# NetIQ Secure Configuration Manager

## Installation Guide

**April 2016**

## Legal Notice

# Contents

# About This Book and the Library

The installation guide provides planning and installation information for the NetIQ Secure Configuration Manager product (Secure Configuration Manager). This book guides you through the installation process and helps you make the correct decisions for your environment.

## Intended Audience

This book provides information for individuals responsible for installing Secure Configuration Manager.

## Other Information in the Library

The library provides the following information resources:

**UNIX Agent Installation and Configuration Guide**

Provides conceptual information about the NetIQ Secure Configuration Manager UNIX Agent and guides you through the installation and configuration process.

**Windows Agent Installation and Configuration Guide**

Provides conceptual information about the NetIQ Secure Configuration Manager Windows Agent and guides you through the installation and configuration process.

**User Guide**

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

**Help**

Provides context-sensitive information and step-by-step guidance for common tasks, descriptions of reports and actions you can run with the product, and definitions for fields on each window.

# Conventions

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

| Convention | Use |
|---|---|
| **Bold** | ◆ Window and menu items<br>◆ Technical terms, when introduced |
| *Italics* | ◆ Book and CD-ROM titles<br>◆ Variable names and values<br>◆ Emphasized words |
| `Fixed Font` | ◆ File and folder names<br>◆ Commands and code examples<br>◆ Text you must type<br>◆ Text (output) displayed in the command-line interface |
| Brackets, such as [*value*] | ◆ Optional parameters of a command |
| Braces, such as {*value*} | ◆ Required parameters of a command |
| Logical OR, such as *value1* \| *value2* | ◆ Exclusive parameters. Choose one parameter. |

# About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measurable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

## Contacting Sales Support

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

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

## Contacting Technical Support

For specific product issues, please contact our Technical Support team.

| | |
|---|---|
| **Worldwide:** | www.netiq.com/Support/contactinfo.asp |
| **North and South America:** | 1-713-418-5555 |
| **Europe, Middle East, and Africa:** | +353 (0) 91-782 677 |
| **Email:** | support@netiq.com |
| **Web Site:** | www.netiq.com/support |

## Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

# Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, please visit http://community.netiq.com.

# 1 Introduction

NetIQ Secure Configuration Manager helps IT security professionals automate compliance with regulations and internal security policies, and meet the demands of auditors. It allows you to proactively identify and prioritize the remediation of misconfigurations that could lead to security breaches, failed audits, or costly server downtime.



## 1.1 Understanding the Secure Configuration Manager Components

The Secure Configuration Manager environment includes three primary components, as well as security agents and compliance evaluation tools. You can install the components, agents, Security Checkup Results Viewer, and Secure Configuration Manager Dashboard on separate systems.

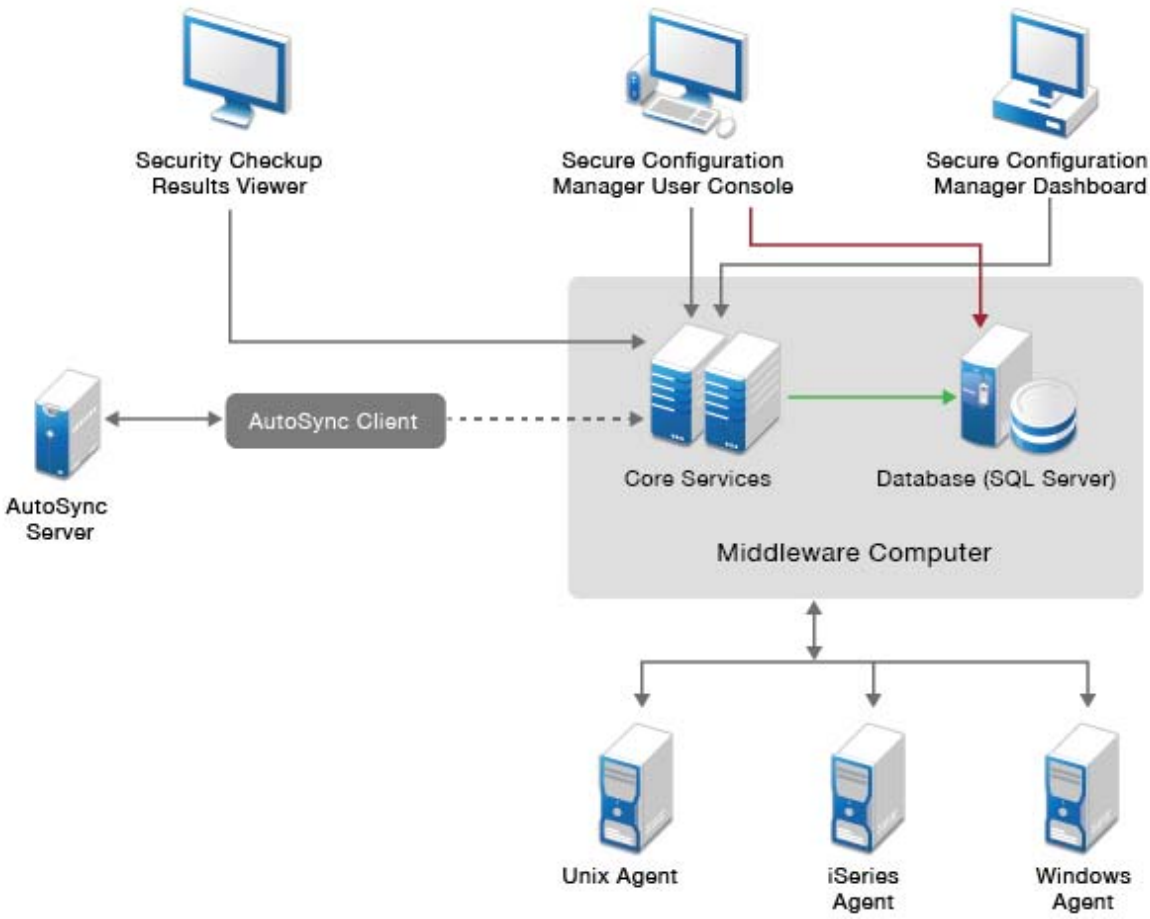
Secure Configuration Manager deploys **agents** to collect information, stores information in a central **database**, and displays reports in the Secure Configuration Manager **console**. Secure Configuration Manager **Core Services** manages communication among the components. Secure Configuration Manager includes the major components listed in the following table.

| Component | Description |
|---|---|
| Agents | Receive requests from Core Services and run commands or respond by returning data, status, or results. Agents run platform-specific software locally on assets throughout your enterprise. |
| Database | Stores product configuration data and results from security checkup reports in Microsoft SQL Server format. |
| Console | Serves as an interface for Secure Configuration Manager so you can perform the following functions:<br>◆ Add, remove, and view your IT resources<br>◆ Execute security checks and run policy templates<br>◆ Remediate policy exceptions<br>◆ Manage jobs<br>◆ Filter information<br>◆ Control automatic AutoSync updates<br>◆ Configure product settings |

| Component | Description |
| --- | --- |
| Core Services | Communicates between agents, the database, and console to perform the following functions:<br>◆ Manage interaction between agents and console<br>◆ Authenticate requests to the agents<br>◆ Receive data from agents and store it in the database<br>◆ Log product activity, security checkup results, and configuration data in the database |
| Dashboard | This Web-based overview of your environment's compliance enables executives and managers to:<br>◆ View the overall compliance of their IT assets<br>◆ Perform a granular assessment of specific groups and computers<br>◆ View the overall posture and trends of security compliance at a single glance<br>For more information about the Dashboard, see the *NetIQ Secure Configuration Manager Dashboard User Guide*. |

# 1.2 Understanding the Secure Configuration Manager Architecture

You can install the Secure Configuration Manager components on separate servers. When planning where to install the components, refer to the following architecture diagram.




