Secure Configuration Manager™

Installation Guide for Secure Configuration Manager

February 2018

Legal Notice

About This Book

The *Installation Guide* provides instructions for upgrading and installing Secure Configuration Manager. This book also includes guidance for initial configuration to get you started.

Intended Audience

This book provides information for individuals responsible for installing, configuring, and upgrading Secure Configuration Manager.

Additional Documentation

The Secure Configuration Manager documentation library includes the following resources:

- *User's Guide for Secure Configuration Manager*
- *Secure Configuration Manager Windows Agent Installation and Configuration Guide*
- *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

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.

Understanding the Secure Configuration Manager Components

The Secure Configuration Manager environment includes three primary components (Core Services, consoles, and the database), security agents, and compliance evaluation tools (Security Checkup Results Viewer and Secure Configuration Manager Dashboard). You can install the components, agents, and the Secure Configuration Manager Dashboard on separate computers.

Secure Configuration Manager deploys **agents** to collect information, stores information in a central **database**, and displays reports in the Secure Configuration Manager **consoles**. Secure Configuration Manager **Core Services** manages communication among the components.

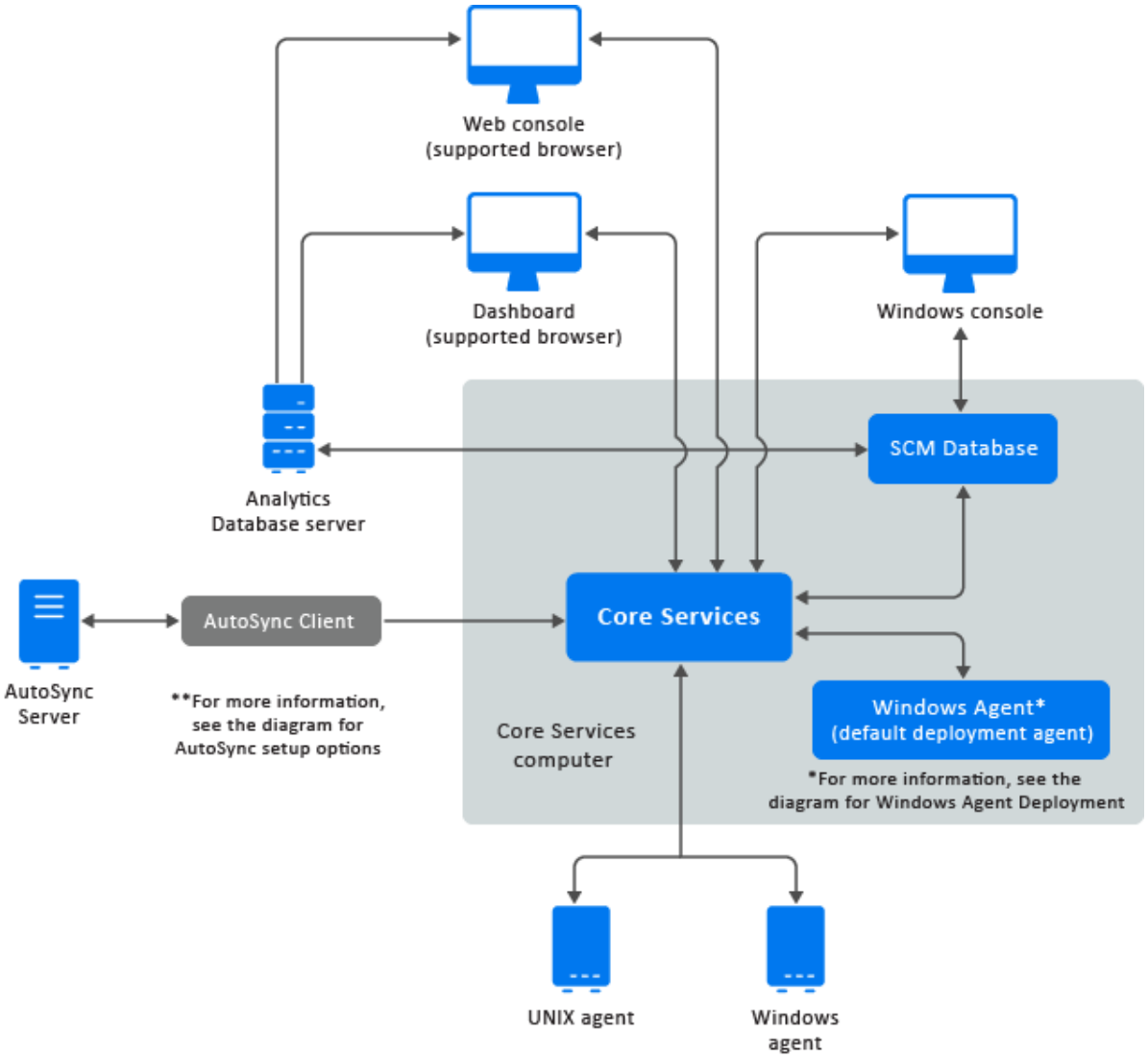
Secure Configuration Manager includes the components listed in the following table.

