page 62 on each agent computer where you want to configure authentication.

6 ***If the issuer certificate for the agent certificate is not already installed on the central computer that monitors the agents you want to authenticate,*** install the issuer certificate in the `Trusted Root Certification Authorities` container of the `Local Computer` certificate store of the central computer.

B.3.3 Issuing and Installing central computer Authentication Certificates

If you want to configure authentication for Agent Manager central computers, each central computer needs to present a trusted certificate to all monitored agent computers. You must install central computer certificates in the `LocalMachine > NetIQ Security Manager` certificate store on each central computer.

central computer certificates should include the Server Authentication EKU, OID `1.3.6.1.5.5.7.3.1`, and must be trusted by all monitored agent computers. You can establish trust by placing all issuer certificates from the certificate chain of the central computer certificate in the `Trusted Root Certification Authorities` container of the `Local Computer` certificate store on each monitored agent computer.

NOTE

- You can install the central computer authentication certificate by logging directly into the central computer using an account that is a member of the local Administrators group or by remotely deploying the certificate to one or more central computers, depending on your environment and PKI.
- If you have multiple certificates with the Server Authentication EKU stored in the `NetIQ Security Manager` container in the `Local Computer` certificate store, Agent Manager uses the first valid certificate and ignores any additional certificates.
- You can configure central computers to search other certficate stores and locations for certificates, if required by your PKI. For more information about configuring certificate stores, see Section B.3.6, “Customizing Certificate Usage,” on page 65.
- If you configure central computer authentication and do not establish trust with all monitored agents, your agents cannot communicate with the untrusted central computer.

To issue and install central computer authentication certificates:

1 ***If you have not configured a certificate authority for your environment,*** establish a certificate authority (CA) to issue central computer authentication certificates. Ensure your certificate authority can issue agent computer certificates that meet all authentication requirements. For more information about certificate requirements, see Section B.3.1, “Certificate Requirements,” on page 61.

NOTE: You can use Microsoft Certificate Services or another CA to issue certificates, as configured in your environment.

2 Use your certificate issuer to issue one or more central computer certificates.

3 Install the central computer certificate in the `NetIQ Security Manager` container of the `Local Computer` certificate store on the central computer.

4 ***If the issuer certificate for the central computer certificate is not already installed on the central computer,*** install the issuer certificate in the `Trusted Root Certification Authorities` container of the `Local Computer` certificate store.

5 Repeat Step 2 on page 63Step 4 on page 63 on each central computer where you want to configure authentication.

6 ***If the issuer certificate for the central computer certificate is not already installed on the agent computer you want to authenticate the central computer,*** install the issuer certificate in the `Trusted Root Certification Authorities` container of the `Local Computer` certificate store of the agent computer.

7 Repeat Step 6 on page 64 on each monitored agent computer.

B.3.4 Enabling Agent Authentication

After creating and installing a valid certificate on your agent computers and installing the issuer certificate for the agent computer on the monitoring central computer, you can enable agent authentication on the central computer by editing the registry.

If you enable agent authentication, you restrict your central computer to only be able to communicate with agents that present valid, trusted Client Authentication certificates.

To enable agent authentication on a central computers:

1 Log on to the central computer using an account that is a member of the local Administrators group.

2 Update the following registry entry using the Registry Editor:

```
HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\Agent
Manager\Configurations\ConfigurationGroupName\Operations\Consolidator\RequireP
eerCerts = 1
```

Where *ConfigurationGroupName* is the name of your configuration group.

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

3 Open the Services Administrative Tool located in the Control Panel.

4 In the Services pane, click **Agent Manager Service**.

5 On the Action menu, click **Restart**.

6 After the service restarts, close the Services Administrative Tool.

NOTE: If you want to enable agent authentication on a central computer that has a 64-bit version of Microsoft Windows installed, update the following registry key using the Registry Editor:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NetIQ\Security
Manager\Configurations\ConfigurationGroupName\Operations\Consolidator\RequirePeerCer
ts = 1
```

B.3.5 Enabling central computer Authentication

After creating and installing a valid certificate on your central computer and installing the issuer certificate for the central computer on all monitored agent computers, you can enable central computer authentication on your agents by editing the registry on each agent computer.

If you enable central computer authentication, you restrict your agent computers to only be able to communicate with a central computer that presents a valid, trusted Server Authentication certificate.

To enable central computer authentication on an agent computer:

1. Log on to the agent computer using an account that is a member of the local Administrators group.
2. Update the following registry entry using the Registry Editor:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\NETIQ\Security
   Manager\Configurations\ConfigurationGroupName\Operations\Agent\Consolidator\Re
   quirePeerCerts = 1
   ```

   Where *ConfigurationGroupName* is the name of your configuration group.