The UNIX, iSeries, and Windows security agents have individual installation programs. However, when you install Secure Configuration Manager, the setup program automatically installs a Windows agent on the Core Services computer. You can install the Secure Configuration Manager Dashboard either along with Secure Configuration Manager, or separately. For more information about the security agents and the Secure Configuration Manager, see the respective documentation in the NetIQ Secure Configuration Manager documentation page.

# 2 Planning to Install Secure Configuration Manager

This chapter describes the supported configuration options and requirements for each Secure Configuration Manager component. This chapter also provides links to additional information.



## 2.1 Implementation Checklist

This chapter provides planning information for installation only. If you are upgrading from a previous version, do not use this installation checklist. For more information about upgrading, see Section 5.3, “Upgrading Secure Configuration Manager,” on page 35.

| | **Checklist Items** |
|---|---|
| ❑ | 1. Review product architecture information to learn about Secure Configuration Manager components. For more information, see Section 1.2, “Understanding the Secure Configuration Manager Architecture,” on page 11. |
| ❑ | 2. Decide how you want to configure your component installation. For more information, see Section 2.5.1, “Supported Configurations,” on page 17. |
| ❑ | 3. Ensure that the computers on which you are installing Secure Configuration Manager components meet the specified requirements. For more information, see Section 2.5.3, “Planning to Install Your Database,” on page 20, Section 2.5.4, “Planning to Install Your Core Services,” on page 21, and Section 2.5.5, “Planning to Install Secure Configuration Manager Consoles,” on page 23. |
| ❑ | 4. Ensure that the system environment variables on the Secure Configuration Manager database computer support the installation process. For more information, see “Database Computer Requirements” on page 20. |
| ❑ | 5. Ensure that you have SQL Server or SQL Server Express configured properly to allow Secure Configuration Manager to connect to the database. For more information, see “Planning to Install Secure Configuration Manager” on page 13.<br><br>**IMPORTANT:** Before beginning to install Secure Configuration Manager, close all the windows that are open against Vigilent database in SQL Server Management Studio.<br><br>**NOTE:** NetIQ Corporation recommends using SQL Server Express for trial environments only. To ensure best performance, do not use the Secure Configuration Manager database with SQL Server Express. |
| ❑ | 6. (Optional) Ensure that the computers on which you are installing the Secure Configuration Manager Dashboard meet the specified requirements. For more information, see the *NetIQ Secure Configuration Manager Dashboard User Guide*. |

| | Checklist Items |
|---|---|
| ❑ | 7. Install Secure Configuration Manager. For more information, see Section 3.2, “Installing Secure Configuration Manager Components,” on page 25.<br><br>**NOTE:** (Optional) You can install the Secure Configuration Manager Dashboard while installing Secure Configuration Manager. |
| ❑ | 8. Ensure that the computers to which you are deploying agents meet the specified requirements. For more information, see Section 2.5.6, “Planning to Install Agents,” on page 24. |
| ❑ | 9. Install your agents. For more information, see Section 2.5.6, “Planning to Install Agents,” on page 24. |
| ❑ | 10. (Conditional) If Core Services is not running, start Core Services. For more information, see Section 6.2, “Starting Core Services,” on page 44. |
| ❑ | 11. Start the Secure Configuration Manager console. For more information, see Section 6.3, “Starting the Secure Configuration Manager Console,” on page 44. |
| ❑ | 12. Configure Secure Configuration Manager to work with the agents. For more information, see Section 2.5.6, “Planning to Install Agents,” on page 24. |

## 2.2 Licensing

Secure Configuration Manager requires a license key that defines how many computers or endpoints you can manage with this product. You can install the license key during installation of the product or you can add the license key later using the Core Services Configuration Utility. For more information, see the Help for the Core Services Configuration Utility.

**NOTE:** If you do not enter a valid license key, the installation program automatically applies a 30-day trial license.

The license key defines an expiration date and the number of computers you can manage with Secure Configuration Manager. You can use the Secure Configuration Manager console Tools menu to check the license status of Secure Configuration Manager and the agents. The License Status window shows information such as the number of available licenses, the number of licenses used by registered endpoints, and the expiration date for the licenses.

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 obtaining license keys, see your NetIQ Corporation sales representative.

- Section 2.2.1, “Licensing for iSeries Agents and Endpoints,” on page 15
- Section 2.2.2, “Licensing for UNIX Agents and Endpoints,” on page 15
- Section 2.2.3, “Licensing for Windows Agents and Endpoints,” on page 15

### 2.2.1 Licensing for iSeries Agents and Endpoints

Every iSeries system that you want to manage must host an iSeries security agent. When you register the iSeries agent, Secure Configuration Manager automatically creates and registers an endpoint representing the operating system on the computer. Secure Configuration Manager issues one iSeries endpoint license for the operating system endpoint.

### 2.2.2 Licensing for UNIX Agents and Endpoints

Every UNIX or Linux system that you want to manage must host an UNIX security agent. When you register the UNIX agent, Secure Configuration Manager automatically creates and registers an endpoint representing the operating system on the computer. Secure Configuration Manager issues one UNIX endpoint license for the operating system endpoint. Also, each instance of an Oracle database on the computer requires a separate endpoint and license. For example, a UNIX computer containing six instances of Oracle requires six Oracle endpoint licenses plus an endpoint license for the operating system, for a total of seven licenses.

### 2.2.3 Licensing for Windows Agents and Endpoints

When you register a Windows agent on a computer, Secure Configuration Manager automatically creates and registers an endpoint representing the operating system on the computer. A managed Windows system can include multiple types of Windows endpoints, such as instances of Oracle and SQL Server databases. To manage Windows-based endpoints, consider the following licensing requirements and recommendations.

**Windows Agent Computer**

Requires one Windows Server endpoint license for the operating system of the computer that hosts the agent.

**Active Directory**

Requires one Windows Server endpoint license for each managed Active Directory endpoint. NetIQ Corporation recommends only one Active Directory endpoint per domain.

**Microsoft IIS**

Requires one license for each managed Internet Information Services (IIS) endpoint instance. For example:

- A Windows computer running IIS to manage six Web sites requires one IIS endpoint license. In addition, NetIQ Corporation recommends an endpoint license for the operating system, for a total of two licenses. However, the operating system license is not a requirement.
- A Windows computer with one Windows proxy agent managing six remote Windows computers with 36 Web sites spread evenly across the computers requires six IIS endpoint licenses. In addition, NetIQ Corporation recommends endpoint licenses for the six operating systems, for a total of 12 licenses. However, the operating system licenses are not a requirement.

**NAS Server**

Requires one endpoint license for each NAS device that is running a managed endpoint.

**Oracle**

Requires one endpoint license for each managed instance of an Oracle database. For example, a Windows computer containing six instances of Oracle requires six Oracle endpoint licenses. In addition, NetIQ Corporation recommends an endpoint license for the operating system, for a total of seven licenses. However, the operating system license is not a requirement.

**Microsoft SQL Server**

Requires one endpoint license for each managed SQL Server instance. For example:

- A Windows computer containing six instances of SQL Server requires six SQL Server endpoint licenses. In addition, NetIQ Corporation recommends an endpoint license for the operating system, for a total of seven licenses. However, the operating system license is not a requirement.
- A Windows computer with one Windows proxy agent managing 36 instances of SQL Server spread evenly across six remote Windows computers requires 36 SQL Server endpoint licenses. In addition, NetIQ Corporation recommends endpoint licenses for the six operating systems, for a total of 42 licenses. However, the operating system licenses are not a requirement.

**Network Device**

Requires one endpoint license for each device that is running a managed endpoint.

