Secure Configuration Manager Windows Agent

Installation and Configuration Guide

January 2018

Legal Notice

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see http://www.netiq.com/company/legal/.

Copyright © 2018 NetIQ Corporation. All Rights Reserved.

For information about NetIQ trademarks, see http://www.netiq.com/company/legal/. All third-party trademarks are the property of their respective owners.

About This Book

The *Installation and Configuration Guide* provides conceptual information about the Secure Configuration Manager Windows Agent. This book includes instructions for upgrading, installing, and deploying the agent. It also provides guidance for managing the supported endpoints.

- Chapter 1, “Introducing the Windows Agent,” on page 9
- Part II, “Deploying or Installing Agents,” on page 35
- Part III, “Managing Endpoints,” on page 47

Intended Audience

This book provides information for individuals responsible for installing or deploying security agents to Windows servers and workstations, as well as managing the endpoints that the agents manage.

Additional Documentation

The Secure Configuration Manager documentation library includes the following resources:

- *Secure Configuration Manager Installation Guide*
- *User's Guide for Secure Configuration Manager*
- *Security Agent for UNIX Installation and Configuration Guide*
- *Secure Configuration Manager SCAP Module User's Guide*
- *GRC Manager for Secure Configuration Manager User’s Guide*
- *Help* in the consoles, which provide context-sensitive information and step-by-step guidance for common tasks

For the most recent version of this guide and other Secure Configuration Manager documentation resources, visit the Secure Configuration Manager website.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the **comment on this topic** link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care at https://www.microfocus.com/support-and-services/.

Contents

About This Book 3

1 Introducing the Windows Agent 9

Part I Planning to Install or Deploy Agents 11

2 Checklist for Installing and Updating Agents 13

3 Understanding Installation, Deployment, and Updates 15

Understanding Agent Registration . . . 15
Installing or Updating an Agent on a Local Computer . . . 15
Installing or Updating Agents on Remote Computers . . . 16
Understanding the Deployment Agent . . . 16
Deploying to Untrusted or High-Security Domains . . . 17
Uninstalling Remote Agents . . . 17

4 Requirements and Considerations for the Windows Agent 19

Windows Agent Computer Requirements . . . 19
Considerations for Managing the Windows Agent Environment . . . 20
Windows Agent Caching Requirements . . . 21
Deployment Requirements . . . 22
Permissions Requirements . . . 23

5 Understanding Windows Agent Behavior 25

Understanding Windows Agent Communication . . . 25
Understanding Port Requirements . . . 25
Understanding Firewall Requirements . . . 26
Understanding FIPS Communication . . . 26
Understanding the Windows Agent Service . . . 27
Changing the Agent Service Account Settings . . . 27
Changing the Automatic Recovery Settings . . . 27

6 Understanding Endpoint Management 29

Understanding Licensing . . . 29
Understanding Management by Proxy . . . 29
Proxy Limitations . . . 30
Proxy Requirements . . . 30
Setting Up Proxy Agents . . . 31
Improving Agent Performance when Managing Endpoints by Proxy . . . 31
Match Endpoints to Agents . . . 31
Install an Appropriate Ratio of Agents to Managed Endpoints . . . 32
Reduce Agent CPU Usage . . . 33
Adjust Endpoint Firewall Settings to Ensure Accurate Security Check Reporting . . . 34

Part II Deploying or Installing Agents 35

7 Installing or Updating Agents on Remote Computers 37

Identifying Agent Packages for Deployment . . . 37
Scheduling and Reporting Agent Deployment . . . 37
Installing or Updating an Agent on Remote Computers . . . 38
Installing a New Windows Agent . . . 38
Updating a Windows Agent . . . 39

8 Installing or Updating an Agent on a Local Computer 41

Using the Setup Program to Install . . . 41
Using the Command Line to Install . . . 43
Using the Setup Program to Update an Agent . . . 44
Uninstalling the Windows Agent . . . 44

Part III Managing Endpoints 47

9 Managing Active Directory Endpoints 49

Active Directory Endpoint Deployment Checklist . . . 49
Planning Active Directory Endpoint Deployment . . . 49
Active Directory Endpoint Requirements . . . 50
Adding Active Directory Endpoints in Secure Configuration Manager . . . 50

10 Managing Microsoft IIS Endpoints 53

Microsoft IIS Endpoint Deployment Checklist . . . 53
Planning Microsoft IIS Endpoint Deployment . . . 54
Microsoft IIS Endpoint Requirements . . . 54
Adding IIS Endpoints in Secure Configuration Manager . . . 54
Enabling NetIQ VBscripts . . . 55

11 Managing NAS Server Endpoints 57

NAS Server Endpoint Deployment Checklist . . . 57
Planning NAS Server Endpoint Deployment . . . 57
NAS Server Endpoint Requirements . . . 58
Adding NAS Server Endpoints in Secure Configuration Manager . . . 58

12 Managing Oracle Endpoints 61

Oracle Endpoint Deployment Checklist . . . 61
Planning Oracle Endpoint Deployment . . . 61
Oracle Endpoint Requirements . . . 62
Adding Oracle Endpoints in Secure Configuration Manager . . . 62

13 Managing Microsoft SQL Server Endpoints 65

Microsoft SQL Server Endpoint Deployment Checklist . . . 65
Planning Microsoft SQL Server Endpoint Deployment . . . 66
Microsoft SQL Server Endpoint Requirements . . . 66
Adding SQL Server Endpoints in Secure Configuration Manager . . . 66

14 Managing Network Device Endpoints 69

Network Device Endpoint Deployment Checklist 69
Planning Network Device Endpoint Deployment. 70
Network Device Endpoint Requirements 70
Adding Network Device Endpoints in Secure Configuration Manager 70

1 Introducing the Windows Agent

The **NetIQ Secure Configuration Manager Windows Agent** (Windows agent) validates the configuration of Windows endpoints managed by NetIQ Secure Configuration Manager to ensure compliance with corporate security policies and pinpoint potential vulnerabilities. An endpoint represents an agent-monitored operating system, application, web server, or database instance.

The Windows agent can monitor the operating system of the computer where you install the agent as well as the following types of assets in your Windows environment:

- Microsoft Active Directory
- Microsoft Internet Information Services (IIS)
- Microsoft SQL Server database instances
- Network Attached Storage (NAS) servers
- Network devices
- Oracle database instances
- Windows operating systems

The Windows agent can collect security compliance information from one or more Windows endpoints. The Windows agent receives requests from Secure Configuration Manager Core Services and runs commands or responds by returning data, status, or results. The Windows agent can run locally on computers throughout your enterprise or you can install the Windows agent locally on a few computers and have those agents manage by proxy endpoints on many other computers. The **NetIQ Security Agent for Windows service** (Windows agent service) must be enabled to run on the Windows agent computer. For more information about the Windows agent service, see “Understanding the Windows Agent Service” on page 27.

When you install a Windows agent, you can add the computer on which the agent resides to the Secure Configuration Manager asset map. Secure Configuration Manager registers the new Windows agent and assigns an endpoint to the agent representing the operating system of the agent computer. As you add more systems and endpoints to the asset map, you can designate the endpoint type. For example, you can specify one new endpoint as Active Directory and another as SQL Server. A single Windows agent can monitor multiple types of endpoints. For more information about monitoring multiple endpoints, see “Understanding Management by Proxy” on page 29. For more information about discovering and adding endpoints to your managed systems in the asset map, see the *User’s Guide for Secure Configuration Manager*.

Each Windows agent sends regular communication, called a **heartbeat**, to Secure Configuration Manager to verify operation. When the agent receives a heartbeat request, the agent polls its monitored endpoints to verify their status and then responds to Secure Configuration Manager. The Windows agent also responds to requests for data sent from Core Services in the form of security checks and policy templates. Policy templates are groups of security checks that audit a specific series of IT controls that match a security policy standard. The agent translates the security checks into queries which it forwards to its monitored endpoints. Upon receiving responses to the queries, the agent reports the results to Secure Configuration Manager. For more information about Secure Configuration Manager, see the *User’s Guide for Secure Configuration Manager*.

Planning to Install or Deploy Agents

This section helps you understand the requirements and processes for installing and deploying agents.

- Chapter 2, “Checklist for Installing and Updating Agents,” on page 13
- Chapter 3, “Understanding Installation, Deployment, and Updates,” on page 15
- Chapter 4, “Requirements and Considerations for the Windows Agent,” on page 19
- Chapter 5, “Understanding Windows Agent Behavior,” on page 25
- Chapter 6, “Understanding Endpoint Management,” on page 29

2 Checklist for Installing and Updating Agents

To install and update your Windows agents on local and remote computers, complete the following steps.

	Checklist Items
❑	1. Decide which types of endpoints you want the Windows agent to manage. For the most current information about supported endpoint versions, see the NetIQ Secure Configuration Manager Technical Information page.
❑	2. Determine whether you want to manage some endpoints by proxy or to place an agent on each computer containing one or more endpoints. For more information, see “Understanding Management by Proxy” on page 29.
❑	3. Ensure that the computers where you want to install the Windows agent can communicate with Core Services and with all endpoints that you want to manage by proxy. For more information, see “Understanding Windows Agent Communication” on page 25.
❑	4. Determine whether you want to install your Windows agents locally or use the Windows console for Secure Configuration Manager to deploy to the target computers. For more information, see Chapter 8, “Installing or Updating an Agent on a Local Computer,” on page 41 and Chapter 7, “Installing or Updating Agents on Remote Computers,” on page 37.
❑	5. Start the required services on the agent computers and computers to be managed by proxy. For more information, see “Understanding Management by Proxy” on page 29.
❑	6. (Conditional) When you want to deploy to remote computers but Core Services cannot access the network or domain, use the local installation process to place a Deployment Agent in the network or domain before deploying additional agents. For more information, see “Understanding the Deployment Agent” on page 16 and “Installing or Updating Agents on Remote Computers” on page 16.
❑	7. (Conditional) To install or update the Windows agent locally, complete the following steps: 1. Ensure that your environment meets all specified requirements for installing the agent. For more information, see Section 4, “Requirements and Considerations for the Windows Agent,” on page 19. 2. Ensure that you have the appropriate credentials to install or update the local agent. For more information, see “Permissions Requirements” on page 23. 3. Run the setup program or use the command line for silent installation. For more information, see Chapter 8, “Installing or Updating an Agent on a Local Computer,” on page 41.

	Checklist Items
❑	8. (Conditional) To install or update Windows agents on remote computers, complete the following steps: 1. Ensure that your environment meets all specified requirements for installing or updating the agent on the target computers. For more information, see Section 4, “Requirements and Considerations for the Windows Agent,” on page 19 and “Deployment Requirements” on page 22. 2. Ensure that Core Services and the Deployment Agent can communicate with the target computers. For more information, see “Understanding Windows Agent Communication” on page 25. 3. (Conditional) To upgrade the agents from a version older than 6.1, run the *Asset Details and Discovery* scheduled job to ensure that Secure Configuration Manager has the appropriate agent domain and computer names. 4. Ensure that the Deployment Agent has appropriate permissions for deploying to the target computers. For more information, see “Understanding the Deployment Agent” on page 16. 5. Ensure that you have access to the packages you want to deploy. For more information, see “Identifying Agent Packages for Deployment” on page 37. 6. Install or update the agents using the deployment feature in the Windows console for Secure Configuration Manager. For more information, see Chapter 7, “Installing or Updating Agents on Remote Computers,” on page 37.