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.
Core Services	Communicates between agents, the database, and consoles to perform the following functions: ◆ Manage interaction between agents and consoles ◆ Authenticate requests to the agents ◆ Receive data from agents and store it in the database ◆ Log product activity, security checkup results, and configuration data in the database
Database	Stores product configuration data and results from security checkup reports in Microsoft SQL Server format.

Component	Description
Web console	Serves as a browser-based interface for Secure Configuration Manager so you can perform the following functions: ◆ Get a high-level view of your IT assets, including the status of their health, compliance, and risk to your enterprise security ◆ Create dynamic reports that combine the results of multiple policy templates and endpoints ◆ View and manage endpoints and groups ◆ Execute security checks and run policy templates so you can perform a granular assessment of specific groups and endpoints ◆ Create and apply saved lists for security check parameters ◆ Create and apply exceptions to assessment results ◆ Create and apply tags to endpoints and policy templates ◆ View the status of jobs ◆ Launch the Dashboard without having to log in again **NOTE:** With the introduction of Secure Configuration Manager 7.0, this console replaces some functionality provided by the Windows console.
Windows console	Serves as the original interface for Secure Configuration Manager so you can perform the following functions: ◆ View, add, remove, and group your IT assets ◆ Execute security checks and run policy templates ◆ Create and apply saved lists for security check parameters ◆ Create and apply exceptions to assessment results ◆ Manage jobs ◆ Filter information ◆ Control automatic AutoSync updates ◆ Configure product settings ◆ Modify, import, and export security checks and policy templates **NOTE:** With the introduction of Secure Configuration Manager 7.0, the Web console replaces some of the console's functionality. Further references to this console will be prefaced with "Windows".
Dashboard	Provides a Web-based overview of your environment's compliance enables executives and managers to: ◆ View the overall compliance of your IT assets ◆ Perform a granular assessment of specific groups and computers ◆ View the overall posture and trends of security compliance at a single glance Includes the Analytics Database and Dashboard website.

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 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.

Planning to Install Secure Configuration Manager

This section provides useful information for planning your Secure Configuration Manager environment. To review the prerequisites and system requirements for the computers where you want to install each component, see the installation sections for those components.

2 Planning Overview

This section helps you plan the installation process for Secure Configuration Manager. Some components must be installed in a specific order because the installation process requires access to previously installed components. For example, you should install the Secure Configuration Manager database before installing Core Services.

For the most recent specifications, see the Secure Configuration Manager Technical Information web page.

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 "Upgrading Secure Configuration Manager" on page 51.

	Checklist Items
❑	1. Review product architecture information to learn about Secure Configuration Manager components. For more information, see "Understanding the Secure Configuration Manager Architecture" on page 11.
❑	2. Decide the deployment type, and how you want to configure your component installation. For more information, see "Deployment Considerations" on page 17 and "Supported Configurations" on page 20.
❑	3. Ensure that the computers on which you are installing Secure Configuration Manager components meet the specified requirements. For more information, see the following sections: ◆ Chapter 3, "Planning to Install the Databases," on page 23 ◆ Chapter 4, "Planning to Install Core Services," on page 27 ◆ Chapter 5, "Planning to Install the Web and Windows Consoles," on page 29 ◆ Chapter 6, "Planning to Install Security Agents," on page 33 ◆ Chapter 7, "Planning to Install the Dashboard," on page 35
❑	4. Ensure that the user account you use to install Secure Configuration Manager components is a member of the Administrators local group on the computer.