## 2.3 Permissions Requirements

The following table provides sources for permissions requirements information for the Secure Configuration Manager components and supported agents.

| For permissions information about... | See... |
|---|---|
| Secure Configuration Manager database computer | “Database Computer Requirements” on page 20 |
| Secure Configuration Manager Core Services computer | “Core Services Computer Requirements” on page 22 |
| Secure Configuration Manager console | “Console Computer Requirements” on page 23 |
| Windows agent | *NetIQ Secure Configuration Manager Windows Agent Installation and Configuration Guide* |
| UNIX agent | *NetIQ Secure Configuration Manager UNIX Agent Installation and Configuration Guide* |
| iSeries agent | *NetIQ Security Solutions for iSeries Installation Guide* |

## 2.4 Planning to Install a Trial Environment

If you do not have a valid license key, you can install Secure Configuration Manager for a 30-day trial. You can upgrade a trial environment to full production mode simply by changing the license key. For more information about license keys, see Section 2.2, “Licensing,” on page 14.

As a best practice, NetIQ Corporation recommends creating a trial environment similar to your intended production one. For example, install the database on a separate computer from the Core Services and console computers. However, you can install all components on one computer to run the trial. For more information about selecting the appropriate location to install the components, see

Section 2.5.1, “Supported Configurations,” on page 17. For more information about using Secure Configuration Manager in a trial environment, see the *NetIQ Secure Configuration Manager User Guide*.

# 2.5 Planning Your Secure Configuration Manager Environment

This section provides requirements, details of supported configurations, and other information necessary for planning your Secure Configuration Manager installation environment. For the most recent information, see the Secure Configuration Manager Web page.



## 2.5.1 Supported Configurations

For small enterprises of 50 computers or fewer, you can install all Secure Configuration Manager components on one computer. You can then install additional consoles on other computers as needed. Installing all required components on one computer is not a recommended configuration for most production networks.

---

**NOTE:** An all-in-one configuration is supported for Windows Server 2008, Server 2008 R2, Server 2012, and Server 2012 R2. You can install Secure Configuration Manager consoles on Windows Vista, but you must install Core Services and the Secure Configuration Manager database on separate computers.

---

For larger enterprises, install Core Services and the Secure Configuration Manager database on separate computers. Then install the console on multiple additional computers to manage the agents and other Secure Configuration Manager components.

Installing Secure Configuration Manager components on domain controllers is neither recommended nor supported for the following reasons:

- When you create a local group on a domain controller, the end result is a domain group. The local group needed to handle authentication is not created.
- This configuration can also cause performance issues because the domain controller is very busy even if you do not install Secure Configuration Manager components on that computer.

## Support for Non-English Language Operating System and Database Versions

Secure Configuration Manager supports Microsoft Windows in English, French, German, and Spanish, and Microsoft SQL Server and Microsoft SQL Server Express in United States - English. Ensure that the language version for the Microsoft Windows operating system is the same across all computers where you install the console, Core Services, and database.

## Multiple Core Services

You also have the option to install Core Services on multiple computers. In this configuration, you must install a separate Secure Configuration Manager database for each Core Services computer.

To install Secure Configuration Manager in the multiple Core Services setup, please contact Technical Support.

Having multiple Core Services allows you to divide managed resources, or endpoints, into **managed groups** based on business units or other organizational needs. Resources managed by one Core Services computer are completely separate from resources managed by a different Core Services. This configuration may be appropriate if your organization needs to maintain a high level of internal security. For more information, see “Multiple Core Services Requirements” on page 22.

Depending on the agents you are deploying, you may be able to share registered agents between Core Services. For more information, see Section 3.3, “Working with Multiple Core Services,” on page 27.

## FIPS Communication

Secure Configuration Manager supports Federal Information Processing Standard (FIPS 140-2) communication among the product components. FIPS 140-2 standards regulate the implementation and communication of cryptographic software. Users working under FIPS guidelines must have Secure Configuration Manager function within a secure FIPS-enabled environment. For more information about configuring components for FIPS communication, see the *NetIQ Secure Configuration Manager User Guide* and the security agent guides.

---

**NOTE:** When you enable Secure Configuration Manager to function in a FIPS-enabled environment, Core Services cannot communicate with iSeries security agents.

---

## AutoSync Client

The Secure Configuration Manager **AutoSync service** lets you regularly download the latest security knowledge from an update service Web site to ensure that the Secure Configuration Manager agents always audit with the latest security intelligence. The **Autosync client** queries and receives updates from the NetIQ AutoSync server. For more information, see the *NetIQ Secure Configuration Manager User Guide*.

You can install the AutoSync client on your Core Services computer, or you can install the standalone AutoSync client separately from Core Services.

Install a standalone AutoSync client when your Core Services computer is not directly connected to the Internet, or if you do not want the Core Services computer to download from the Internet. For more information about the standalone AutoSync client, see Section 3.4, “Deploying the Standalone AutoSync Client,” on page 28.

## 2.5.2 Default Ports

Open the ports listed in the following table on the firewall for proper communication between Secure Configuration Manager components.

| Port Number | Component Computer | Port Use |
|---|---|---|
| 700 | Security Agent for Windows (Deployment Agent) | Used by the Deployment Agent and remote computer during deployment. |
| 1433 | Database | Used by Microsoft SQL Server or SQL Server Express if you are using a default instance of SQL Server. This port is also used by the console to listen for communication from the database. When used by Core Services, the port uses bi-directional communications to communicate with the console and the database. |
| 1621 | Core Services | Used by Core Services to listen for communication from the Windows agent when both the agent and the Core Services computer are in FIPS mode. |
| 1622 | Security Agent for Windows | Used by the Windows agent to listen for communications from Core Services. This port uses bi-directional communications. |
| 1622 | Security Agent for iSeries | Used by NetIQ Security Solutions for iSeries PSAudit and PSSecure to listen for communication from Core Services. Core Services uses this port to run reports and actions. This port uses bi-directional communications. |
| 1622 | UNIX Agent | Used by the UNIX agent to listen for communication from Core Services. Core Services uses this port to run reports and actions. This port uses bi-directional communications. |
| 1626 | Core Services | Used by Core Services to communicate with Agents using SSL (Secure Sockets Layer) protocol. Agents include Windows, UNIX, and iSeries agents. SSL is a protocol developed by Netscape for ensuring security and privacy in Internet communications. SSL uses a private key to encrypt data that is transferred over the SSL connection. |
| 1627 | Core Services | Used by Core Services to listen for communication from the Security Agent for Windows or UNIX. |
| 8044 | Core Services | Used by Core Services to communicate with the console computer. This port uses bi-directional communications. |
| 8044 | Web Server | Used by the Web server that is embedded in Core Services. The Web server uses port 8044 by default, but this port is configurable. |
| 2005 | Security Agent for Windows | Used by the Windows agent to interact with the utility tools in Secure Configuration Manager. Ensure that this port is reserved for Secure Configuration Manager.<br><br>**NOTE:** If this port is already reserved and not available for Secure Configuration Manager, you can use any other free port, but ensure that you change the port number in the `HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\VigilEnt` registry accordingly. |

## 2.5.3 Planning to Install Your Database

This section provides requirements, recommendations, and configuration information for the Secure Configuration Manager **database computer**, which hosts the Secure Configuration Manager database. The size of your Secure Configuration Manager database and the number of concurrent connections can affect console performance.



### Database Computer Requirements

This section provides hardware, software, and permissions requirements for installing the Secure Configuration Manager database.

**NOTE:** Named instances cannot contain special characters. If you are using a named instance that contains special characters, rename the database instance so that it does not contain special characters.