3 Understanding Installation, Deployment, and Updates

You can choose to install and update the Windows agent on each local computer or use the Deployment wizard in the Windows console for Secure Configuration Manager to push the agent installation and updates out to multiple computers concurrently. Each installation provides the capabilities to audit, report, and analyze the following Windows agent components:

Component	Installs support for...
Microsoft IIS	Managing Microsoft Internet Information Services (IIS) endpoints
Microsoft SQL Server	Managing Microsoft SQL Server endpoints
Oracle	Managing an Oracle database running on a Windows system
Windows Agent	Managing Windows, Active Directory, NAS Server, and network device endpoints

- "Understanding Agent Registration" on page 15
- "Installing or Updating an Agent on a Local Computer" on page 15
- "Installing or Updating Agents on Remote Computers" on page 16
- "Uninstalling Remote Agents" on page 17

When you install or upgrade Secure Configuration Manager, the setup program automatically includes a Windows agent on the Core Services computer.

For more information about the endpoint versions currently supported by the Windows agent, see the NetIQ Secure Configuration Manager Technical Information page.

Understanding Agent Registration

You can use a LocalSystem account or specify a different account for the NetIQ Security Agent for Windows service (Windows agent service). During installation, when you provide the name or IP address of the Secure Configuration Manager Core Services computer, the installation process automatically registers the installed agent with Core Services. You can also specify the ports used by the agent to communicate with Secure Configuration Manager. For more information about the agent service account, see "Changing the Agent Service Account Settings" on page 27. For more information about ports, see "Understanding Port Requirements" on page 25.

Installing or Updating an Agent on a Local Computer

The Windows agent installation and update packages include an `.msi` file from which you can either run a setup wizard or perform a local, silent installation from the command line. The setup wizard walks you through the configuration settings for the Windows agent. The command line option enables you to specify the setting for installing on the local computer without user intervention. For

more information about installing with the setup program, see “Using the Setup Program to Install” on page 41. For more information about silent installation, see “Using the Command Line to Install” on page 43.

NOTE

- The local installation process does not include the capability for deploying the agent package to remote computers. You must use the Windows console for Secure Configuration Manager for remote deployment.
- If you want to manage systems in domains other than the domain for the Core Services computer, you must locally install at least one agent in that domain. For more information, see “Understanding the Deployment Agent” on page 16 and “Deploying to Untrusted or High-Security Domains” on page 17.

Installing or Updating Agents on Remote Computers

Secure Configuration Manager enables you to install agents on remote computers and push service packs and hotfixes to existing Windows agents. This deployment process minimizes the time required to install and update agents in your environment. By using Deployment Agents you can also install and update agents in untrusted domains or highly secure networks.

NOTE: To use the deployment process for updating an existing Windows agent, the agent must be version 6.1 or later.

For more information about using the deployment feature, see “Installing or Updating an Agent on Remote Computers” on page 38.

Understanding the Deployment Agent

By default, the deployment process uses port 700 and TLS with Diffie-Hellman protocol for communication between Core Services and the target computer. Moreover, Secure Configuration Manager provides the **Deployment Agent** function to establish a more secure connection between Secure Configuration Manager components during agent installation and updates. When you initiate deployment, Core Services passes instructions securely to the Deployment Agent over the designated ports. Then the Deployment Agent communicates with the target computer over port 700 using TLS with Diffie-Hellman. For more information about ports, see “Understanding Port Requirements” on page 25.

NOTE: If Secure Configuration Manager is in FIPS 140-2 mode, it uses TLS 1.1 for communication with the Windows agent.

Any Windows agent registered with Core Services can be a Deployment Agent. By default, Secure Configuration Manager uses the agent installed on the Core Services computer as the Deployment Agent. However, you can select additional Windows agents to serve as the Deployment Agent by enabling the **Is Deployment Agent** option in the Agent Component Properties window. You must have a Deployment Agent in each domain where you want to install or update agents. You must also specify a fully qualified host name for the Windows endpoint that represents the Deployment Agent. Otherwise, Core Services cannot use the agent for deployment.

The Deployment Agent also reduces the need for specifying credentials when installing and updating agents on remote computers. During deployment, you must have appropriate permissions, such as Local or Domain Administrator permissions, to modify the target computer. You can use the credentials of the Windows agent service that serves as the Deployment Agent. If a particular Deployment Agent does not have proper permissions, you can specify a separate set of credentials for accessing the remote computers. For more information about permissions, see “Permissions Requirements” on page 23.

Secure Configuration Manager also uses the Deployment Agent to enable discovery of new systems in Active Directory. For more information about system and endpoint discovery, see the *User’s Guide for Secure Configuration Manager*.

Deploying to Untrusted or High-Security Domains

If you want to use the deployment process to install or update agents in a high-security network or domain, such as a demilitarized zone, you must locally install and register one agent in that network or domain. Secure Configuration Manager marks that first registered agent as the Deployment Agent for the network or domain. The deployment process then uses the secure connection between the Deployment Agent and Core Services to deploy packages to the target computers in the domain.

Uninstalling Remote Agents

You can use the deployment process to uninstall agents on remote computers. You must have a Deployment Agent in the domain where you want to remove the agents. If the Deployment Agent is the only agent in the domain, you must uninstall that agent manually. For more information about uninstalling agents, see “Uninstalling the Windows Agent” on page 44.

4 Requirements and Considerations for the Windows Agent

This section addresses requirements for the Windows agent, including those for the agent computer, the managed environment, and deployment to remote computers.

- “Windows Agent Computer Requirements” on page 19
- “Considerations for Managing the Windows Agent Environment” on page 20
- “Windows Agent Caching Requirements” on page 21
- “Deployment Requirements” on page 22
- “Permissions Requirements” on page 23

Windows Agent Computer Requirements

The following table lists the requirements for a Windows agent computer. For the most recent recommendations, see the NetIQ Secure Configuration Manager Technical Information web page.

Category	Minimum Requirement
Memory	256 MB 384 MG for computers running an Oracle database
Processor	2 Ghz or faster
Free disk space	100 MB 50 MB additional disk space for caching
Operating system	One of the following versions: ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows 10 ◆ Windows 8.1 ◆ Windows 7 (64-bit) ◆ Windows Server 2008 R2 ◆ Windows Server 2008 (32-bit) NetIQ Corporation strongly recommends the Microsoft hotfixes described in the following Microsoft Knowledge Base articles for computers on which you plan to install Windows agents, whether remotely or manually: ◆ Microsoft Knowledge Base Article 2649868 (applies to Windows 7 and Windows Server 2008 R2)

Category	Minimum Requirement
Additional software	All of the following products: ◆ Microsoft Group Policy Management Console on all endpoint computers that you want to audit for Group Policy Object settings ◆ IIS Management Scripts and Tools component on the endpoint computers running Internet Information Services (IIS) version 7 or 7.5 that you want to monitor

To ensure a successful installation, you must configure a Windows temporary folder for the environment variable TEMP. If you deleted the Windows temporary folder associated with the environment variable, you must create a new temporary folder. For more information about environment variables, see your Microsoft Windows documentation.

To create a new temporary folder:

1. Find the Windows environment variable for the temporary folder and make note of the **Variable value**, such as `%USERPROFILE%\Local Settings\Temp`.

   In most Windows operating systems, you can find the variable in **System Properties > Advanced**.
2. Create a new Windows temporary folder, using the directory path and folder you noted from the environment variable's **Variable value** field.

Considerations for Managing the Windows Agent Environment

When planning the systems you want the Windows agent to manage and where you want to install a Windows agent, consider the following:

- Only one agent can be installed on each physical or virtual computer.
- At least one agent must be installed per WAN. The agent must reside at the remote end of the network so requests between the service and the managed computers are executed over a local area network.
- At least one agent must be installed per domain. The agent can manage computers in the same domain by proxy. For more information, see "Understanding Management by Proxy" on page 29.

  NOTE: For optimal performance, install at least one agent per 50 managed computers in a domain. Performance might vary depending on processor speeds, memory, locations, and network bandwidth. The size of reports and how frequently you run them also affects performance.
- Administrative permissions must be set. Configure the Windows agent service to run with full administrative access to the local computer and domain. For more information, see "Permissions Requirements" on page 23.
- To successfully run security checks for Windows patch assessments, ensure that the following programs are running on the endpoint computers that you want to assess:
  - Windows Update or Automatic Updates service, depending on the operating system
  - Windows Update Agent 7.4 or later

  Secure Configuration Manager does not require specific settings for these Windows services.

- (Conditional) When installing the agent on a local computer, the Workstation service must be running.
- (Conditional) If you want Secure Configuration Manager to receive and display IPv6 addresses from managed endpoints, the agent computer must be running Windows Server 2003 or a later operating system. Also, the Windows agent must be set up as a dual-stack host to support both IPv4 and IPv6 addresses. The agent uses IPv4 addresses when communicating with Core Services. For more information about agent operating systems, see “Windows Agent Computer Requirements” on page 19.
- (Conditional) If an endpoint uses only an IPv6 address, that endpoint must be managed by Windows proxy. For more information, see “Proxy Requirements” on page 30.
- (Conditional) To use the Effective Policy object to audit Group Policy Object (GPO) settings, ensure that your environment meets the following requirements:
  - The Windows agent computer should run the same operating system as the endpoint computer that the agent monitors. Using computers that run the same operating systems ensures a consistent name and path convention for the reported GPOs. The names and paths for GPOs vary by Microsoft operating system. For example, if you used a computer running Windows Server 2008 to edit and distribute GPOs to a domain controller, you should query all endpoints in that domain from an agent running on a Windows Server 2008 computer. Otherwise, the names of or paths to reported GPOs on an endpoint computer might not match the names and paths for the same GPOs on the agent computer. For more information, see “Match Endpoints to Agents” on page 31.
  - The Windows agent computer should run the same operating system as the computer from which you deployed the GPOs to ensure a consistent name and path convention for the reported GPOs.
  - The Windows agent service account must have Administrative permissions on the endpoint to collect GPO settings information. That is, the service account cannot run as the Local System account on queried endpoints.

Windows Agent Caching Requirements

The Windows agent uses caching features to enhance performance. The following types of data are persisted in the agent:

- Users - Local, Domain, and Active Directory users
- Groups - Global groups and Active Directory groups
- OUs - Active Directory only
- Password Hashes - Local, Domain, and Active Directory user passwords

It is important that you plan for the disk space needed to store this information in the agent. Use the following guide to calculate how much space is needed:

- Users - 1 KB per user
- Groups - 1 KB per group
- OUs - 1 KB per OU
- Password Hashes - 1 KB per 4 users

Other factors that affect caching storage space include numbers of events and the types of reports you are running. Additionally, if you manage endpoints by proxy, the number of managed endpoints affects the amount of disk space used.

In addition to the space reserved for caching information, the agent also uses the cache for temporary storage while processing reports and actions. The first time you run reports, the agent may require more time to collect data for the reports. In addition, it may take a few minutes for recently completed actions to be reflected in subsequent reports. The agent automatically cleans up this disk usage during normal processing. Allocate 20 MB of working space for the agent to use for normal processing.

Deployment Requirements

When you use the Deployment feature in the Windows console for Secure Configuration Manager to push the agent installation or updates to remote computers, ensure that your environment meets the following requirements:

- Your console account must have the following permissions:
  - Access IT Assets
  - Remote Deploy and Install
  - Remote Uninstall
  - Run Security Checks

  For more information about managing console permissions, see the *User's Guide for Secure Configuration Manager*.
- The computer from which you deploy agents, such as the Deployment Agent computer, must be running the following Windows services:
  - DHCP client (if the computer uses DHCP)
  - Server service
  - Workstation service
- The target computers to which you are deploying the agent software must be running the Remote Registry service.
- The Deployment Agent and target computers must support communication through network and personal computer firewalls. For more information about required firewall settings, see "Understanding Firewall Requirements" on page 26.
- Port 700 must be open for outbound communication on the deploying computer, such as the Deployment Agent computer, and for inbound communication on the target computer. For more information about default ports, see "Understanding Port Requirements" on page 25. For more information about the Deployment Agent, see "Understanding the Deployment Agent" on page 16.
- If the target computers reside in a domain outside the Core Services computer or in a secure network, such as a demilitarized zone, you must locally install at least one Windows agent in that domain or network. Once registered with Core Services, the locally installed agent becomes the Deployment Agent for that network or domain. For more information about the Deployment Agent, see "Understanding the Deployment Agent" on page 16.