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

3. Open the Services Administrative Tool located in the Control Panel.
4. In the Services pane, click **Agent Manager Service**.
5. On the Action menu, click **Restart**.
6. After the service restarts, close the Services Administrative Tool.
7. Repeat Step 1 on page 65Step 6 on page 65 on each agent computer.

NOTE: If you want to enable central computer authentication on a central computer that has a 64-bit version of Microsoft Windows installed, update the following registry key using the Registry Editor:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NETIQ\Security
Manager\Configurations\ConfigurationGroupName\Operations\Agent\Consolidator\RequireP
eerCerts = 1
```

B.3.6 Customizing Certificate Usage

Agent Manager uses several registry values to configure the default certificate store location, certificate store name, certificate name, and names of trusted issuers. You can modify the following default registry values to configure how Agent Manager finds agent and central computer authentication certificates.

The agent registry values are in the following location in the registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\Security
Manager\Configurations\ConfigurationGroupName\Operations\Agent\Consolidators
```

Where *ConfigurationGroupName* is the name of your current configuration group.

The central computer registry values are in the following location in the registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\Security
Manager\Configurations\ConfigurationGroupName\Operations\Consolidator
```

Where *ConfigurationGroupName* is the name of your current configuration group.

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

Registry Value	Registry Data Type	Default Value Data	Definition
`CertificateStoreLocation`	String	`LocalMachine`	Specifies the location of the certificate store containing the agent or central computer authentication certificate. This property determines whether Agent Manager searches the local computer, current user, or service-specific store to find Agent Manager certificates. Possible values are `LocalMachine`, `CurrentUser`, or `Service:`*ServiceName*, where *ServiceName* is the name of the specific service.
`CertificateStoreName`	String	`NetIQ Security Manager`	Specifies the name of the certificate store containing the agent or central computer authentication certificate. Possible values are `NetIQ Security Manager`, `My`, `Root`, or *CustomCertificateStoreName*, where *CustomCertificateStoreName* is a customized certificate store you create.
`CertificateSubjectName`	String	[EMPTY]	Specifies the subject distinguished name of the specific agent or central computer authentication certificate. If empty, the agent uses the first certificate found with a Client Authentication EKU, and the central computer uses the first certificate found with Server Authentication EKU.

Registry Value	Registry Data Type	Default Value Data	Definition
RequirePeerCerts	DWORD	0	Specifies whether or not the computer is configured to establish trust for the certificate an agent or central computer presents, depending on the computer type, when trying to connect. If the computer is not configured to trust a certificate received from another computer, the computer cannot communicate with the other computer. For more information about enabling authentication, see Section B.3.4, “Enabling Agent Authentication,” on page 64 and Section B.3.5, “Enabling central computer Authentication,” on page 64.
TrustedIssuerSubjectNames		[EMPTY]	Specifies a list of issuers Agent Manager trusts. Agent Manager uses this list when validating certificates. If you want to restrict Agent Manager to only trust certificates issued by certain issuers, you can specify a semicolon-separated list of subject distinguished names for certificate issuers you want to trust. For example, if you want to only trust certificates issued by the `Agent Manager Trusted Root` certification authority, specify `CN=NetIQ Agent Manager Trusted Root`.

B.3.7 Verifying Authenticated Communication

The Sentinel Web console devices view shows the authentication status of agents using the Authentication Mode and Authenticated columns. **Authenticated** shows `yes` when authentication of the device is required, and the device is properly authenticated.

Authentication mode displays one of the following values:

Not Applicable

The value for the Central Computer, because the central computer has no need to authenticate itself or be authenticated by itself.

Agent Authenticates Central Computer

The value when the agent computer requires authentication, but the central computer does not.

Central Computer Authenticates Agent

The value when the central computer requires authentication, but the agent computer does not.

Mutual Authentication

The value when both the agent computer

and the central computer require authentication.

Authentication not required

The value when neither the agent

nor the central computer require authentication.

B.3.8 Troubleshooting Authentication Problems

If one or more agents and central computers cannot communicate, you may not have configured authentication correctly. If an agent or central computer does not present a certificate, presents an invalid certificate, or presents a certificate issued by an untrusted certificate issuer, Agent Manager cannot enable authenticated communication.

An authentication error is not the only possible cause of faulty communication between an agent and a central computer. Other network, software, and hardware problems can also cause the failure of communication between agents and central computers. Before you attempt to correct authentication problems, verify that the communication problem is actually caused by an authentication error.

If the error was caused because a computer was offline when a certificate was presented, the central computer and agent computer automatically attempt to present certificates to one another, as applicable depending on your configuration, at the next communication attempt.

Verifying Authentication Certificates