The following table lists the requirements and recommendations for the database computer.

| Category | Minimum Requirements and Recommendations |
|---|---|
| Processor | See the NetIQ Secure Configuration Manager Technical Information web page. |
| Disk Space | |
| Memory | |
| Operating System | |
| Database | |
| Installation Permissions | The user account used to install the database must be a member of the Administrators local group on the computer. |
| Port | 1433: Used by Microsoft SQL Server or SQL Server Express if you are using a default instance of SQL Server.<br><br>**NOTE:** If you specified a non-default instance of SQL Server or SQL Server Express when you installed Secure Configuration Manager, ensure that the associated port is available and is open on the firewall. |
| Additional Settings | Set the System variable **TEMP** to `C:\windows\temp` in the System Properties > Environment Variables window on the Secure Configuration Manager database computer. |
| Settings for distributed setup and cluster environment | If you are installing the Secure Configuration Manager in a distributed environment or in a cluster environment, ensure the following:<br><br>◆ You have write permissions to the data and log file locations of the SQL Server data directory.<br><br>◆ A DNS Resolve method is present that queries a DNS server for the IP address associated with a host name or vice-versa. |

## Using the Database in a Cluster Environment

You can install SCM database in Microsoft SQL server cluster environment. While installing the database, provide the clustered SQL Server name when prompted to provide the database server name.

## Installing and Configuring Microsoft SQL Server

The Secure Configuration Manager database computer requires that Microsoft SQL Server or Microsoft SQL Server Express use mixed-mode authentication. Non-U.S. language versions of SQL Server and SQL Server Express are not supported. For more information about supported SQL Server versions, see “Database Computer Requirements” on page 20.

Follow the instructions provided in the Microsoft SQL Server documentation to install the database software.

### Configuring the SQL Server Browser Service

To complete the Secure Configuration Manager installation, the Browser Service must be running in SQL Server or SQL Server Express.

**To verify the SQL Server or SQL Server Express Browser Service is running:**

1. Open SQL Server Configuration Manager.
2. In the left pane, select the SQL Server services.
3. In the right pane, ensure that **SQL Server Browser** is set to **Running**.
4. (Conditional) If the SQL Server Browser is stopped, select **SQL Server Browser**, and on the Action menu, click **Start**.

### Configuring the SQL Server TCP/IP Protocol

To complete the Secure Configuration Manager installation, the TCP/IP protocol must be enabled in SQL Server or SQL Server Express.

**To verify the SQL Server TCP/IP protocol is enabled:**

1. Open SQL Server Configuration Manager.
2. In the left pane, expand SQL Server Network Configuration and select **Protocols for MSSQLSERVER**.
3. In the right pane, ensure that **TCP/IP** is set to Enabled.
4. (Conditional) If the TCP/IP protocol is disabled, select **TCP/IP**, and on the Action menu, click **Enable**.

# 2.5.4 Planning to Install Your Core Services

This section provides hardware, software, and permissions requirements for Core Services computers.

- “Core Services Computer Requirements” on page 22
- “Multiple Core Services Requirements” on page 22

## Core Services Computer Requirements

When planning to install Core Services, take into account the following considerations:

- Secure Configuration Manager supports IPv4 and IPv6 addresses, but uses IPv4 addresses for communication among the console, Core Services, and the Secure Configuration Manager database. The Core Services computer must be configured for IPv4 addresses at a minimum. Alternatively, you can set up the Core Services computer as a dual-stack host to support both IPv4 and IPv6 addresses.

The following table lists the requirements and recommendations for the Core Services computer.

| Category | Minimum Requirements and Recommendations |
|---|---|
| Processor | See the NetIQ Secure Configuration Manager Technical Information web page. |
| Disk Space | |
| Memory | |
| Operating System | |
| Additional Software | |
| Installation Permissions | The user account used to install Core Services must be a member of the Administrators local group on the computer. |
| Ports | 1621: Used by Core Services to communicate with the Security Agent for Windows when both the agent and Core Services are in FIPS mode.<br><br>1626: Used by Core Services to communicate with SSL agents.<br><br>For more information about SSL and non-SSL agents, see Section 2.5.2, “Default Ports,” on page 19.<br><br>1627: Used by Core Services to listen for communication from the Security Agent for UNIX or Windows.<br><br>8044: Used by Core Services to communicate with the console computer. Also used by the Web server that is embedded in Core Services. (This port is configurable.)<br><br>**NOTE:** If you are using non-default ports, ensure that those ports are available and are open on the firewall. |

## Multiple Core Services Requirements

If you plan to install more than one Core Services computer, each Core Services computer must meet the requirements specified in this section. In addition, depending on the agents you deploy, you may need to complete an additional step to enable multiple Core Services to communicate with registered agents.

Windows, UNIX, and iSeries agents support shared secret authentication. Therefore, you must export the domain keys from your first Core Services, and the other Core Services must import those keys to communicate with that agent. For more information, see Section 3.3, “Working with Multiple Core Services,” on page 27.

## 2.5.5 Planning to Install Secure Configuration Manager Consoles

This section provides hardware, software, and permissions requirements for the Secure Configuration Manager console computer.

### Console Computer Requirements

This section provides requirements for a Secure Configuration Manager environment. When planning to install the console, take into account the following considerations:

- Running more than 10 active consoles concurrently can reduce product performance.
- The size of your Secure Configuration Manager database and the number of concurrent connections can affect console performance. You can adjust the refresh period to improve performance. For more information, see the *NetIQ Secure Configuration Manager User Guide*.
- Secure Configuration Manager supports IPv4 and IPv6 addresses, but uses IPv4 addresses for communication among the console, Core Services, and the Secure Configuration Manager database. The console computer must be configured for IPv4 addresses at a minimum. Alternatively, you can set up the console computer as a dual-stack host to support both IPv4 and IPv6 addresses.

The following table lists the requirements for console computers.

| Category | Minimum Requirements and Recommendations |
|---|---|
| Processor | See the NetIQ Secure Configuration Manager Technical Information web page. |
| Disk Space | |
| Memory | |
| Operating System | |
| Monitor | |
| Additional Software | |
| Installation Permissions | The user account you use to install the console must be a member of the Administrators local group on the computer. |
| Usage Permissions | The Windows user account you use to run the console must be one of the following:<br>◆ Member of the local Administrators group<br>◆ Account with write permissions to the `NetIQ\Secure Configuration Manager` folder and its subfolders<br>If you are running the console on the database computer, your account must have write permissions to the `NetIQ\Secure Configuration Manager` folder and its subfolders and must be a member of the VigilEnt_Users group. |

## 2.5.6 Planning to Install Agents

This section lists the agent versions supported by Secure Configuration Manager, and also directs you to specific requirements information for each agent.

When you install Secure Configuration Manager, the setup program automatically installs and registers a Windows agent on the Core Services computer. The run-as account for the Windows agent service on the Core Services computer should have appropriate permissions, such as Domain Administrator permissions, to modify remote computers. For more information about the Windows agent service and required permissions, see the *NetIQ Secure Configuration Manager Windows Agent Installation and Configuration Guide* and Section 3.2, “Installing Secure Configuration Manager Components,” on page 25.


- “Agent Ports” on page 24
- “Agent Computer Requirements” on page 24


**NOTE:** To ensure optimum deployment of Windows agents to remote computers, do not remove the Windows agent from the Core Services computer.

### Agent Ports

Ensure that the required ports are open to enable communication between the agent computers and Secure Configuration Manager Core Services. For more information about the ports used to communicate with the agents, see the Help.

### Agent Computer Requirements

In Secure Configuration Manager, **platform** represents the type of endpoint. The requirements for agent computers vary depending on the platform. All agent installations require Administrator permissions on the computer on which you are installing the agent.

The following table lists the agent platforms that Secure Configuration Manager supports and where you can find the requirements for those platforms.

| Platform | Location of Requirements Information |
|---|---|
| Windows | *NetIQ Secure Configuration Manager Windows Agent Installation and Configuration Guide* |
| UNIX and Linux | *NetIQ Secure Configuration Manager UNIX Agent Installation and Configuration Guide* |
| iSeries | *NetIQ Security Solutions for iSeries Installation Guide* |

# 3 Installing Secure Configuration Manager

This chapter addresses licensing and permissions requirements for Secure Configuration Manager, provides guidance for determining the appropriate installation type, and outlines the installation steps.