Permissions Requirements

If you are installing agents only on the local computer, you must have Administrator permissions on that computer. You can log on either with a domain administrator account or as a local administrator.

When you install or update agents on remote computers, the Windows agent service account on the Deployment Agent computer must have Administrator permissions for the target computers. The agent service account can either be a member of the Domain Admins group or you can add the account to the Administrators local group of the target computer. You also need remote access to the file system (for example, through the admin share) and remote access to the registry through the Remote Registry Service. For more information about the Deployment Agent, see “Installing or Updating Agents on Remote Computers” on page 16.

To run the Windows agent service, the Log On As service account you specify during installation or update must have the “Log on as a service” permission on the agent computer. If you change the service account to a local account from a domain one, or vice versa, after the installation or update, the Windows agent service might not restart on systems where the new account does not have the required permission by default.

5 Understanding Windows Agent Behavior

This section provides an explanation of the Windows agent service as well as how the agent communicates with Core Services and endpoints.

- "Understanding Windows Agent Communication" on page 25
- "Understanding the Windows Agent Service" on page 27

Understanding Windows Agent Communication

The Windows agent must be able to send requests to and receive requests from Core Services and all endpoints managed by proxy. When a request from Core Services cannot reach the Windows agent, Secure Configuration Manager makes multiple attempts to connect before reporting a communication failure. For more information about Core Services retry attempts, see the *User's Guide for Secure Configuration Manager* and the Core Services Configuration Utility help.

The Windows agent communicates with Core Services using encrypted SSL protocol.

- "Understanding Port Requirements" on page 25
- "Understanding Firewall Requirements" on page 26
- "Understanding FIPS Communication" on page 26

Understanding Port Requirements

Open the ports listed in the following table to ensure proper communication among the Windows agent, Core Services, Secure Configuration Manager consoles, and remote computers. The ports must also be open to ensure communication through network and personal computer firewalls. For more information about communicating with remote computers, see "Deployment Requirements" on page 22 and "Understanding Management by Proxy" on page 29. For more information about required firewall settings, see "Understanding Firewall Requirements" on page 26.

Port Number	Component Computer	Port Use
700	◆ Deployment agent computer ◆ Remote computer	During deployment, used by the Deployment Agent and target computers for inbound and outbound communications.
1622	◆ Agent computer	Used by the Windows agent computer to listen for communications from Core Services.
1626	◆ Core Services computer	Used by the Core Services computer to listen for communication from Security Agent for Windows 5.8 Service Pack 2 or older.
1627	◆ Core Services computer	Used by the Core Services computer to listen for communication from the Windows agent.

Understanding Firewall Requirements

In general, network and personal computer firewalls can block data transmission when you deploy the agent and during day-to-day communications among the agent, endpoints, and Secure Configuration Manager Core Services.

Ensure that your environment meets the following requirements for communicating through firewalls:

- When using a high-security firewall in a network, such as for a demilitarized zone, install agents on the same side of the firewall as the endpoints and install Core Services on the other side of the firewall.
- When you deploy the agent to a remote computer, File and Printer Sharing must be enabled in the Windows firewall settings on the remote computer.
- Enable Remote Administration and Windows Remote Management in the Windows firewall settings for inbound and outbound communication on endpoints managed by proxy. Typically, firewall settings do not include exceptions for the proxy agent, which blocks the agent from gathering data and might cause security checks to report endpoints as Offline. Enabling Remote Administration and Windows Remote Management in the firewall settings for endpoints ensures more accurate security check reporting of your endpoints.

Understanding FIPS Communication

Secure Configuration Manager supports Federal Information Processing Standard (FIPS) 140-2 communication among the product components, including between the Windows agent and managed endpoints. To configure the Windows agent to function in FIPS communication mode, you can enable the GPO setting for System Cryptography: Use FIPS Compliant Algorithms for Encryption, Hashing, and Signing. You must restart the Windows agent service after you change the GPO setting.

You can also configure the Windows agent to function in FIPS mode without configuring a global setting on the computer. You must restart the agent service when you change the registry setting.

NOTE: You do not need to enable FIPS in the Core Services Configuration Utility for Core Services to communicate with a FIPS-enabled agent. However, to be compliant with FIPS standards, all components must communicate in FIPS mode. For more information, see the *User's Guide for Secure Configuration Manager*.

To configure FIPS mode for the Windows agent only:

1. (Conditional) For a Windows agent running on 64-bit computer, set the following registry key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NetIQ\VigilEnt\vigilent_adapter\useFipsMode (REG_DWORD: 1)
   ```

2. (Conditional) For a Windows agent running on 32-bit computer, set the following registry key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\VigilEnt\vigilent_adapter\useFipsMode (REG_DWORD: 1)
   ```

3. Restart the Windows agent service.

Understanding the Windows Agent Service

The Windows agent service enables the Windows agent to interact with the local computer and endpoints managed by proxy, as well as communicate with Core Services. During local and remote installation, the installation program modifies the following properties for the Windows agent service:

Log on as a service	Grants the “Log on as a service” permission to the Windows agent service account for the local computer
Recovery from failure	Changes the automatic recovery settings for First failure and Second failure to **Restart the Service**

- “Changing the Agent Service Account Settings” on page 27
- “Changing the Automatic Recovery Settings” on page 27

Changing the Agent Service Account Settings

The account for the Windows agent service must have the “Log on as a service” permission to perform queries on the local and proxied agent computers. During agent installation and deployment, you can specify whether the service account logs on as a LocalSystem account or uses a different Windows account. The installation and deployment programs automatically grant the specified account the “Log on as a service” permission to the local computer.

After installation or remote deployment, if you change the service account to a local account from a domain account, or vice versa, the Windows agent service might not restart on systems where the new account does not have the required permission by default. For more information about permissions for the Windows agent service, see “Permissions Requirements” on page 23.

When you specify a Deployment Agent for deployment, the service account on the Deployment Agent must have Administrator permissions for the computers targeted for new agent installation or updates. For more information, see “Installing or Updating Agents on Remote Computers” on page 16.

Changing the Automatic Recovery Settings

To ensure that the Services utility in the Windows Control Panel automatically restarts the Windows agent service after a failure, the agent installation program modifies the automatic recovery settings for the service. The modifications instruct Windows Services to make two attempts at restarting the agent service. By default, each restart attempt occurs one minute after the service failure. The installation program also instructs the Services utility to reset the failure count every 15 minutes. You can change these settings in the Properties window for the Windows agent service.

NOTE

- Although the installation and deployment program specifies a value of 15 minutes for the **Reset fail count after** setting, the Recovery tab on the Properties window for the Windows agent service displays 0 for the setting. This discrepancy occurs because the Properties window allows users to specify values only in increments of days.
- As a best practice, avoid enabling the Services utility to attempt restarts after two failures. Multiple restart attempts can prevent Windows from reporting essential error messages.

---

6 Understanding Endpoint Management

To manage endpoints, the asset on that hosts them must be licensed. The endpoints can be on the same computer as the Windows agent or on a remote computer in a process called **management by proxy**. A computer can host multiple endpoints, which are managed by a single Windows agent.

When you register a Windows agent on a computer, Secure Configuration Manager automatically creates and registers a Windows operating system endpoint that represents the operating system for that computer. You must have a Windows operating system endpoint on the same computer where you manage an Active Directory endpoint. You do not need the Windows operating system endpoint on computers that host IIS, Oracle, SQL Server, and network device endpoint

- “Understanding Licensing” on page 29
- “Understanding Management by Proxy” on page 29
- “Setting Up Proxy Agents” on page 31
- “Improving Agent Performance when Managing Endpoints by Proxy” on page 31

Understanding Licensing

Secure Configuration Manager includes a license key that defines the number of servers, workstations, and network devices that you can manage with this product. While Secure Configuration Manager does not prevent you from exceeding the number of allotted licenses, you should request an updated license key.

For more information about licensing, see the *Secure Configuration Manager Installation Guide*. For more information about obtaining license keys, see your sales representative.

Understanding Management by Proxy

Secure Configuration Manager allows you to manage Windows computers without installing an agent on each computer. A single Windows agent can manage several computers by proxy, as long as the computers are members of the domain in which the agent service is installed. This proxy capability greatly simplifies deployment. Most organizations with large Windows environments use management by proxy to reduce the number of Windows agents to a manageable number.

NOTE: If a Windows endpoint is managed by a proxy agent, the agent returns data with qualifiers (for example, `HOUWIN2KSRV\Administrator`). If a Windows endpoint is not managed by proxy, the agent returns data without qualifiers (for example, `Administrator`).

- “Proxy Limitations” on page 30
- “Proxy Requirements” on page 30

Proxy Limitations

If you plan to manage Windows computers by proxy, you should be aware of certain limitations. The Windows agent cannot perform the following functions by proxy:

- Windows actions and reports
  - List Instant Messenger Applications report
  - Users with Weak Passwords report
  - Users with Password = User Name report
  - Users without a Password report
  - Users with Password Too Short report
  - Set Disk Quota for User action
  - Show User Quota for a Specified Volume report
- Windows security checks
  - Accounts with Password Equal to Any User Name
  - Accounts with Password Equal to User Name
  - Accounts with Password Equal to Reverse User Name
  - Accounts with Short Passwords
  - Accounts with Blank Passwords
  - Instant Messenger Setting
- Queries of the Port object
- Any default port scan reports, such as the Port Scan (TCP/UDP Endpoints) report
- Queries of the HKLM/Current User registry hive or any reports that rely on that hive

Proxy Requirements

To manage a computer by proxy, the service account by which the Windows agent operates must be a member of the Domain Admins group in the domain of the managed computer, and it must be a member of the Local Admins group on the managed computer.

Consider the following additional requirements when using the Windows agent to manage a computer by proxy:

- The agent computer must be running the following services:
  - Workstation
  - DHCP Client
- The Remote Registry Service must be running on all computers being managed by proxy.
- The Microsoft Remote Procedure Call service must be running on both the agent computer and all computers being managed by proxy.
- (Conditional) For Secure Configuration Manager to receive and display IPv6 addresses from managed endpoints, the Windows agent must be set up as a dual-stack host to support both IPv4 and IPv6 addresses because the agent uses IPv4 addresses when communicating with Core Services. For more information about agent operating systems, see “Windows Agent Computer Requirements” on page 19.

- (Conditional) To monitor endpoint computers running IIS version 7.0 or 7.5, you must install the IIS Management Scripts and Tools component on the endpoint. You must also enable NetIQ VBscripts scripts to run on the computer containing the Windows agent monitoring the endpoint. For more information about enabling scripts to run, see “Enabling NetIQ VBscripts” on page 55.
- (Conditional) To collect Group Policy Object data from endpoint computers running the Windows Server 2008 Core or 2008 Core R2 operating system, you must mange those endpoints by proxy. The Core operating systems do not support Group Policy Management Console (GPMC) installation, which the agent requires.

Setting Up Proxy Agents

The Windows console for Secure Configuration Manager enables you to organize proxy agents and their managed endpoints. Use the following checklist as a guide in setting up proxy agents. For more information about optimizing the agent to efficiently manage endpoints, see “Improving Agent Performance when Managing Endpoints by Proxy” on page 31.