After ruling out network, software, and hardware problems as the cause of faulty communication between one or more agents and central computers, ensure all agent and central computer authentication certificates are valid and are installed in the `NetIQ Security Manager` container of the `Local Computer` certificate store.

To verify an authentication certificate:

1. Log on to the agent or central computer using an account that is a member of the local Administrators group.
2. Start **Microsoft Management Console**.
3. On the File menu in the Console window, click **Add/Remove Snap-in**.
4. Click **Add**.
5. Select **Certificates**.
6. Click **Add**.
7. Select **Computer account**.
8. Click **Next**.
9. Select **Local computer (the computer this console is running on)**.
10. Click **Finish**.
11. Click **Close**.
12. Click **OK**.

13 On the File menu, click **Save**.

14 Specify a location on the computer for the `.msc` file and click **Save**.

15 In the left pane of the Console window, expand **Certificates (Local Computer) > NetIQ Security Manager**.

16 In the left pane, click **Certificates**.

17 ***If the Certificates folder is missing or does not contain an authentication certificate,*** issue and install a new agent or central computer authentication certificate.

For more information about installing agent authentication certificates, see Section B.3.2, "Issuing and Installing Agent Authentication Certificates," on page 62. For more information about installing central computer authentication certificates, see Section B.3.3, "Issuing and Installing central computer Authentication Certificates," on page 63.

NOTE: By default, the `NetIQ Security Manager` container of the `Local Computer` certificate store on the central computer contains the self-signed certificate `NetIQ Security Manager Server`, which Agent Manager uses to enable communication between the central computer and agents. This default certificate is not a Server Authentication certificate.

18 ***If the Certificates folder contains an authentication certificate,*** complete the following steps:

18a In the right pane, double-click the authentication certificate.

18b On the General tab, ensure the certificate details are correct and that the certificate has a corresponding private key.

18c Click the Certification Path tab.

18d ***If the certificate status is*** *This certificate is OK*, click **OK**.

18e ***If the certificate status is not*** *This certificate is OK*, re-issue and install a new agent or central computer authentication certificate. For more information about installing agent authentication certificates, see Section B.3.2, "Issuing and Installing Agent Authentication Certificates," on page 62. For more information about installing central computer authentication certificates, see Section B.3.3, "Issuing and Installing central computer Authentication Certificates," on page 63.

19 Close the Microsoft Management Console.

Verifying Trust of the Certificate Issuer

If the authentication certificate installed on your agent or central computer is valid, ensure the computer to which the agent or central computer presents a certificate trusts the certificate issuer. The issuer certificate must be installed in the `Trusted Root Certification Authorities` container of the `Local Computer` certificate store on the authenticating computer.

To verify an authenticating computer trusts a certificate issuer:

1 Log on to the authenticating agent or central computer using an account that is a member of the local Administrators group.

2 Start **Microsoft Management Console**.

3 On the File menu in the Console window, click **Add/Remove Snap-in**.

4 Click **Add**.

5 Select **Certificates**.

6 Click **Add**.

7 Select **Computer account**.

8 Click **Next**.

9 Select **Local computer (the computer this console is running on)**.

10 Click **Finish**.

11 Click **Close**.

12 Click **OK**.

13 On the File menu, click **Save**.

14 Specify a location on the computer for the `.msc` file and click **Save**.

15 In the left pane of the Console window, expand **Certificates (Local Computer) > Trusted Root Certification Authorities**.

16 In the left pane, click **Certificates**.

17 ***If the Certificates folder does not contain the issuer certificate,*** install the certificate chain for the authentication certificate issuer in the `Trusted Root Certification Authorities` container.

18 ***If the Certificates folder contains the issuer certificate,*** complete the following steps:

18a In the right pane, double-click the issuer certificate.

18b On the General tab, ensure the issuer certificate details are correct.

18c Click the Certification Path tab.

18d ***If the certificate status is*** *This certificate is OK*, click **OK**.

18e ***If the certificate status is not*** *This certificate is OK*, re-install the certificate chain for the authentication certificate issuer in the `Trusted Root Certification Authorities container`.

19 Close the Microsoft Management Console.

B.4 Using Agent Manager with FIPS-Compliant Security Algorithms Enabled

Agent Manager takes advantage of the Federal Information Processing Standards (FIPS)-compliant security features available in Microsoft Windows to allow you to further secure your environment.

You can enable FIPS-compliant security algorithms only when monitoring Windows agents using Agent Manager version 6.5 or later. If you enable the `System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing` local security policy on your central computer, that central computer can no longer communicate with certain components of Agent Manager:

- UNIX agents
- iSeries agents

Agent Manager does not support communication with legacy agents because the existing legacy agent communication protocol does not meet the requirements necessary to use the FIPS 140-2 Inside logo.

After you enable this setting, your central computer can communicate with Windows agents using only Agent Manager 6.5 or later.

NOTE: If you want to use FIPS-compliant security algorithms, NetIQ recommends that you enable the FIPS-compliant local security policy on all domain controllers in your environment.