## 3.1 Installation Checklist

Install Secure Configuration Manager in a production environment by completing the following checklist.

| | Checklist Items |
|---|---|
| ❑ | 1. Ensure that you have the appropriate licenses for the components you plan to install. For more information, see Section 2.2, “Licensing,” on page 14. |
| ❑ | 2. Locate the installation kit for Secure Configuration Manager and any agents that you plan to install. |
| ❑ | 3. Ensure that you have the appropriate permissions for the computers on which you will be installing components. For more information, see Section 2.3, “Permissions Requirements,” on page 16. |
| ❑ | 4. Install Secure Configuration Manager. For more information, see Section 3.2, “Installing Secure Configuration Manager Components,” on page 25. |
| ❑ | 5. Install your agents. For more information, see the appropriate chapter or guide for each agent. |
| ❑ | 6. Run the AutoSync update service to download the latest security checks and policy templates. For more information, see Section 5.4, “Updating Security Knowledge,” on page 38. |

## 3.2 Installing Secure Configuration Manager Components

To successfully install Secure Configuration Manager, you must install the Secure Configuration Manager database and Core Services.

**NOTE:** By default, console is installed with Core Services.

First, install the Secure Configuration Manager database (and Core Services, if appropriate) on the database computer. Then, if you did not install Core Services on the same computer as the database, install that component on a separate dedicated computer. Finally, install consoles on all computers that you want to host a user interface.

The Secure Configuration Manager setup program automatically installs and registers a Windows agent on the Core Services computer. You must specify a run-as account for the Windows agent service. The account requires specific permissions, such as the ability to deploy agents to remote computers. For more information about the Windows agent service and permissions, see the *NetIQ Secure Configuration Manager Windows Agent Installation and Configuration Guide*.

If you do not enter a valid license key, the installation program automatically applies a 30-day trial license. You can change the license key any time after installing Secure Configuration Manager. For more information about license keys, see the Help for the Core Services Configuration Utility.

---

**NOTE:** In addition to the files installed in the `Program Files` folder, the installation program installs a `scmnss` folder in the root directory on the Core Services computer. Do not remove the `scmnss` folder or the files within the folder. Secure Configuration Manager requires these files for FIPS communication.

---

**To install Secure Configuration Manager components:**

1. Log on with an Administrator account to the computer where you want to install the Secure Configuration Manager components.
2. Exit all programs on the computer.
3. Ensure that the Windows Services window, accessed through the Windows Control Panel, is closed.
4. Run the setup program, `Setup.exe`, from the root folder of the Secure Configuration Manager installation kit.
5. Click **Start Installation** to start the Secure Configuration Manager installation.

   Follow the instructions in the wizard to proceed with the installation.
6. (Optional) If you do not want to install the database and want to use an existing Secure Configuration Manager database, clear the **Database** selection in the Component Selection section.
7. (Optional) To specify an account for the Core Services service and the port, complete the following steps:

   **7a** In the **Service Account** field, type the user name of the account you want to assign to the Core Services service.

   **NOTE**

   - If you specify a local account, use the `.\username` format.
   - 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 **Service Account** field. Leaving the field blank results in an error.
   - If you start the service within a specific domain, you must specify the domain name using the `domainname\username` format. For example, `AcmeMidWest\smithj`.

   **7b** In the **Password** field, type the password for the specified service account.

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

   **7c** If you want to use a non-default port for Core Services, clear the **Use Default Port** option, and specify the port in the **Core Port** field.
8. (Optional) To specify the SQL server connection, complete the following steps:

   **8a** Specify the server name.

**NOTE:** If you have unchecked the **Database** selection in the Component Selection section, select the SQL sever that contains the Secure Configuration Manager database.

**8b** Select the **Use Default Port** option if you want to use the default port for SQL database. Default port 1433. Specify the port number in the **Database Port** field if you want to use a non-default port.

**8c** Select the type of authentication. Provide user name and password if you select SQL authentication.

**9** (Optional) To specify an account for the Windows agent service, complete the following steps:

**9a** In the **Service Account** field, type the user name of the account you want to assign to the agent service.

**NOTE**

- The Windows agent service running on the Core Services computer requires an account with enough permissions to modify remote computers. For example, specify a domain administrator account. This Windows agent becomes the default Deployment Agent for the domain.
- If you specify a local account, use the `.\username` format.
- 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 **Service Account** field. Leaving the field blank results in an error.
- If you start the service within a specific domain, you must specify the domain name using the `domainname\username` format. For example, `AcmeMidWest\smithj`.

**9b** In the **Password** field, type the password for the specified service account.

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

**10** Follow the instructions in the wizard until you finish installing Secure Configuration Manager.

**NOTE:** An installation summary, which contains prominent installation parameters you have specified, is displayed for your review. The `C:\Program Files (x86)\NetIQ\Secure Configuration Manager\installconfig.txt` file is created during installation, which contains ALL the values you have specified for installation parameters. You can use this file for reference.

**11** (Optional) Install the Secure Configuration Manager Dashboard. Click **Cancel** when prompted if you do not want to install the Dashboard.

# 3.3 Working with Multiple Core Services

When you run Core Services for the first time, it generates a set of authentication keys called **domain keys**. If you have more than one Core Services, and if you register an agent in Secure Configuration Manager that supports shared secret authentication, another Core Services cannot communicate with that agent unless it has those domain keys. You must export the domain keys from your first Core Services, and import them into the other Core Services to communicate with that agent. Agents that support shared secret authentication include Windows, UNIX, and iSeries agents.

**To set up multiple Core Services to communicate with agents:**

**1** On the Core Services computer that registered the agents, open the `ExportDomainKeys.bat` file. By default, this file is located in the `Program Files\NetIQ\Secure Configuration Manager\Core Services\bin` folder.

2 At the **Filename** prompt, type the name of the file to store the domain keys and press Enter. You can enter just the file name, which will be saved in the same folder, or you can enter a full path and file name.

3 At the **Password** prompt, type a password that the other Core Services must use to access the domain keys for importing, and press Enter.

4 For each Core Services computer that needs to access the agents registered on the first Core Services, complete the following steps:

**4a** Open the `ImportDomainKeys.bat` file.

**4b** At the **Filename** prompt, type the name of the file where the domain keys are stored and press Enter.

**4c** At the **Password** prompt, type the password to access the domain keys and press Enter.

**4d** Restart Core Services.

5 Open the console to see the registered agents.

# 3.4 Deploying the Standalone AutoSync Client

The Secure Configuration Manager AutoSync service lets you regularly download the latest security knowledge from an update service Web site to ensure that the Secure Configuration Manager agents always audit with the latest security intelligence. The **Autosync client** queries and receives updates from the NetIQ AutoSync server. For more information, see the *NetIQ Secure Configuration Manager User Guide*.

You can install the AutoSync client on the same computer as Core Services, or you can install the standalone AutoSync client on a different computer so that it runs separately from Core Services.

Install a standalone AutoSync client when your Core Services computer is not directly connected to the Internet, or if you do not want the Core Services computer to download from the Internet. Ensure that the standalone AutoSync client computer has connectivity to the Internet and to Core Services.


- Section 3.4.1, “Installing the Standalone AutoSync Client,” on page 28
- Section 3.4.2, “Configuring the Standalone AutoSync Client,” on page 29


## 3.4.1 Installing the Standalone AutoSync Client

Complete the following steps to install the standalone AutoSync client.

**To install the standalone AutoSync client:**

1 Log on with an Administrator account to the computer where you want to install the standalone AutoSync client.

2 Ensure that the Windows Services window, accessed through the Windows Control Panel, is closed.

3 Run the setup program from the root folder of the Secure Configuration Manager installation kit.

4 Start installation.

5 Follow the instructions in the wizard until you reach the Component Selection window.

On the Component Selection window, select *only* the **Standalone AutoSync Client** component.