	Checklist Items
❑	1. Deploy the Windows agent to the computer that will manage endpoints by proxy. For more information about deployment, see Chapter 7, “Installing or Updating Agents on Remote Computers,” on page 37. Alternatively, manually add the agent to a local computer, and register the agent with Core Services. For more information about manual installation, see Chapter 8, “Installing or Updating an Agent on a Local Computer,” on page 41.
❑	2. Verify that the deployed Windows agent computer is a managed system in the IT Assets list in the Windows console. For more information about adding managed systems to the console, see the *User’s Guide for Secure Configuration Manager* or the console Help.
❑	3. In the Windows console for Secure Configuration Manager, select the Windows agent and then add the endpoints that you want to manage by proxy.

Improving Agent Performance when Managing Endpoints by Proxy

The Windows agent regularly communicates with both its managed endpoints and Core Services. When the agent manages a large number of endpoints by proxy, the agent consumes valuable resources on the computer. The size of reports and how frequently you run them also affects agent performance. This section provides tips for optimizing the Windows agent performance to reduce CPU usage and ensure accurate report results.

- “Match Endpoints to Agents” on page 31
- “Install an Appropriate Ratio of Agents to Managed Endpoints” on page 32
- “Reduce Agent CPU Usage” on page 33
- “Adjust Endpoint Firewall Settings to Ensure Accurate Security Check Reporting” on page 34

Match Endpoints to Agents

As a best practice, the Windows agent should manage endpoints with operating systems similar to the agent computer’s operating system. As Microsoft improves operating system capabilities, older versions might not have the same features as newer versions. For example, Windows Server 2008 does not have the same advanced Audit settings as Windows Server 2012 R2. If you use a Windows

Server 2008 agent to monitor a Windows Server 2012 R2 endpoint, the agent might not report the audit settings accurately. In general, an agent can manage endpoints with older Windows operating system than the agent computer's operating system.

To optimize agent performance, assign endpoints to agents according to the following table.

Agent Computer	Endpoint Managed by Proxy
Windows Server 2016	◆ Windows Server 2016 ◆ Windows Server 2012 R2
Windows Server 2012 R2	◆ Windows Server 2012 R2 ◆ Windows Server 2008 R2 ◆ Windows Server 2008
Windows Server 2008 R2	◆ Windows Server 2008 R2 ◆ Windows Server 2008 ◆ SQL Server 2008
Windows Server 2008	◆ Windows Server 2008 ◆ SQL Server 2008
Windows 10	◆ Windows 10 ◆ Windows 8.1 ◆ Windows 8 ◆ Windows 7
Windows 8.1	◆ Windows 8.1 ◆ Windows 8 ◆ Windows 7
Windows 8	◆ Windows 8 ◆ Windows 7
Windows 7	Windows 7

Install an Appropriate Ratio of Agents to Managed Endpoints

For optimal agent performance, limit the number of endpoints in a domain that a single agent manages. A ratio of 50 endpoints to one Windows agent works well in most environments. Agent performance might vary depending on processor speeds, memory, locations, and network bandwidth on the agent and endpoint computers.

Reduce Agent CPU Usage

You can manage the CPU resources the Windows agent requires by adjusting settings in Secure Configuration Manager and on the agent computer. Review the following methods for optimizing the Windows agent.

- "Schedule Policy Template Runs" on page 33
- "Modify Thread Counts" on page 33
- "Increase the Automatic Polling Interval" on page 34

Schedule Policy Template Runs

When Core Services asks a Windows agent to run a policy template, the agent processes the template for each endpoint the agent manages. If the agent manages 50 endpoints, it is the same as Core Services submitting 50 templates to the agent. The agent then processes the 50 policy templates multiplied by the number of security checks within the template. For example, if the template contains 100 security checks, the agent processes 5,000 checks (50 endpoints x 100 checks). Also, some security checks require more processing time than others. For example, a security check querying a registry value can process more quickly than a check looking at the entitlement for a directory with a large number of files.

By default, the Windows agent must process all policy template queries and respond to Core Services within a two-hour window. If you regularly run large policy templates against a large number of endpoints, you can reduce the likelihood of delays or cancelled policy template runs. In the Windows console for Secure Configuration Manager, schedule the date and time for regular policy template runs to occur when the Windows agent computer is least active.

Modify Thread Counts

You can modify the number of threads the Windows agent and any installed agent components use. If the agent or component consumes too much CPU when processing policy templates, particularly for a large number of endpoints, you might consider increasing the thread count. NetIQ recommends synchronizing the thread counts for the agent and the component to ensure that they have equal processing capability. If you plan to adjust the Windows thread count, you should make the agent thread count match the value selected for the Windows component.

To modify thread counts:

1. Modify the thread count in the SCM GUI:
   - **1a** Go to **IT Assets** > **Agents** > **OS** > **Windows**.

     All the endpoints running on the Windows agent are displayed.
   - **1b** Right-click the endpoint for which you want to modify the thread count, and then select **Properties**.

     Agent Component Properties window is displayed.
   - **1c** Modify the value of the **Maximum Concurrent Requests** field. Default value is 5.

     Click **OK**.
2. Modify the thread count value in the registry keys files:
   - **2a** Open the registry editor using the following command:

     ```
     regedit
     ```

2b Go to the `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NetIQ\VigilEnt\providers\windows` registry.

2c Modify the value of the `threadPoolSize` field.

3 Restart the Windows agent.

Increase the Automatic Polling Interval

The Heartbeat Automatic Polling feature in Secure Configuration Manager ensures Core Services knows whether an agent and its endpoints are active. By default, Core Services sends a heartbeat request every 60 minutes. The agent then forwards the request to all its endpoints to determine their status. If the agent monitors a large number of endpoints, the heartbeat queries can add to the already considerable number of tasks the agent performs at any given moment. For example, the agent might be processing a high volume of queries for a policy template.

To mitigate the number of tasks the agent must perform, you can increase the interval between heartbeat requests. For more information about configuring the Automatic Polling Interval, see the Help for the Core Services Configuration Utility.

Adjust Endpoint Firewall Settings to Ensure Accurate Security Check Reporting

Enable Remote Administration and Windows Remote Management in the Windows firewall settings on all endpoints for inbound and outbound communication. Typically, firewall settings do not include exceptions for the proxy agent, which blocks the agent from gathering data and might cause security checks to report endpoints as Offline. Enabling Remote Administration and Windows Remote Management in the firewall settings for endpoints ensures more accurate security check reporting of your endpoints.

Deploying or Installing Agents

Secure Configuration Manager enables you to install and update the Windows agent on a local system or push the agent package to remote systems using the Deployment wizard in the Windows console.

- Chapter 7, “Installing or Updating Agents on Remote Computers,” on page 37
- Chapter 8, “Installing or Updating an Agent on a Local Computer,” on page 41

7 Installing or Updating Agents on Remote Computers

The Windows console for Secure Configuration Manager provides a convenient and uniform method for installing and updating Windows agents on remote computers. This section includes information about the deployment process and configuring ports for remote deployment.

- "Identifying Agent Packages for Deployment" on page 37
- "Scheduling and Reporting Agent Deployment" on page 37
- "Installing or Updating an Agent on Remote Computers" on page 38

Identifying Agent Packages for Deployment

Secure Configuration Manager requires a special package, stored as a `.nap` file, for installing or updating Windows agents on remote computers. Each package contains a new installation, hotfix, or service pack. Some packages might also include an update for Secure Configuration Manager components. You can download these packages from the NetIQ Secure Configuration Manager Online Support website and copy them to the local Windows console or Core Services computers.

When you install or upgrade the Windows agent on the Core Services computer, the setup program copies the `.nap` file associated with the agent version or update to the `%Program Files%\NetIQ\Secure Configuration Manager\Core Services\SyncStore` folder. The deployment feature automatically lists the packages stored in the `SyncStore` folder. If the package you want to deploy is not stored in the SyncStore folder, the Agent Update wizard enables you to browse to the package's current location. When you select the package, Secure Configuration Manager automatically adds that `.nap` to the SyncStore folder.

NOTE: Some console users might not have access to the files located on the Core Services computer. To work around this issue, maintain a copy of the `.nap` files you want to deploy on the local Windows console computer.

Scheduling and Reporting Agent Deployment

To reduce the impact on performance in your production environment, you can schedule the agent deployment to occur at specified times. For example, you might want to schedule agent installations to occur when the system experiences less traffic, such as early Sunday morning. Alternatively, if you have a large number of agents to update, you might want to schedule the updates for groups of agents to occur at different times.

When the deployment process completes, Secure Configuration Manager creates a report containing the successful and failed results. In the Deployment wizard, you can choose to distribute the report to specified email recipients, a folder, or a file share. Secure Configuration Manager always adds a copy of the completed report to the Completed jobs queue.

Installing or Updating an Agent on Remote Computers

The deployment feature in the Windows console for Secure Configuration Manager enables you to install or update the Windows agent on selected remote computers. Upon successful deployment, Secure Configuration Manager populates the asset map with those agents and their associated systems and endpoints. For more information about assets and the asset map, see the *User's Guide for Secure Configuration Manager*.

Installing or updating agents on remote computers requires permissions, such as Local Administrator permissions, on the target computer. For efficient delivery, you can use the credentials of the Windows agent service running on the Deployment Agent computer. Alternatively, you can specify a separate set of credentials that the Deployment Agent uses to access the target computers.

- "Installing a New Windows Agent" on page 38
- "Updating a Windows Agent" on page 39

Installing a New Windows Agent

Use the deployment feature to install a new Windows agent on a remote computer. For more information about deploying Windows agents, see the Help.

To install agents on remote computers:

1. Download or copy the `.nap` file for the latest Windows agent release to the local computer that hosts the Windows console for Secure Configuration Manager. For more information about the `.nap` file, see "Identifying Agent Packages for Deployment" on page 37.
2. (Conditional) If you are using a firewall, ensure that the settings meet the requirements for communication. For more information, see "Understanding Firewall Requirements" on page 26 and "Deployment Requirements" on page 22.
3. Ensure that the required services are running on the Deployment Agent and target computers. For more information, see "Deployment Requirements" on page 22.
4. Ensure that no other users are running the Deployment wizard in a Windows console for Secure Configuration Manager.
5. Log in to the Windows console with an account that has the required permissions. For more information about console and remote computer permissions, see "Permissions Requirements" on page 23 and "Deployment Requirements" on page 22.
6. Click **Discovered Systems**.
7. In the Discovered Systems content pane, select the systems on which you want to install the Windows agent.
8. Right-click a selected system, and then click **Deploy**.
9. (Optional) To add computers that do not appear in the Discovered Systems pane, complete the following steps:
   - **9a** On the Computers window of the Deployment wizard, click **Add**.
   - **9b** In the Add Computers window, click **Manually Add a Computer**.
   - **9c** Select **New System**.
   - **9d** Specify the domain and computer names.
   - **9e** (Optional) Specify the other settings in the Properties window.

10 Follow the instructions in the wizard until you finish installing the agents on the target computers.

11 Start the following Windows services on the target computers:

- DHCP Client
- Workstation
- (Optional) Windows Update or Automatic Updates service, depending on the operating system

Updating a Windows Agent

Use the deployment feature to upgrade existing Windows agents to the latest release. You can also push hotfixes and service packs to the agents in your asset map.

The deployment process uses the credentials for the agent service account that you specified when you installed the Windows agent. You cannot modify these credentials while deploying an update because the agent service is running on the target computer.

As a best practice, consider updating all Deployment Agents first, before delivering the update to other agents. Updating the Deployment Agents ensures that the agents have any new information that might be required to communicate with Core Services or remote computers. You can update Deployment Agents locally or use the deployment feature in the Windows console for Secure Configuration Manager.