	Checklist Items
❑	5. Ensure that you have SQL Server configured properly to allow Secure Configuration Manager to connect to the database. For more information, see “Installing and Configuring Microsoft SQL Server” on page 24.
❑	6. Install the primary Secure Configuration Manager components. **NOTE:** You can install the Dashboard also while installing Secure Configuration Manager. For more information, see “Installing Core Services, Database, and the Consoles” on page 39.
❑	7. Install the Dashboard. For more information, see Chapter 7, “Planning to Install the Dashboard,” on page 35. **NOTE:** You can install the Secure Configuration Manager Dashboard while installing Secure Configuration Manager.
❑	8. Install or deploy your agents. For more information, see Chapter 9, “Adding or Updating Security Agents,” on page 43.
❑	9. Start the Windows console so you can add additional console users. For more information, see “Starting the Consoles” on page 59.
❑	10. Configure Secure Configuration Manager to work with the agents. For more information, see Chapter 9, “Adding or Updating Security Agents,” on page 43.
❑	11. (Conditional) Deploy the standalone AutoSync client on a separate computer. By default, the AutoSync client is installed along with Secure Configuration Manager components. For more information about deploying the standalone AutoSync client, see “Deploying the Standalone AutoSync Client” on page 41.

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. 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 and network devices that you can manage with Secure Configuration Manager. You can use the **Tools** menu in the Windows console 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 servers, and the expiration date for the licenses.

Secure Configuration Manager requires a license for each of the following managed assets:

Network devices

You must manage these devices with a Windows security agent.

Servers

Multi-user servers, such as a database server, might have both an operating system endpoint and the database endpoint. This includes servers that host SCAP modules or endpoints. Regardless of the number of endpoints, you need a single license for the server.

Workstations

Single-user workstations might have an operating system endpoint and application or database endpoints. This includes workstations that host SCAP modules or endpoints. Regardless of the number of endpoints, you need a single license for the workstation.

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.

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 “Understanding Licensing” on page 16.

As a best practice, NetIQ recommends creating a trial environment similar to your intended production environment. For example, install the database on a separate computer from the Core Services and Windows console computers. However, you can install all components on one computer to run the trial. For more information about selecting the appropriate deployment type, see “Deployment Considerations” on page 17 and “Supported Configurations” on page 20.

Deployment Considerations

You can choose one of the following deployment types based on the size of your IT environment.

All-in-One Deployment

For small enterprises of 50 computers or fewer, you can install all Secure Configuration Manager components on one computer. You can then install additional Windows consoles on other computers as needed. For most console users, you do not need to install the Windows console. Rather, give them the URL to access the Web console from a supported browser.

Distributed Deployment

For larger enterprises, install Core Services, the Dashboard, and the databases on separate computers. The infrastructure for the Web console is installed with Core Services, so most console users simply need the URL to access the Web console from a supported browser. However, you

might want to install the Windows console on additional computers for those console users who need to manage agents and other Secure Configuration Manager components. For more information, see “Recommended Server Setup” on page 18.

NetIQ does not recommend or support installing Secure Configuration Manager components on domain controllers 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.

Multiple Core Services

You also have the option to install Core Services on multiple computers. In this configuration, you can install Core Services and the Secure Configuration Manager database on a computer or install the database on a computer, and install Core Services in other computers and enable them to connect to the database.

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 might be appropriate if your organization needs to maintain a high level of internal security. For more information, see “Multiple Core Services Requirements” on page 28.