6 Follow the instructions in the wizard until you finish installing the standalone AutoSync client.

### 3.4.2 Configuring the Standalone AutoSync Client

Once you have installed the standalone AutoSync client, you must provide configuration information in Secure Configuration Manager so the AutoSync client can query and receive updates from the NetIQ AutoSync server. In addition to basic AutoSync settings, you can also set up a proxy Internet server. For more information about configuring the standalone AutoSync client, see the *NetIQ Secure Configuration Manager User Guide*.

# 4 Adding or Updating Security Agents

When you install or upgrade to a new version of Secure Configuration Manager, the installation program automatically installs a Windows security agent on the Core Services computer. You can add or update other security agents after completing the installation process.



## 4.1 Deploying UNIX Agents

The Security Agent for UNIX (UNIX agent) collects security information from one or more UNIX and Linux computers. The UNIX agent is also configured to collect information from Oracle endpoints on your UNIX and Linux computers. Secure Configuration Manager can automatically install and uninstall agents on UNIX and Linux computers as needed. For detailed information about the requirements for and capabilities of UNIX agents, see the *NetIQ UNIX Agent Guide* available from the UNIX agent installation kit.

## 4.2 Deploying iSeries Agents

NetIQ Security Solutions for iSeries is a suite of integrated products including PSAudit, PSSecure, PSDetect, PSPasswordManager, and Privilege Manager. These products simplify security auditing, vulnerability assessment, user access control, and event management for iSeries servers. NetIQ Security Solutions for iSeries includes solutions for managing user profiles and enforcing and strengthening password policies.

For detailed planning, installation, and configuration information for deploying iSeries agents, refer to the *Installation Guide for NetIQ Security Solutions for iSeries* available from the NetIQ Security Solutions for iSeries installation kit.

## 4.3 Deploying Windows Agents

The Windows agent collects security information from one or more Windows computers in one or more domains. The agent is can also collect information from Microsoft SQL Server, Microsoft Internet Information Services (IIS), Oracle, Active Directory, and Network Attached Storage (NAS) endpoints. Secure Configuration Manager can automatically install and uninstall agents on Windows computers as needed.

For more information about deploying Windows agents, see the *NetIQ Security Agent for Windows Installation and Configuration Guide* available from the Secure Configuration Manager and Windows agent installation kits.

# 5 Upgrading Secure Configuration Manager

This chapter addresses planning considerations and provides a checklist to help you upgrade Secure Configuration Manager.

The upgrade process does not support upgrades from previous trial installations.

**NOTE:** If you are using Secure Configuration Manager with an operating system and/or a database version that is no longer certified, please contact NetIQ Technical Support to migrate to a certified version of the operating system and/or the database. For more information about certified operating system and database versions, see the Secure Configuration Manager Technical Information web page.



## 5.1 Secure Configuration Manager Upgrade Checklist

Upgrade your Secure Configuration Manager installation using the following checklist.

| | Checklist Items |
|---|---|
| ❑ | 1. Back up the Secure Configuration Manager configuration data. For more information, see Section 5.2, “Backing Up Configuration Data,” on page 34. |
| ❑ | 2. Close all Secure Configuration Manager consoles and shut down Core Services. For more information, see Section 5.3.1, “Preparing to Upgrade,” on page 35. |
| ❑ | 3. Using Microsoft SQL Server Enterprise Manager, ensure that no users are connected to the Secure Configuration Manager database. |
| ❑ | 4. Back up your Secure Configuration Manager database. For more information, see the Microsoft SQL Server documentation. |
| ❑ | 5. Ensure that the computers on which you want to upgrade Secure Configuration Manager components meet the specified requirements. For more information, see Section 2.5, “Planning Your Secure Configuration Manager Environment,” on page 17 and Step 6 of Section 5.3.1, “Preparing to Upgrade,” on page 35. |

| | Checklist Items |
|---|---|
| ❑ | 6. Ensure that you have SQL Server configured properly to allow Secure Configuration Manager to connect to the database. For more information, see Step 7 in Section 5.3.1, “Preparing to Upgrade,” on page 35.<br><br>**IMPORTANT:** Before beginning to install Secure Configuration Manager, close all the windows that are open against Vigilent database in SQL Server Management Studio. |
| ❑ | 7. Stop all pending and scheduled jobs. For more information, see Section 5.3.2, “Stop Scheduled Jobs Before Upgrade,” on page 36. |
| ❑ | 8. Upgrade Core Services and the Secure Configuration Manager database. After the upgrade dialog box closes, Secure Configuration Manager continues to run the upgrade process. Do not stop Core Services until the upgrade fully completes. For more information, see Section 5.3.3, “Upgrading Secure Configuration Manager,” on page 37. |
| ❑ | 9. Upgrade each console computer. Secure Configuration Manager displays a message if you attempt to log on to the console before the database upgrade process completes. For more information, see Section 5.3.3, “Upgrading Secure Configuration Manager,” on page 37. |
| ❑ | 10. Restore all the Secure Configuration Manager data. For more information, see Section 5.6, “Recovering Configuration Data,” on page 40. |
| ❑ | 11. Run the AutoSync update service to download the latest security checks and policy templates. For more information, see Section 5.4, “Updating Security Knowledge,” on page 38. |
| ❑ | 12. Check the NetIQ Web site to ensure that you have the latest version for your currently installed agents. For more information, see the Secure Configuration Manager Technical Information web page. |
| ❑ | 13. (Conditional) If you do not have the latest version of an agent, download the appropriate software update from the NetIQ Web site and use the instructions provided in the installation kit to upgrade the agent or see “Updating Agent Content ” in the *NetIQ Secure Configuration Manager User Guide*. |

## 5.2 Backing Up Configuration Data

To back up configuration data before you upgrade Secure Configuration Manager:

1. Back up the SCM installation directory. Generally, the installation directory is `C:\Program Files\NetIQ\Secure Configuration Manager`.
2. Back up the SCMNSS directory. Generally, the SCMNSS directory is `C:\scmnss`.
3. Back up registry keys by exporting the following registry keys. To export the registry keys, open the command prompt and type `regedit.exe`, and then go to `File` > `Export`. Save the registry key file in `.reg` format.
   - `HKEY_CURRENT_USER\Software\PENTASAFE`
   - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PSService`

   (Conditional) For 32-bit computers:
   - `HKEY_LOCAL_MACHINE\SOFTWARE\PENTASAFE`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NetIQ Core Services`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NetIQ Secure Configuration Manager`

(Conditional) For 64-bit computers:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PENTASAFE`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\NetIQ Core Services`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\NetIQ Secure Configuration Manager`

4 Back up the SCM shortcuts by backing up the `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\NetIQ Secure Configuration Manager` directory.

**NOTE:** The `ProgramData` directory might be hidden. If it is not visible, change the folder options settings to show the hidden files and folders.

5 Back up the Vigilent database.

**NOTE:** If you are using a 64-bit computer, the default installation directory for SCM is `C:\Program Files (x86)\NetIQ\Secure Configuration Manager`.

# 5.3 Upgrading Secure Configuration Manager

This section provides requirements and instructions for upgrading Secure Configuration Manager.



## 5.3.1 Preparing to Upgrade

Before upgrading Secure Configuration Manager, you need to prepare the environment through the following steps.

**To prepare your environment for upgrade:**

1 Verify that the version of Secure Configuration Manager currently running in your environment is supported by the upgrade process. For more information, see Section 5.1, “Secure Configuration Manager Upgrade Checklist,” on page 33.

2 To ensure a clean snapshot of your Secure Configuration Manager database, close all consoles and shut down Core Services. Follow these steps to shut down Core Services:

2a Log on to the Core Services computer.

2b Click **Services** in the Administrative Tools program folder, and then click **NetIQ Core Services**.

2c On the Action menu, click **Stop**.

3 Using Microsoft SQL Server Enterprise Manager, ensure no users are connected to the Secure Configuration Manager database.