To deploy updates to registered agents:

1 Download or copy the `.nap` file for the latest Windows agent update to the local Windows console computer. For more information about the `.nap` file, see “Identifying Agent Packages for Deployment” on page 37.

2 (Conditional) If you are using a firewall, ensure that the settings meet the requirements for communication. For more information, see “Understanding Firewall Requirements” on page 26 and “Deployment Requirements” on page 22.

3 Ensure that the required services are running on the Deployment Agent and target computers. For more information, see “Deployment Requirements” on page 22.

4 Ensure that no other users are running the Deployment wizard in a Windows console for Secure Configuration Manager.

5 Log in to the Windows console with an account that has the required permissions. For more information about console and remote computer permissions, see “Permissions Requirements” on page 23 and “Deployment Requirements” on page 22.

6 Expand **IT Assets > Agents > OS > Windows**.

7 In the content pane, select the agents that you want to update.

8 Right-click a selected agent, and then click **Deploy or Update**.

9 (Conditional) To update a Deployment Agent, complete the following steps:

9a In the Computers window, select the target agents, and then click **Edit Settings**.

9b For Deployment Method, specify **Use the Existing Agent**.

9c Click **OK**.

10 Follow the instructions in the wizard until you finish updating the agents on the target computers.

8 Installing or Updating an Agent on a Local Computer

This section provides instructions for installing and updating the Windows agent on a local computer. For more information about managing the agent on remote systems, see Chapter 7, “Installing or Updating Agents on Remote Computers,” on page 37.

- “Using the Setup Program to Install” on page 41
- “Using the Command Line to Install” on page 43
- “Using the Setup Program to Update an Agent” on page 44
- “Uninstalling the Windows Agent” on page 44

Using the Setup Program to Install

This section guides you through the process of installing Windows agents using the `NetIQSecurityAgentForWindows.msi` setup program. By default, the setup program uses the local system account for the Windows agent service. You can assign a different account to the agent service to provide different permissions when you run the service. You can also specify the ports that the agent uses to communicate with Secure Configuration Manager. The agent communicates with Secure Configuration Manager Core Services using encrypted SSL protocol.

WARNING: The installation procedure requires the Workstation service to be running, and must be performed locally. Performing the installation from a remote share can cause issues or errors with the installation.

NOTE: Use the setup program only if you are installing the Windows agent for the first time. Use the command line to update an existing version of the Windows agent. For more information about using the command line for installation, see “Using the Command Line to Install” on page 43.

To use the setup program for installing the Windows agent:

1. Log in with an administrator account to the computer on which you want to install the Windows agent components.
2. Start the Workstation service.
3. Run the `NetIQSecurityAgentForWindows.msi` setup program from the root folder of the Windows agent installation kit.
4. In the setup window, click **Next**.
5. Read the license agreement. If you accept the terms of the agreement, select **I accept the terms in the license agreement**, and then click **Next**.

6 (Optional) To specify an account other than LocalSystem for the Windows agent service, complete the following steps:

6a Deselect the **Run agent service as a LocalSystem account** check box.

6b In the **Service Account** field, type the user name of the account you want to assign to the agent service.

NOTE

- The agent service requires an account with administrative permissions to function properly.
- (Conditional) If you start the service within a specific domain, you must specify the domain name using the `domainname\username` format. For example, `AcmeMidWest\smithj`.
- (Conditional) If you specify a local account on a workgroup computer, you must either specify the workgroup name using the `workgroupname\username format`, or type a space in the **User Name** field. Leaving the field blank results in an error.

6c In the **Service Password** field, type the password for the specified service account.

The setup wizard validates the specified service account when you click **Next**.

7 In the **Agent Port** field, specify the port that the Windows agent uses to listen for communications from Secure Configuration Manager Core Services. For more information about ports, see "Understanding Port Requirements" on page 25.

8 (Conditional) If this is a new installation, you can choose where to install the product. If you previously installed a version of the Windows agent on this computer, the setup program installs the product in the previous installation folder.

9 Click **Next**.

10 (Conditional) To automatically register the agent with Secure Configuration Manager, complete the following steps:

10a In the **Core Services Computer** field, specify the DNS name, NetBIOS name, or IP address of the Secure Configuration Manager Core Services computer. For example, type `NQ1234Dev.NetIQ.com` for the DNS name.

10b In the **Core Services Port** field, specify the port that Core Services uses to listen for communications from the agent. If you change the default value of 1627, you must update the Network tab of the Core Services Configuration Utility to match the change.

10c (Optional) To verify that the agent computer can connect to the specified Core Services computer, click **Test Connection**.

11 (Conditional) To register the agent manually later, leave the **Core Services Computer** field blank.

12 Click **Next**. Review your installation selections.

13 Click **Install** to install the product.

14 Click **Finish** to exit the setup program.

15 To enable complete functionality in the Windows agent after installation, on the computers where the agent is installed, start the following Windows services:

- DHCP Client
- Workstation

16 Repeat Step 1 through Step 15 on each computer where you want to install the Windows agent.

17 Verify that each agent is registered with Secure Configuration Manager Core Services. For more information about managing systems and manually registering agents, see the *User's Guide for Secure Configuration Manager*.

18 Check AutoSync updates to ensure that the agent audits the latest security intelligence. For more information about AutoSync, see the *User's Guide for Secure Configuration Manager*.

Using the Command Line to Install

This section guides you through the process of silently installing the Windows agent using the `.msi` file. By default, the `.msi` program uses the LocalSystem account for the Windows agent service. However, you can specify a different account to the Windows agent service to provide different permissions when you run the service. The `.msi` program also includes default values for the installation path and the ports for the agent and Core Services computers, so you do not need to include those parameters in the command line unless you want to specify different values.

To perform a silent installation:

1 Log in to the computer where you want to install the agent.

2 Copy the `NetIQSecurityAgentForWindows.msi` file to the local computer.

3 Open a command prompt with the **Run as administrator** option enabled.

4 (Conditional) If you are installing the Windows agent for the first time, run the following command from the directory containing the `.msi` file:

```
msiexec /i NetIQSecurityAgentForWindows.msi /quiet /lv* Install.log
INSTALLDIR=c:\MyDirectory\Agent CORE_HOST=CoreComputer
```

For example:

```
msiexec /i NetIQSecurityAgentForWindows.msi /quiet /lv* Install.log
INSTALLDIR="c:\NetIQ\SCM Windows Agent" CORE_HOST=hou10mktg.product.com
```

(Conditional) If you are updating an existing version of the Windows agent, run the following command:

```
msiexec /i NetIQSecurityAgentForWindows.msi REINSTALL=ALL REINSTALLMODE=vomus
/quiet /lv* Install.log INSTALLDIR=c:\MyDirectory\Agent CORE_HOST=CoreComputer
```

For example:

```
msiexec /i NetIQSecurityAgentForWindows.msi REINSTALL=ALL REINSTALLMODE=vomus
/quiet /lv* Install.log INSTALLDIR="c:\NetIQ\SCM Windows Agent"
CORE_HOST=hou10mktg.product.com
```

Use the following parameters in the command line.

INSTALLDIR

Specifies the target directory for installation. For example, `c:\NetIQ\SCM Windows Agent`. If you do not include this command, the program uses the `%ProgramFiles%` environment variable, by default the `C:\Program Files` or `C:\Program Files (x86)` folder.

CORE_HOST

Specifies the DNS name, NetBIOS name, or IP address of the Secure Configuration Manager Core Services computer. For example, `hou10mktg.product.com`. If you do not specify a Core Services computer, you must manually register the agent in the Windows console for Secure Configuration Manager.

CORE_PORT

Specifies the port that the Core Services computer uses to listen for communications from the agent. If you do not specify the port, Secure Configuration Manager uses the default port 1627. If you specify a value other than 1627, you must update the Network tab of the Core Services Configuration Utility to match the change.

AGENT_PORT

Specifies the port that the agent computer uses to listen for communications from Secure Configuration Manager Core Services. If you do not specify the port, Secure Configuration Manager uses the default port 1622. If you specify a value other than 1622, you must update the Network tab of the Core Services Configuration Utility to match the change.

SERVICE_ACCOUNT

Specifies the name of the account used to start and run the Windows agent service. For example, `AdminJoeV`. If you do not specify a service account name, Secure Configuration Manager uses the LocalSystem account.

SERVICE_PASSWORD

Specifies the password for the specified Service Account Name. For example, `p@SSw0rd`. If you specify the LocalSystem account, you do not need to specify a password.

5 To enable complete functionality in the Windows agent after installation, on the computers where the agent is installed, start the following Windows services:

- DHCP Client
- Workstation

Using the Setup Program to Update an Agent

If you want to apply a hotfix, service pack, or new version to an existing Windows agent, you can use one of two methods. You can run the setup program for the update on a local agent computer. Alternatively, you can use the Windows console for Secure Configuration Manager to update multiple agent computers concurrently. For more information about distributing the update to multiple agents, see “Installing or Updating Agents on Remote Computers” on page 37. To update a single, local agent computer, complete the following steps.

NOTE: When you upgrade an agent, the setup program keeps the existing agent settings, such as the credentials for the Windows agent service.

To use the setup program for updating a Windows agent:

1 Log in to the agent computer with an administrator account.

2 Run the setup program for the service pack or hotfix from the root folder of the update kit.

3 Follow the instructions until you have finished installing the update.

Uninstalling the Windows Agent

After you uninstall a Windows agent, you should also permanently delete the agent from the list of managed systems in the Windows console for Secure Configuration Manager. Deleting the agent and the system on which the agent resides ensures that the uninstalled agent does not cause a problem with future versions of Core Services. By deleting the agent’s system, you both un-register the agent from Core Services and delete it from your asset map.

NOTE

- Uninstalling the agent software on a computer does not remove the agent from the Secure Configuration Manager asset map or un-register the agent from Core Services. For more information about deleting an agent, see the *User's Guide for Secure Configuration Manager*.
- Before deleting a managed system that hosts an agent, you must remove all attached endpoints. Otherwise, the endpoints will be deleted as well as the agent and the managed system.
- When you use the Windows console for Secure Configuration Manager to uninstall a remote agent that includes the NetIQ® SCAP Module for Windows Agent, the deployment process also uninstalls the module.

You can use one of several methods to remove the Windows agent software from the agent computer:

- On the computer where you installed the Windows agent, use the `NetIQSecurityAgentForWindows.msi` file in the installation kit for the Windows agent.
- On the computer where you installed the Windows agent, use the Control Panel utility for adding and removing programs.
- In the Windows console for Secure Configuration Manager, right-click the Windows agent and then select **Uninstall**. Complete the wizard to remove the agent. You can use the credentials already assigned for the Deployment Agent that runs the uninstallation process or specify credentials that have appropriate permissions for the computer's domain.

Managing Endpoints

This section helps you understand the processes for managing the various Windows-type endpoints.

For the latest list of endpoint versions supported by Secure Configuration Manager, see the NetIQ Secure Configuration Manager Technical Information page or the Release Notes provided with this version.

- Chapter 9, “Managing Active Directory Endpoints,” on page 49
- Chapter 10, “Managing Microsoft IIS Endpoints,” on page 53
- Chapter 11, “Managing NAS Server Endpoints,” on page 57
- Chapter 12, “Managing Oracle Endpoints,” on page 61
- Chapter 13, “Managing Microsoft SQL Server Endpoints,” on page 65
- Chapter 14, “Managing Network Device Endpoints,” on page 69

9 Managing Active Directory Endpoints

The Windows agent 7.0 can manage the following Microsoft Active Directory endpoints:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2008 R2

The Active Directory endpoint type is essentially a subcomponent of the Windows agent, but has the same registration and management functions as the Windows agent, including both local and proxy support. For more information, see “Adding Active Directory Endpoints in Secure Configuration Manager” on page 50.