Depending on the agents you are deploying, you might be able to share registered agents between Core Services. For more information, see “Working with Multiple Core Services” on page 41

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

Recommended Server Setup

In a typical environment, you might install Secure Configuration Manager on several servers. The following are sample scenarios. Note that the recommendations place the Windows agent on all Windows servers. In most environments, you install the Secure Configuration Manager database on a separate server from the other components.

Scenario 1 - Combining Like Components

Install similar components, such as the databases, on the same server.

Computer setup	Component setup
Server 1	Core Services, includes Web console
	Windows console
	Windows agent
	Dashboard (website infrastructure)
Server 2	Databases ◆ Secure Configuration Manager database ◆ Analytics Database
	Windows agent
Other servers in your environment	Security Agents (UNIX or Windows) and AutoSync Client

Scenario 2 - Partially Distributed Environment

Install the Dashboard components on servers separate from Core Services.

Computer setup	Component setup
Server 1	Core Services, includes Web console
	Windows console
	Windows agent
Server 2	Secure Configuration Manager database
	Windows agent
Server 3	Dashboard components ◆ Dashboard (website infrastructure) ◆ Analytics Database
	Windows agent
Other servers in your environment	Security Agents (UNIX or Windows) and AutoSync Client

Scenario 3 - Fully Distributed Environment

Install Core Services, the Dashboard components, and the databases on separate servers.

Computer setup	Component setup
Server 1	Core Services, includes Web console
	Windows console
	Windows agent

Computer setup	Component setup
Server 2	Secure Configuration Manager database
	Windows agent
Server 3	Dashboard (website infrastructure)
	Windows agent
Server 4	Analytics Database
	Windows agent
Other servers in your environment	Security Agents (UNIX or Windows) and AutoSync Client

Supported Configurations

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 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 Windows console, Core Services, and database.

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 *User's Guide for Secure Configuration Manager* and the security agent guides.

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.

Port Number	Component Computer	Port Use
1433	Database	Used by Microsoft SQL Server if you are using a default instance of SQL Server. This port is also used by the Windows console to listen for communication from the database. When used by Core Services, the port uses bi-directional communications to communicate with the Windows console and the database.
1621	Core Services	Used by Core Services to listen for communication from the Windows agent or standalone AutoSync server when both the agent or standalone AutoSync server 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	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 and UNIX 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 Windows console computer. This port uses bi-directional communications.
8044	Web Server	Used by the Web server that is embedded in Core Services, which supports the Web console. 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. **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.
TCP 8045	Dashboard	Used by the Dashboard infrastructure for communication with the Dashboard Website.
TCP 8044	Core Services computer	Used by the Dashboard for communication with the Secure Configuration Manager Core Services computer.
TCP 9200	Analytics Database	Used by the Dashboard for communication with Dashboard Database using its REST services.
TCP 9300	Analytics Database	Used by the Dashboard for communication with Dashboard Database using its native protocol.

NOTE: If you have used non-default ports for the Analytics Database, Dashboard, and Core Services computers, ensure that those ports are open.

3 Planning to Install the Databases

This section provides requirements, recommendations, and configuration information for the Secure Configuration Manager database and the Analytics Databse computers. The Dashboard and the Web console use the Analytics Database to display assessment results.

NOTE: The size of your Secure Configuration Manager database and the number of concurrent connections can affect performance of the consoles.

Database Computers Requirements

The following sections lists the requirements for the database computers. This section assumes that you will install the databases on separate computers.

For the most recent recommendations, see the NetIQ Secure Configuration Manager Technical Information web page.

Calculating the Size of the Database

To estimate the potential size of the Secure Configuration Manager database, use the following calculation:

security checks x *endpoints* x *policy templates* x (1440/*timeframe*) x 0.000004

where

Security checks

Represents the total number of security checks in the policy templates scheduled to run in the timeframe

Endpoints

Represents the number endpoints that will be assessed in the timeframe

Policy templates

Represents the number of jobs with policy templates scheduled to run in the timeframe

Timeframe

Represents the total number of minutes during which you will run the assessments

This calculation assumes that you have 500 to 1,000 endpoints.