4 To ensure that your session is not timed out during the upgrade, modify time-out settings, by using the following steps:

   **4a** Log in to the Microsoft SQL Server Enterprise Manager.

   **4b** Select your SQL server by right-clicking the name of the server, and then go to **Properties** > **Connections**.

   **4c** Set the value of the `Remote Query Timeout` property to 0.

5 Back up your Secure Configuration Manager database. For more information, see the Microsoft SQL Server documentation.

6 Ensure the free disk space allocated for the database upgrade is at least four times the size of the current `VigilEnt.mdf` file. By default, you can find the `VigilEnt.mdf` file at `C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data`.

7 To ensure that the Browser Service is running in SQL Server, complete the following steps:

   **7a** Open SQL Server Configuration Manager.

   **7b** In the left pane, select the SQL Server services.

   **7c** In the right pane, ensure **SQL Server Browser** is set to Running.

   **7d** (Conditional) If the SQL Server Browser is stopped, select **SQL Server Browser**, and on the Action menu, click **Start**.

8 To ensure that the TCP/IP protocol is enabled in SQL Server, complete the following steps:

   **8a** In the left pane, expand SQL Server 2005 Network Configuration and select **Protocols for <*database server name*>**.

   **8b** In the right pane, ensure that **TCP/IP** is set to Enabled.

   **8c** (Conditional) If the TCP/IP protocol is disabled, select **TCP/IP**, and on the Action menu, select **Enable**.

9 Before you run the upgrade program, ensure that no users are connected to the database and no Secure Configuration Manager consoles are running. The database upgrade fails if users attempt to connect to the database at any time during the upgrade process.

## 5.3.2 Stop Scheduled Jobs Before Upgrade

You cannot run scheduled jobs during the upgrade of Secure Configuration Manager. Scheduled jobs that complete or start during the upgrade process indicate a zero score upon completion. You must run the jobs again.

**To stop pending jobs:**

1 In the Pending jobs queue, right-click the job.

2 On the context menu, click **Cancel**.

**To prevent jobs from running:**

1 In the Scheduled jobs queue, right-click the job.

2 On the context menu, click **Disable**.

3 After upgrading Secure Configuration Manager, right-click the job in the Scheduled jobs queue.

4 On the context menu, click **Enable**.

## 5.3.3 Upgrading Secure Configuration Manager

If a Windows agent exists on the Core Services computer, the setup program upgrades the agent. Otherwise, the setup program installs and registers a new Windows agent on the computer. The new agent and the endpoint representing the computer's operating system become a managed system in your asset map.

**To upgrade Secure Configuration Manager:**

1. Ensure that you have prepared your environment for upgrade. For more information, see Section 5.3.1, "Preparing to Upgrade," on page 35.
2. Ensure that the computers on which you want to upgrade Secure Configuration Manager components meet the specified requirements. For more information, see Chapter 2, "Planning to Install Secure Configuration Manager," on page 13 and Step 6 on page 36 of Section 5.3.1, "Preparing to Upgrade," on page 35.
3. To upgrade Core Services and the Secure Configuration Manager database, complete the following steps:
   - **3a** Log on to the Core Services computer with the appropriate permissions:
     - (Conditional) If Core Services and the database are installed on the same computer, log on as a user with local administrator rights.
     - (Conditional) If Core Services and the database are installed on different computers, you must log on to the Core Services computer with an account that has administrator rights in SQL Server.

     **NOTE:** If Core Services and the Secure Configuration Manager database are installed on different computers, the Secure Configuration Manager installation kit detects the database location and upgrades it along with Core Services.
   - **3b** Exit all programs that are open on the computer.
   - **3c** Run the setup program from the root folder of the Secure Configuration Manager installation kit.
   - **3d** Select the type of authentication—Windows or SQL. If you select SQL, provide the user name and password for the account. And then click **Upgrade**.
   - **3e** Follow the instructions in the wizard until you have finished upgrading the product.
   - **3f** (Conditional) If the upgrade process prompts you to install the Windows agent, you must specify a run-as account for the Windows agent service. For more information about the Windows agent service and permissions, see the *Installation and Configuration Guide for NetIQ Secure Configuration Manager Windows Agent*.
   - **3g** Do not stop or start Core Services until the upgrade process completes.

     After the upgrade window closes, Secure Configuration Manager continues to run the upgrade processes.
4. To upgrade consoles, complete the following steps on each console computer:
   - **4a** Log on to the console computer with an administrator account.

     **NOTE:** You must wait until the database upgrade completes before you can log on to a Secure Configuration Manager console.
   - **4b** Exit all programs open on the computer.
   - **4c** Run the setup program from the root folder of the Secure Configuration Manager installation kit.

4d (Conditional) If you accept the terms in the license agreement, click **Accept** and then click **Next**.

4e Select **Upgrade** and then click **Next**.

4f Follow the instructions in the wizard until you have finished installing the product.

5 Once you have completed the upgrade, re-run the AutoSync wizard in Secure Configuration Manager to download the latest security knowledge. For more information about the AutoSync feature, see Section 5.4, “Updating Security Knowledge,” on page 38 and the *NetIQ Secure Configuration Manager User Guide*.

### Troubleshooting Database Upgrade Failure

If your database upgrade fails due to a power outage, users connecting to the database during upgrade, or other errors, restore the database backup you made prior to upgrade and run the database upgrade again. You can find information to help you troubleshoot database issues in the log files. To access your log files, enter `%TEMP%` in the Windows Run command window. For information about restoring a database, see the Microsoft SQL Server documentation.

## 5.4 Updating Security Knowledge

The upgrade process might not include the latest security checks and policy templates for Secure Configuration Manager. It is important to run the AutoSync update service to download and apply the latest security intelligence to keep your enterprise protected. For more information, see the *NetIQ Secure Configuration Manager User Guide*.

---

**NOTE:** Secure Configuration Manager downloads, but does not update, patch level database files during this process. For more information, see Section 5.5, “Agent Considerations,” on page 39 and the *NetIQ Secure Configuration Manager User Guide*.

---

**To update security knowledge:**

1 After completing the upgrade process, launch Secure Configuration Manager.

2 On the Tools menu, click **AutoSync Wizard**.

3 Click **Check for Updates.**

4 (Optional) To download and apply all policy templates and security checks, select the check box in the column header.

5 (Optional) To download and apply specific policy templates and security checks, complete the following steps:

5a Clear the check box in the column header to deselect all items in the window.

5b Select the check box next to each policy template and security check you want to download and apply.

6 Click **Apply Updates**.

7 Click **OK**.

8 Click **Finish** when the wizard completes the download.

## 5.5 Agent Considerations

When you upgrade Secure Configuration Manager, the endpoint and agent information persists from the previous version so you can continue running reports on existing endpoints. However, in some cases, you must delete old agents and add them as new endpoints. For more information about supported agent versions, see the Secure Configuration Manager Technical Information web page.



### 5.5.1 Windows Agent

When you install the Windows agent, Secure Configuration Manager also includes support for Active Directory, Microsoft IIS, Microsoft SQL Server, NAS, Oracle, and Network Device endpoints. To manage Active Directory, Microsoft IIS, SQL Server, NAS, Oracle, or Network Device endpoints with the Windows agent, you must add the endpoints in Secure Configuration Manager after you install the Windows agent.

If you previously managed Microsoft IIS endpoints using the VigilEnt Security Agent for Web Servers (VSA for Web Servers), and want to continue managing those endpoints, delete the old agents and add them as new endpoints of the Windows agent.

No upgrade path is available from the legacy Oracle agent to the new endpoint type. If you are currently managing Oracle databases with the legacy Oracle agent and want to continue managing those databases using the Windows agent, delete your old agents and add them as new endpoints of the Windows agent.

To take advantage of new features in Secure Configuration Manager, you must upgrade each agent to the latest agent versions. For more information about upgrading Windows agents, see the *NetIQ Secure Configuration Manager User Guide* and the *Installation and Configuration Guide for NetIQ Secure Configuration Manager Windows Agent*.