- “Active Directory Endpoint Deployment Checklist” on page 49
- “Planning Active Directory Endpoint Deployment” on page 49
- “Active Directory Endpoint Requirements” on page 50
- “Adding Active Directory Endpoints in Secure Configuration Manager” on page 50

Active Directory Endpoint Deployment Checklist

Complete the following steps to deploy your Active Directory endpoints.

	Checklist Items
❑	1. Ensure that the Windows agent version supports the Active Directory endpoints you want to manage. For more information, see the NetIQ Secure Configuration Manager Technical Information web page.
❑	2. Ensure that your environment meets the specified requirements for installing the Windows agent. For more information, see “Windows Agent Computer Requirements” on page 19 and “Planning Active Directory Endpoint Deployment” on page 49.
❑	3. Install the Windows agent locally or deploy to remote agent computers, including the Windows Agent component if you are installing the Windows agent manually. For more information, see Chapter 8, “Installing or Updating an Agent on a Local Computer,” on page 41 and Chapter 7, “Installing or Updating Agents on Remote Computers,” on page 37.
❑	4. Add the Active Directory endpoints that you want to manage to the registered Windows agent. For more information, see “Adding Active Directory Endpoints in Secure Configuration Manager” on page 50.

Planning Active Directory Endpoint Deployment

To manage an Active Directory endpoint or group of endpoints, you must install at least one Windows agent in each Active Directory domain. The agent must also run under the domain administrator account.

NOTE: You can assign multiple domain controllers to a single domain, but only one Active Directory endpoint is required per domain. A **domain controller** is a computer that helps manage all aspects of user domain interactions. Some domains have multiple domain controllers.

You can manually add endpoints for your Active Directory instances in Secure Configuration Manager, and then manage those Active Directory instances locally with a Windows agent or using a proxy Windows agent. If you want to manage an Active Directory endpoint by proxy, review the proxy requirements, particularly if the Windows agent does not reside on the domain controller. For more information about proxy requirements, see "Proxy Requirements" on page 30.

Secure Configuration Manager does not allow an endpoint to be monitored by more than one agent on a computer. You must use a unique endpoint name when you add an Active Directory endpoint, otherwise an error will occur. You can use Admin Reports to run a report containing every known agent and its associated system and endpoints. To run this report, select **Tools > Admin Reports > All Systems, Agents, and Endpoints**.

Active Directory Endpoint Requirements

To manage Active Directory endpoints using the Windows agent, ensure that your environment meets the requirements for the Windows agent listed in "Windows Agent Computer Requirements" on page 19.

Adding Active Directory Endpoints in Secure Configuration Manager

Complete the following steps to add Active Directory endpoints that you want to manage with a Windows agent.

To add an Active Directory endpoint:

1. Log in to the Windows console for Secure Configuration Manager.
2. Expand **IT Assets > Agents > OS > Windows**.
3. In the content pane, right-click the Windows agent to which you want to add the Windows Domain or Active Directory endpoint, and then click **Add Endpoint**.
4. Click **Next**.
5. (Optional) To find an existing system on which to add an endpoint, click **Existing Systems**. Select a system, and then click **OK**.
6. In the **Name** field, type a name for the endpoint.

   NOTE: The endpoint name must be different from the original Windows Machine endpoint name. In addition, you must enter an endpoint name that does not already exist on the computer, because Secure Configuration Manager does not allow an endpoint to be monitored by more than one agent. For more information, see "Planning Active Directory Endpoint Deployment" on page 49.
7. For **Endpoint Type**, select **Active Directory**.
8. Click **IP Lookup** to look up the IP address of the endpoint or type the IP address in the **IP Address** field.

   Secure Configuration Manager supports IPv4 and IPv6 addresses.

9 In the endpoint properties table, verify or type the following required information.

Field	Description
Host Name	Name of the computer where the Windows Domain or Active Directory endpoint resides.
IP Address	IP address of the computer where the Active Directory endpoint resides. Secure Configuration Manager supports IPv4 and IPv6 addresses.

10 (Optional) To add more information about the endpoint, complete the following endpoint properties.

Field	Description
Contact Email	Email address of the contact person.
Contact Name	Name of the designated contact person.
Domain Name	Name of the Windows or Active Directory domain.
Importance	Criticality level of the endpoint.
Is DHCP Client	Whether this computer has its IP address dynamically assigned by a DHCP server.
License Type	Product for which you are licensing this endpoint.
Location	Location of the computer hardware.
Major Version	Major version of the operating system.
Minor Version	Minor version of the operating system.
Notes	Descriptive notes about the endpoint.
Service Pack	Microsoft Service Pack applied to the Windows operating system.
Time Zone	Time zone in which the computer hardware is located.
Use	Description for the usage of the computer.

11 (Optional) To add the endpoint to a group, complete the following steps:

11a Click **Add Endpoint to a Group**, and then click **Groups**.

11b To add the endpoint to an existing group, select the group.

11c To add a new group for the endpoint, enter the new group name and description, and then click **Create New Group**.

11d Click **Finish** to return to the Define Endpoint window.

12 (Optional) To add more than one endpoint, click **Add Endpoint**. Repeat Step 5 through Step 11 for each endpoint that you want to add.

13 Click **Finish**.

10 Managing Microsoft IIS Endpoints

The Windows agent 7.0 can manage the following Microsoft Internet Information Services (IIS) endpoints:

- 10
- 8.0 (64-bit only)
- 7.5
- 7.0

The IIS endpoint type is essentially a subcomponent of the Windows agent, but has the same registration and management functions as the Windows agent, including both local and proxy support. To report on Microsoft IIS endpoints using a proxy Windows agent, both the proxy endpoint computer and the agent computer must be running IIS.

- "Microsoft IIS Endpoint Deployment Checklist" on page 53
- "Planning Microsoft IIS Endpoint Deployment" on page 54
- "Microsoft IIS Endpoint Requirements" on page 54
- "Adding IIS Endpoints in Secure Configuration Manager" on page 54
- "Enabling NetIQ VBscripts" on page 55

Microsoft IIS Endpoint Deployment Checklist

Complete the following steps to deploy your Microsoft IIS endpoints.

	Checklist Items
❑	1. Ensure that the Windows agent version supports the Microsoft IIS endpoints that you want to manage. For more information, see the NetIQ Secure Configuration Manager Technical Information web page.
❑	2. Ensure that your environment meets the specified requirements for installing the Windows agent and the IIS component. For more information, see "Windows Agent Computer Requirements" on page 19 and "Planning Microsoft IIS Endpoint Deployment" on page 54.
❑	3. Install the Windows agent locally or deploy to remote agent computers, including the IIS component if you are installing the Windows agent manually. For more information, see Chapter 8, "Installing or Updating an Agent on a Local Computer," on page 41 and Chapter 7, "Installing or Updating Agents on Remote Computers," on page 37.
❑	4. Add the IIS endpoints that you want to manage to the registered Windows agent. For more information, see "Adding IIS Endpoints in Secure Configuration Manager" on page 54.

Planning Microsoft IIS Endpoint Deployment

To manage a Microsoft IIS endpoint or group of endpoints, you must install at least one Windows agent in the domain.

The Windows proxy agent supports a maximum of 50 instances of Microsoft IIS from a single service. You can manually add endpoints for your IIS instances in Secure Configuration Manager, and then manage those IIS instances locally with a Windows agent or using a proxy Windows agent.

Secure Configuration Manager does not allow an endpoint to be monitored by more than one agent on a computer. You must use a unique endpoint name when you add an IIS endpoint, otherwise an error will occur. You can use Admin Reports to run a report containing every known agent and its associated system and endpoints. To run this report, select **Tools > Admin Reports > All Systems, Agents, and Endpoints**.

Microsoft IIS Endpoint Requirements

To manage Microsoft IIS endpoints using the Windows agent, ensure that your environment meets the requirements for the Windows agent listed in "Windows Agent Computer Requirements" on page 19. For more information about which versions of Microsoft IIS the Windows agent can support, see the NetIQ Secure Configuration Manager Technical Information web page.

NOTE: To monitor endpoint computers running IIS version 7.0 or 7.5, you must install the IIS Management Scripts and Tools component on the computer. You must also enable NetIQ VBscripts scripts to run on the computer containing the Windows agent monitoring the endpoint. For more information about enabling scripts to run, see "Enabling NetIQ VBscripts" on page 55.

Adding IIS Endpoints in Secure Configuration Manager

Complete the following steps to add IIS endpoints that you want to manage with a Windows agent.

To add IIS endpoints to an existing agent in Secure Configuration Manager:

1. Log in to the Windows console for Secure Configuration Manager.
2. Expand **IT Assets > Agents > OS > Windows**.
3. In the content pane, right-click the Windows agent to which you want to add the endpoint, and then click **Add Endpoint**.
4. Click **Next**.
5. (Optional) To find an existing system on which to add an endpoint, click **Existing Systems**. Select a system and click **OK**.
6. In the **Name** field, type a name for the endpoint.

   NOTE: Secure Configuration Manager does not allow an endpoint to be monitored by more than one agent, so you must enter an endpoint name that does not already exist on the computer. For more information, see "Planning Microsoft IIS Endpoint Deployment" on page 54.

   ---

7. For **Endpoint Type**, select **IIS**.
8. Click **IP Lookup** to look up the IP address of the endpoint or type the IP address in the **IP Address** field. Secure Configuration Manager supports IPv4 and IPv6 addresses.

9 In the endpoint properties table, verify or type the following required information.

Field	Description
Host Name	Name of the computer where the IIS endpoint resides.
IP Address	IP address of the computer where the IIS endpoint resides. Secure Configuration Manager supports IPv4 and IPv6 addresses.

10 (Optional) To add more information about the endpoint, complete the following endpoint properties.

Field	Description
Contact Email	Email address of the contact person.
Contact Name	Name of the designated contact person.
Importance	Criticality level of the endpoint.
Is DHCP Client	Whether this computer has its IP address dynamically assigned by a DHCP server.
License Type	Product for which you are licensing this endpoint.
Location	Location of the computer hardware.
Major Version	Version of IIS that the endpoint is running.
Notes	Descriptive notes about the endpoint.
Service Pack	Microsoft Service Pack applied to the Windows operating system.
Time Zone	Time zone in which the computer hardware is located.
Use	Description for the usage of the computer.

11 (Optional) To add the endpoint to a group, complete the following steps:

11a Click **Add Endpoint to a Group**, and then click **Groups**.

11b To add the endpoint to an existing group, select the group.

11c To add a new group for the endpoint, enter the new group name and description, and then click **Create New Group**.

11d Click **Finish** to return to the Define Endpoint window.

12 (Optional) To add more than one endpoint, click **Add Endpoint**. Repeat Step 6 through Step 11 for each endpoint that you want to add.

13 Click **Finish**.

Enabling NetIQ VBscripts

To ensure that Windows agent computers can run queries on IIS version 7.0 and 7.5 endpoints, you must ensure that local and domain group policies allow NetIQ VBscripts to run.

To enable NetIQ VBscripts:

1 (Conditional) To create a local policy, log on with a local administrator account to the computer where you want to create the new software restriction policy.

2. (Conditional) To create a domain group policy, log on with a domain administrator account to the domain controller where you want to create the new software restriction policy.
3. Open the group policy editor for the local computer or the domain group policy object (GPO).
4. In the policy editor, navigate to **Security Settings\Software Restriction Policies\Additional Rules**.
5. Right-click **Additional Rules**, and then select **New Certificate Rule**.
6. Click **Browse**, and then navigate to the `NetIQ Corporation.cer` file in the `Vulnerability Manager Agent` folder, by default the following location:

   `\%Program Files%\NetIQ\Secure Configuration Manager\NetIQ Security Agent for Windows`
7. Click **Open**.
8. For Security level, select **Unrestricted**.
9. Click **OK** to enable the new software restriction policy.

11 Managing NAS Server Endpoints

The Windows agent 7.0 can manage the Network Attached Storage (NAS) device NetApp Filer 7.2.4.

NOTE: To collect data from a NAS device, you must use a Windows proxy agent. For more information about managing by proxy, see “Understanding Management by Proxy” on page 29.

NAS devices provide a cost-effective means of expanding your capacity for data storage and retrieval. These file sharing devices can be contained within a primary server, but they also can exist anywhere on a local area network. You can use multiple networked NAS devices to further extend your data storage capability.

- “NAS Server Endpoint Deployment Checklist” on page 57
- “Planning NAS Server Endpoint Deployment” on page 57
- “NAS Server Endpoint Requirements” on page 58
- “Adding NAS Server Endpoints in Secure Configuration Manager” on page 58

NAS Server Endpoint Deployment Checklist

Complete the following steps to deploy your NAS Server endpoints.

	Checklist Items
❑	1. Ensure that the Windows agent version supports the NAS Server endpoints you want to manage. For more information, see the NetIQ Secure Configuration Manager Technical Information web page.
❑	2. Ensure that your environment meets the specified requirements for installing the Windows agent. For more information, see “Windows Agent Computer Requirements” on page 19 and “Planning NAS Server Endpoint Deployment” on page 57.
❑	3. Install the Windows agent locally or deploy the agent to remote agent computers. For more information, see Chapter 8, “Installing or Updating an Agent on a Local Computer,” on page 41 and Chapter 7, “Installing or Updating Agents on Remote Computers,” on page 37.
❑	4. Add the NAS Server endpoints that you want to manage to the registered Windows agent. For more information, see “Adding NAS Server Endpoints in Secure Configuration Manager” on page 58.

Planning NAS Server Endpoint Deployment

To manage a NAS Server endpoint or group of endpoints, you must install at least one Windows agent in the same domain as the NAS Server.

You can manually add endpoints for your NAS servers in Secure Configuration Manager, and then manage those NAS servers locally using a proxy Windows agent.

Secure Configuration Manager does not allow an endpoint to be monitored by more than one agent on a computer. You must use a unique endpoint name when you add a NAS endpoint, otherwise, an error will occur. You can use Admin Reports to run a report containing every known agent and its associated system and endpoints. To run this report, select **Tools > Admin Reports > All Systems, Agents, and Endpoints**.

NAS Server Endpoint Requirements

To manage NAS Server endpoints using the Windows proxy agent, ensure that your environment meets the requirements described in “Proxy Requirements” on page 30.

Adding NAS Server Endpoints in Secure Configuration Manager

Complete the following steps to add NAS Server endpoints you want to manage with a Windows agent.

To add NAS Server endpoints to an existing agent in Secure Configuration Manager:

1. Log in to the Windows console for Secure Configuration Manager.
2. Expand **IT Assets > Agents > OS > Windows**.
3. In the content pane, right-click the Windows agent to which you want to add the endpoint, and then click **Add Endpoint**.
4. Click **Next**.
5. (Optional) To find an existing system on which to add an endpoint, click **Existing Systems**. Select a system and click **OK**.
6. In the **Name** field, type the name of the target endpoint.

   NOTE: Secure Configuration Manager does not allow an endpoint to be monitored by more than one agent, so you must enter an endpoint name that does not already exist on the computer. For more information, see “Planning NAS Server Endpoint Deployment” on page 57.

7. For **Endpoint Type**, select **NAS Server**.
8. Click **IP Lookup** to look up the IP address of the endpoint or type the IP address in the **IP Address** field. Secure Configuration Manager supports IPv4 and IPv6 addresses.
9. In the endpoint properties table, verify or type the following required information.

Field	Description
Host Name	Name of the computer where the NAS Server endpoint resides.
IP Address	IP address of the computer where the NAS Server endpoint resides. Secure Configuration Manager supports IPv4 and IPv6 addresses.

10 (Optional) To add more information about the endpoint, complete the following endpoint properties.

Field	Description
Contact Email	Email address of the contact person.
Contact Name	Name of the designated contact person.
Importance	Criticality level of the endpoint.
License Type	Product for which you are licensing this endpoint.
Location	Location of the computer hardware.
Major Version	Product name of the particular NAS Server endpoint.
Minor Version	Version number of the NAS Server endpoint.
Time Zone	Time zone in which the computer hardware is located.
Notes	Descriptive notes about the endpoint.

11 (Optional) To add the endpoint to a group, complete the following steps:

11a Click **Add Endpoint to a Group**, and then click **Groups**.

11b To add the endpoint to an existing group, select the group.

11c To add a new group for the endpoint, enter the new group name and description, and then click **Create New Group**.

11d Click **Finish** to return to the Define Endpoint window.

12 (Optional) To add more than one endpoint, click **Add Endpoint**. Repeat Step 6 through Step 11 for each endpoint that you want to add.

13 Click **Finish**.

12 Managing Oracle Endpoints

The Windows agent 7.0 can manage the following Oracle database instances:

- 11g R2
- 11g
- 10g

The Oracle endpoint type is essentially a subcomponent of the Windows agent, but has the same registration and management functions as the Windows agent, including both remote and local support.

- "Oracle Endpoint Deployment Checklist" on page 61
- "Planning Oracle Endpoint Deployment" on page 61
- "Oracle Endpoint Requirements" on page 62
- "Adding Oracle Endpoints in Secure Configuration Manager" on page 62

Oracle Endpoint Deployment Checklist

Complete the following steps to deploy your Oracle endpoints.

	Checklist Items
❑	1. Ensure that the Windows agent version supports the Oracle databases you want to manage. For more information, see the NetIQ Secure Configuration Manager Technical Information web page.
❑	2. Ensure that your environment meets the specified requirements for installing the Windows agent. For more information, see "Windows Agent Computer Requirements" on page 19 and "Planning Oracle Endpoint Deployment" on page 61.
❑	3. Install the Windows agent locally or deploy the agent to remote agent computers. For more information, see Chapter 8, "Installing or Updating an Agent on a Local Computer," on page 41 and Chapter 7, "Installing or Updating Agents on Remote Computers," on page 37.
❑	4. Ensure that your computers meet the specified requirements for Oracle endpoints. For more information, see "Oracle Endpoint Requirements" on page 62.
❑	5. Add the Oracle endpoints that you want to audit to the registered Windows agent. For more information, see "Adding Oracle Endpoints in Secure Configuration Manager" on page 62.

Planning Oracle Endpoint Deployment

Before you begin your Oracle endpoint deployment, read "Deployment Requirements" on page 22. The requirements and guidelines for Windows agent deployment are equally applicable to your Oracle environment.

You can monitor Oracle endpoints with a locally installed Windows agent. To monitor an Oracle endpoint or group of endpoints, you must install at least one Windows agent in the domain.

Secure Configuration Manager does not allow an endpoint to be monitored by more than one agent on a computer. You must use a unique endpoint name when you add an Oracle endpoint, otherwise an error will occur. You can use Admin Reports to run a report containing every known agent and its associated system and endpoints. To run this report, select **Tools > Admin Reports > All Systems, Agents, and Endpoints**.

Oracle Endpoint Requirements

To audit Oracle endpoints using the Windows agent, ensure that your environment meets all of the specified requirements for the Windows agent. For more information, see "Deployment Requirements" on page 22. Oracle endpoints on Windows computers must also meet the following requirements:

- The `dynamic_registration` parameter must be set to `ON`.
- You must install the Oracle 11g database (32-bit) on 32-bit or 64-bit operating system platforms using the Administrator account.
- You must install a Windows agent on the Oracle endpoint.

Adding Oracle Endpoints in Secure Configuration Manager

Complete the following steps to add Oracle endpoints you want to audit with a Windows agent.

To add Oracle endpoints to an existing agent in Secure Configuration Manager:

1. Log in to the Windows console for Secure Configuration Manager.
2. Expand **IT Assets > Agents > OS > Windows**.
3. In the content pane, right-click the Windows agent to which you want to add the endpoint, and then click **Add Endpoint**.
4. Click **Next**.
5. (Optional) To find an existing system on which to add an endpoint, click **Existing Systems**. Select a system and click **OK**.
6. In the **Name** field, type the name of the target endpoint.

   NOTE: Secure Configuration Manager does not allow an endpoint to be monitored by more than one agent, so you must enter an endpoint name that does not already exist on the computer. For more information, see "Planning Oracle Endpoint Deployment" on page 61.

7. For **Endpoint Type**, select **Oracle**.
8. In the endpoint properties table, verify or type the following required information.

Field	Description
Host Name	Name of the computer where the Oracle endpoint resides.
Oracle Instance ID	Alphanumeric ID of the Oracle instance.

Field	Description
User Name	User name for the Oracle authenticated login account or the account being impersonated. The best practice recommendation is to avoid using the Oracle SYS account when adding Oracle endpoints.
Password	Password for the Oracle authenticated login account or the account being impersonated.

9 (Optional) To add more information about the endpoint, complete the following endpoint properties.

Field	Description
Oracle oratab File Path	This field is valid only for instances of Oracle running on UNIX.
Contact Email	Email address of the contact person.
Contact Name	Name of the designated contact person.
Importance	Criticality level of the endpoint.
Location	Location of the computer hardware.
Version	Version of the Oracle database that the endpoint represents.

10 (Optional) To add the endpoint to a group, complete the following steps:

10a Click **Add Endpoint to a Group**, and then click **Groups**.

10b To add the endpoint to an existing group, select the group.

10c To add a new group for the endpoint, enter the new group name and description, and then click **Create New Group**.

10d Click **Finish** to return to the Define Endpoint window.

11 (Optional) To add more than one endpoint, click **Add Endpoint**. Repeat Step 5 through Step 10 for each endpoint that you want to add.

12 Click **Finish**.

13 Managing Microsoft SQL Server Endpoints

The Windows agent 7.0 can manage the following Microsoft SQL Server database instances:

- 2016
- 2014
- 2012
- 2008 R2
- 2008

The SQL Server endpoint type is essentially a subcomponent of the Windows agent, but has the same registration and management functions as the Windows agent, including both remote and local support.

- “Microsoft SQL Server Endpoint Deployment Checklist” on page 65
- “Planning Microsoft SQL Server Endpoint Deployment” on page 66
- “Microsoft SQL Server Endpoint Requirements” on page 66
- “Adding SQL Server Endpoints in Secure Configuration Manager” on page 66

Microsoft SQL Server Endpoint Deployment Checklist

Complete the following steps to deploy your SQL Server endpoints.

	Checklist Items
❑	1. Ensure that the Windows agent version supports the SQL Server endpoints you want to manage. For more information, see the NetIQ Secure Configuration Manager Technical Information web page.
❑	2. Ensure that your environment meets the specified requirements for installing the Windows agent and the SQL Server component. For more information, see “Windows Agent Computer Requirements” on page 19 and “Planning Microsoft SQL Server Endpoint Deployment” on page 66.
❑	3. Install the Windows agent locally or deploy the agent to remote agent computers, including the SQL Server component if you are installing the Windows agent manually. For more information, see Chapter 8, “Installing or Updating an Agent on a Local Computer,” on page 41 and Chapter 7, “Installing or Updating Agents on Remote Computers,” on page 37.
❑	4. Install the Microsoft Data Access Components (MDAC) 2.6 on the Windows agent computer.
❑	5. Add the SQL Server endpoints that you want to audit to the registered Windows agent. For more information, see “Adding SQL Server Endpoints in Secure Configuration Manager” on page 66.