### 5.5.2 UNIX Agent

When you install the UNIX agent, Secure Configuration Manager also includes support for Oracle endpoints. To manage Oracle endpoints using the UNIX agent, you must add the endpoints in Secure Configuration Manager after you install the UNIX agent.

No upgrade path is available from the legacy Oracle agent to the new endpoint type supported by the UNIX agent. If you are currently managing Oracle databases with the legacy Oracle agent and want to continue managing those databases using the UNIX agent, delete your old agents and add them as new endpoints of the UNIX agent.

To take advantage of new features in Secure Configuration Manager, you must upgrade each agent to the latest agent versions. For more information, see Section 4.1, “Deploying UNIX Agents,” on page 31, and the *Installation and Configuration Guide for NetIQ Secure Configuration Manager UNIX Agent*.

### 5.5.3 iSeries Agent

You must upgrade Secure Configuration Manager on each iSeries system. Also, you must re-register each iSeries agent with the upgraded Core Services. To take advantage of new features in Secure Configuration Manager, update the iSeries agents to the latest agent versions.

The following table shows where you can find additional information about upgrading iSeries systems and agents to Secure Configuration Manager 5.8.

| If you want to... | See... |
|---|---|
| Deploy iSeries agents | *Installation Guide for NetIQ Security Solutions for iSeries* |
| Update Security Knowledge for iSeries agents | Section 5.4, “Updating Security Knowledge,” on page 38 |
| Install Secure Configuration Manager on iSeries systems | *Installation Guide for NetIQ Security Solutions for iSeries* |

## 5.6 Recovering Configuration Data

If the SCM upgrade fails or is interrupted, you can recover the SCM configuration data. NetIQ recommends that you recover the configuration data before trying to upgrade again if the upgrade fails or is interrupted.

To recover SCM configuration data:

1. Stop the **Netiq Security Agent for Windows** service in **Control Panel** > **Administrative Tools** > **Services**.
2. Rename or copy the backed up installation folder to `C:\Program Files\NetIQ\Secure Configuration Manager`.
3. Rename or copy the backed up SCMNSS folder to `C:\scmnss`.
4. Import the backed up registry keys. To import the registry, open the command prompt and enter `regedit.exe` and then go to `File` > `Import`.

   Browse to the backed up `.reg` file:

   - `HKEY_CURRENT_USER\Software\PENTASAFE`
   - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PSService`

   (Conditional) For 32-bit computers:

   - `HKEY_LOCAL_MACHINE\SOFTWARE\PENTASAFE`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NetIQ Core Services`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NetIQ Secure Configuration Manager`

   (Conditional) For 64-bit computers:

   - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PENTASAFE`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\NetIQ Core Services`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\NetIQ Secure Configuration Manager`

5 Rename or copy the backed up shortcuts folder to `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\NetIQ Secure Configuration Manager`.

6 Restore the backed up Vigilent database.

7 Restart **NetIQ Core Service** in **Control Panel** > **Administrative Tools** > **Services**.

8 Restart **NetIQ Security Agent for Windows**.

---

**NOTE:** If you are using a 64-bit computer, the default installation directory for SCM is `C:\Program Files (x86)\NetIQ\Secure Configuration Manager`.

---

# 6 Getting Started with Secure Configuration Manager

This chapter provides information about Windows and SQL authentication, and helps you get started with the Secure Configuration Manager console and Core Services.



## 6.1 Configuring Windows Authentication

By default, Secure Configuration Manager uses SQL authentication for communication between Core Services and the database. SQL authentication creates a user ID and password that are valid only for Microsoft SQL Server. You can also use Windows authentication.

When using Windows authentication, the database checks with the Windows domain controller to see if the user ID and password you used to log on to the computer are allowed to use the database.

**To use Windows authentication:**

1. (Conditional) If the database is on the same computer as Core Services, complete the following steps on this computer:
   - **1a** Start the **Core Services Configuration Utility** in the NetIQ Secure Configuration Manager program folder.
   - **1b** On the Database tab, set the **Use Windows Authentication** field to **True**.
   - **1c** Click **OK** to save the changes and close the Configuration Utility.
   - **1d** Restart Core Services.
2. (Conditional) If the database is on a different computer from Core Services, complete the following steps on the Core Services computer:
   - **2a** Start the **Core Services Configuration Utility** in the NetIQ Secure Configuration Manager program folder.
   - **2b** On the Database tab, set the **Use Windows Authentication** field to **True**.
   - **2c** Click **OK** to save the changes and close the Configuration Utility.
   - **2d** Browse to the Services list in Control Panel.
   - **2e** Select **NetIQ Core Services** from the Services list.
   - **2f** Change the service properties to log on with the account you specify to connect to the database.
   - **2g** Click **OK**.
   - **2h** Click **Start Service**.
3. Close the Services and Administrative Tools windows.

## 6.2 Starting Core Services

Core Services handles communication between the console and the other Secure Configuration Manager components. Core Services must be running before you can use Secure Configuration Manager.

The Secure Configuration Manager setup program automatically starts Core Services for you. However, you can also manually start Core Services. To manually start the Core Services service, use the Services utility in the Windows Control Panel.

When you run Core Services for the first time, it generates a set of authentication keys called **domain keys**. If you are using a single Core Services, back up the domain keys for your Core Services to a disk or to another computer in case you need to re-install Core Services at any point. Otherwise, when you install a new Core Services, new keys are created and you cannot access the agents you registered with the set of domain keys generated by the initial Core Services installation.

**Console administrators**, console users assigned to the Secure Configuration Manager Administrator's role, can use the Core Services Configuration Utility to configure Core Services. For more information, see the Help for the Core Services Configuration Utility.

## 6.3 Starting the Secure Configuration Manager Console

When starting Secure Configuration Manager for the first time after installation, you must use the user account and password that you entered during installation to log on. After you set up the product and create other user and administrator accounts, you can use any of those accounts to log on to the console.

By default, Secure Configuration Manager uses Windows authentication for communication between the console and the database. When using Windows authentication, the database checks with the Windows domain controller to see if the user ID and password you used to log on to the console computer are allowed to use the database through Core Services.

You can also use SQL authentication. For more information, see Section 6.4, "Configuring SQL Authentication," on page 45.

**To start the Secure Configuration Manager console:**

1. Start Secure Configuration Manager in the NetIQ Secure Configuration Manager program folder.
2. In the **Core Services** field, select the computer that hosts the Core Services you want to use.
3. (Optional) To configure the Core Services that you are using, complete the following steps:
   - **3a** Click **Configure**.
   - **3b** Edit the appropriate fields.
   - **3c** Click **OK**.
4. Type the user name for your default Secure Configuration Manager administrator account in the **User Name** field. Type the password that you specified during installation in the **Password** field.
5. Click **OK**.

# 6.4 Configuring SQL Authentication

You can also use SQL authentication for communication between the console and the database. SQL authentication creates a user ID and password that are valid only for SQL Server. For more information about authentication, see the Authentication article in the SQL Server Books Online, which are delivered with the full version of SQL Server.

**To set up SQL authentication:**

1. Set up the database in mixed-mode security in SQL Server Enterprise Manager. For more information, see the Microsoft SQL Server documentation.
2. On the Core Services computer, complete the following steps:
   - **2a** Start the **Core Services Configuration Utility** in the NetIQ Secure Configuration Manager program folder.
   - **2b** On the Database tab, set the **Allow SQL Authentication** field to **True**.
   - **2c** Click **OK** to save the changes and close the Configuration Utility.
   - **2d** Restart Core Services using the Windows Services utility. You can access the Windows Services utility through Control Panel.
3. Enable SQL authentication in Secure Configuration Manager by completing the following steps:
   - **3a** Start Secure Configuration Manager in the NetIQ Secure Configuration Manager program folder.
   - **3b** On the console login window, click **Configure**.
   - **3c** Select the **Enable SQL Authentication** check box.
   - **3d** Click **OK**.
4. Specify your user name and password and click **OK**.