Planning Microsoft SQL Server Endpoint Deployment

Before you begin your Microsoft SQL Server endpoint deployment, read “Deployment Requirements” on page 22. The requirements and guidelines for Windows agent deployment are equally applicable to your SQL Server environment.

You can monitor Microsoft SQL Server endpoints with a locally installed Windows agent or using a proxy Windows agent. To audit a SQL Server endpoint or group of endpoints, you must install at least one Windows agent in the domain. The Windows proxy agent supports a maximum of 50 instances of Microsoft SQL Server from a single agent.

Secure Configuration Manager does not allow an endpoint to be monitored by more than one agent on a computer. You must use a unique endpoint name when you add a SQL Server endpoint, otherwise an error will occur. You can use Admin Reports to run a report containing every known agent on the computer and its associated system and endpoints. To run this report, select **Tools > Admin Reports > All Systems, Agents, and Endpoints**.

Microsoft SQL Server Endpoint Requirements

To audit Microsoft SQL Server endpoints using the Windows agent, ensure that your environment meets all of the specified requirements for the Windows agent. For more information, see “Windows Agent Computer Requirements” on page 19.

In addition to the requirements for the Windows agent, ensure that your environment meets the following specific SQL Server requirements:

- Microsoft Data Access Components (MDAC) 2.6 must be installed on the Windows agent computer.
- If you choose to use the Named Pipes protocol to connect to a SQL Server instance, even if the SQL Server instance is using Mixed Mode authentication, the Windows agent must use an account that can be authenticated to the SQL Server’s domain controller.
- You must specify an sa or equivalent super-user account for the SQL Server authenticated login account when you register the endpoint. Secure Configuration Manager and the Windows agent do not support the least privilege model (LPM).

Adding SQL Server Endpoints in Secure Configuration Manager

Complete the following steps to add SQL Server endpoints you want to audit with a Windows agent.

NOTE: Microsoft Data Access Components (MDAC) 2.6 is required on the Windows agent computer to audit SQL Server endpoints. Secure Configuration Manager checks for MDAC when you add a SQL Server endpoint and displays an error if it is not already installed on the agent computer.

To add SQL Server endpoints to an existing agent in Secure Configuration Manager:

1. Log in to the Windows console for Secure Configuration Manager.
2. Expand **IT Assets > Agents > OS > Windows**.
3. In the content pane, right-click the Windows agent to which you want to add the endpoint, and then click **Add Endpoint**.
4. Click **Next**.

5 (Optional) To find an existing system on which to add an endpoint, click **Existing Systems**. Select a system and click **OK**.

6 In the **Name** field, type a name for the endpoint.

NOTE: Secure Configuration Manager does not allow an endpoint to be monitored by more than one agent, so you must enter an endpoint name that does not already exist on the computer. For more information, see "Planning Microsoft SQL Server Endpoint Deployment" on page 66.

7 For **Endpoint Type**, select **SQL Server**.

8 Click **IP Lookup** to look up the IP address of the endpoint or type the IP address in the **IP Address** field. Secure Configuration Manager supports IPv4 and IPv6 addresses.

9 In the endpoint properties table, verify or type the following required information.

Field	Description
Host Name	Name of the host computer running the SQL Server database.
IP Address	IP address of the database. Secure Configuration Manager supports IPv4 and IPv6 addresses.
Database Protocol	Connection protocol used by the Windows agent to connect to the SQL Server database.
Database Port or Pipe	Property for the database connection protocol specified in the Database Protocol field. ◆ If you selected `TCP/IP`, enter the port number (1433 by default). ◆ If you selected `Named Pipes` and the pipe name is the default `\\.\pipe\sql\query`, enter `sql\query`. Otherwise, enter the full pipe name.
Authentication Mode	Account used by the Windows agent to log in to the SQL Server endpoint. ◆ Select `SQL` to use a SQL Server account (requires mixed-mode) defined in Enterprise Manager. ◆ Select `Current Credentials` to use the Windows-authenticated account defined when you installed the Windows agent. ◆ Select `Use Impersonation` to use another specified Windows authenticated account. This account must be within your domain. Whether you use a SQL Server or Windows authenticated account, ensure that you have added this account to the sysadmin (System Administrators) role in SQL Server Enterprise Manager.
User Name	User name for the SQL Server authenticated login account or the account being impersonated. This field is not required if you selected `Current Credentials` in the Authentication Mode field.
Password	Password for the SQL Server authenticated login account or the account being impersonated. This field is not required if you selected `Current Credentials` in the Authentication Mode field.

Field	Description
Major Version	Version of SQL Server the endpoint is running.

10 (Optional) To add more information about the endpoint, complete the following endpoint properties.

Field	Description
Instance Name	Name of the database instance.
Contact Email	Email address of the contact person.
Contact Name	Name of the designated contact person.
Importance	Criticality level of the endpoint.
License Type	Product for which you are licensing this endpoint.
Location	Location of the computer hardware.
Notes	Descriptive notes about the endpoint.
Time Zone	Time zone in which the computer hardware is located.
Service Pack	Microsoft Service Pack applied to the Windows operating system.
Version	Version of the SQL Server database that the endpoint represents.

11 (Optional) To add the endpoint to a group, complete the following steps:

11a Click **Add Endpoint to a Group**, and then click **Groups**.

11b To add the endpoint to an existing group, select the group.

11c To add a new group for the endpoint, enter the new group name and description, and then click **Create New Group**.

11d Click **Finish** to return to the Define Endpoint window.

12 (Optional) To add more than one endpoint, click **Add Endpoint**. Repeat Step 5 on page 67Step 11 on page 68 for each endpoint that you want to add.

13 Click **Finish**.

14 Managing Network Device Endpoints

The Windows agent 7.0 can manage multiple types of network devices. Secure Configuration Manager categorizes the endpoint as *generic network device* unless it is one of the following routers:

- Cisco IOS 15.0M
- Juniper Junos 10.x
- Juniper Junos 9.x
- Juniper Junos 8.x

NOTE: To collect data from a network device, you must use a Windows proxy agent. For more information about managing by proxy, see “Understanding Management by Proxy” on page 29.

The network device endpoint type is essentially a subcomponent of the Windows agent, but has the same registration and management functions as the Windows agent, but only with proxy support.

- “Network Device Endpoint Deployment Checklist” on page 69
- “Planning Network Device Endpoint Deployment” on page 70
- “Network Device Endpoint Requirements” on page 70
- “Adding Network Device Endpoints in Secure Configuration Manager” on page 70

Network Device Endpoint Deployment Checklist

Complete the following steps to deploy your network device endpoints.

	Checklist Items
❑	1. Ensure that the Windows agent version supports the network device endpoints you want to manage. For more information, see the NetIQ Secure Configuration Manager Technical Information page.
❑	2. Ensure that your environment meets the specified requirements for installing the Windows agent. For more information, see “Windows Agent Computer Requirements” on page 19 and “Planning Network Device Endpoint Deployment” on page 70.
❑	3. Install the Windows agent locally or deploy to remote agent computers, including the Windows Agent component if you are installing the Windows agent manually. For more information, see Chapter 8, “Installing or Updating an Agent on a Local Computer,” on page 41 and Chapter 7, “Installing or Updating Agents on Remote Computers,” on page 37.
❑	4. Add the network device endpoints that you want to manage to the registered Windows agent. For more information, see “Adding Network Device Endpoints in Secure Configuration Manager” on page 70.

Planning Network Device Endpoint Deployment

To manage a network device endpoint or group of endpoints, you must install at least one Windows agent in the domain. Before you begin your network device endpoint deployment, see “Deployment Requirements” on page 22. The requirements and guidelines for Windows agent deployment are equally applicable to network device endpoint deployment.

You can manually add endpoints for your network devices in Secure Configuration Manager, and then manage those network devices using a proxy Windows agent.

Secure Configuration Manager does not allow an endpoint to be monitored by more than one agent. You must use a unique endpoint name when you add a network device endpoint, otherwise an error will occur. You can use Admin Reports to run a report containing every known agent and its associated system and endpoints. To run this report, select **Tools > Admin Reports > All Systems, Agents, and Endpoints**.

Network Device Endpoint Requirements

To manage network device endpoints using the Windows agent, ensure that your environment meets the requirements for the Windows agent listed in “Windows Agent Computer Requirements” on page 19.

For information about the requirements for licensing a network device, see “Understanding Licensing” on page 29.

Adding Network Device Endpoints in Secure Configuration Manager

Complete the following steps to add network device endpoints that you want to manage with a Windows agent.

To add a network device endpoint:

1. Log in to the Windows console for Secure Configuration Manager.
2. Go to **IT Assets > Agents > OS > Windows**.
3. In the content pane, right-click the Windows agent to which you want to add the network device endpoint, and then click **Add Endpoint**.

   Add Endpoints dialog box is displayed.
4. Select the agent component to which you want to add endpoints. Click **Next**.
5. In the Name field, type a name for the endpoint you want to add.

   NOTE: The endpoint name must be different from the original Windows Machine endpoint name. In addition, you must enter an endpoint name that does not already exist on the computer, because Secure Configuration Manager does not allow an endpoint to be monitored by more than one agent. For more information, see “Planning Network Device Endpoint Deployment” on page 70.
6. In the Endpoint Type field, select **Network Device**.

7 In the endpoint properties table, verify or type the following required information.

Field	Description
Protocol	The type of protocol used to connect with the network device - Telnet or SSH.
Authentication Type	This field is displayed only if you have chosen SSH as the protocol. Options are Password and Key. Select Password if you require password-based SSH authentication; select Key if you require key-based SSH authentication.
Network Device Type	Type of the network device for which you are configuring this endpoint. This drop-down list has three options - IOS, JUNOS, and GENERIC. Select IOS if the network device is a Cisco device, JUNOS if it is a Juniper device, and GENERIC if it is any other device.
IP Address	IP address of the network device.
IP Port	The port through which the endpoint interacts with the network device.
User Name	User name to log in to the network device.
Password	This field is displayed only if you have selected Password as the authentication type. Enter the password of the network device.
Key	This field is displayed only if you have selected Key as the authentication type. Specify the private key file path.
Expect Script Name	This field is displayed only if you have selected Generic as the network device type. Specify the name of the scripting file that interacts with the network device.

NOTE: Some fields display default values. However, you can update the values.

8 (Optional) To add more information about the endpoint, specify the following endpoint properties.

Field	Description
Passphrase	This field is displayed only if you have selected SSH as protocol and Key as authentication type. Specify the passphrase for the private key file.
Privilege Password	This field is displayed only if you have selected IOS as the network device type. Specify the privilege password of the network device.
Contact Email	Email address of the contact person.
Contact Name	Name of the designated contact person.
Importance	Criticality level of the endpoint.
License Type	Product for which you are licensing this endpoint.
Location	Location of the computer hardware.
Version	Version of the SQL Server database that the endpoint represents.
Time Zone	Time zone in which the computer hardware is located.
Notes	Descriptive notes about the endpoint.

NOTE: Some fields display default values. However, you can update the values.

9 (Optional) To add the endpoint to a group, perform the following steps:

9a Click **Add Endpoint to a Group**, and then click **Groups**.

9b To add the endpoint to an existing group, select the group.

9c To add a new group for the endpoint, enter the new group name and description, and then click **Create New Group**.

9d Click **Finish** to return to the Define Endpoint window.

10 (Optional) To add more than one endpoint, click **Add Endpoint**. Repeat Step 5 through Step 11 for each endpoint that you want to add.

11 Click **Finish**.