Requirements Table

Category	Minimum and Recommended Requirements
Memory	8 GB for Secure Configuration Manager database
	6 GB for Analystics Database
Processor	8 GHz for Secure Configuration Manager database
	4 GHz for Analystics Database
Free disk space	200 GB for Secure Configuration Manager database
	100 GB for Analystics Database
Microsoft SQL Server	One of the following versions: ◆ 2016 ◆ 2014 ◆ 2012 SP2 ◆ 2008 R2
Ports	See the ports information in “Default Ports” on page 20.

Using the Database in a Cluster Environment

You can install the Secure Configuration Manager 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.

If you are installing the Secure Configuration Manager in a distributed environment or in a cluster environment, ensure the following:

- You have write permissions to the data and log file locations of the SQL Server data directory.
- A DNS Resolve method is present that queries a DNS server for the IP address associated with a host name or vice-versa.

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 Computers Requirements” on page 23.

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

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.

- "Configuring the SQL Server Browser Service" on page 25
- "Configuring the SQL Server TCP/IP Protocol" on page 25

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**.

4 Planning to Install Core Services

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

Considerations for Installing Core Services

Before installing Core Services, review the following considerations:

- The installation process for Core Services includes the infrastructure for the Web console.
- The installation 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*.
- 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.
- 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.
- 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.

For more information about your server setup, see "Deployment Considerations" on page 17.

Core Services Computer Requirements

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

Category	Minimum Requirements
Memory	6 GB
Processor	4 Ghz or faster
Free disk space	100 GB

Category	Minimum Requirements
Operating system	One of the following versions: ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2008 R2 ◆ Windows Server 2008 (32-bit)
Microsoft Excel	To distribute reports in .xls format, Microsoft Excel must be installed on the Core Services and Windows console computers. One of the following versions: ◆ 2016 ◆ 2013 ◆ 2010
Ports	See the ports information in “Default Ports” on page 20.

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 might need to complete an additional step to enable multiple Core Services to communicate with registered agents.

Windows and UNIX 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 “Working with Multiple Core Services” on page 41.

5 Planning to Install the Web and Windows Consoles

This section provides the software and permissions requirements for the computer supporting the Web and Windows Secure Configuration Manager consoles.

Considerations for Installing the Consoles

Before installing the consoles, review 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 *User's Guide for Secure Configuration Manager*.
- When you install Core Services, the installation process includes the infrastructure for the Web console. You do not need to perform a separate installation.
- You must install a Windows console on the Core Services computer.
- Secure Configuration Manager supports IPv4 and IPv6 addresses, but uses IPv4 addresses for communication among the consoles, Core Services, and the Secure Configuration Manager database. The Windows console computer must be configured for IPv4 addresses at a minimum. Alternatively, you can set up the Windows console computer as a dual-stack host to support both IPv4 and IPv6 addresses.
- You can allow Web console users to launch the Dashboard without re-entering their credentials. For more information, see "Enabling the Web Console to Launch the Dashboard" on page 46.

For more information about your server setup, see "Deployment Considerations" on page 17.

Web Console Requirements

The following table lists the requirements for running the Web console. For the most recent recommendations, see the NetIQ Secure Configuration Manager Technical Information web page.

Category	Minimum Requirements
Web browser	Latest version of the following: ◆ Google Chrome ◆ Microsoft Edge ◆ Microsoft Internet Explorer ◆ Mozilla Firefox

Category	Minimum Requirements
Analytics Database	Analytics Database (NetIQDatabaseService) service, which is provided in installation program for the Secure Configuration Manager Dashboard. To ensure that the Web console functions appropriately, install the Dashboard in your environment and connect it to Core Services. For more information, see Chapter 7, “Planning to Install the Dashboard,” on page 35.

Windows Console Computer Requirements

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

Category	Minimum and Recommended Requirements
Memory	6 GB
Processor	2 Ghz or faster
Free disk space	100 GB
Operating system	One of the following versions: ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2008 R2 ◆ Windows Server 2008 (32-bit) ◆ Windows 10 ◆ Windows 8.1 ◆ Windows 7 (64-bit)
MDAC	2.6 or later
Microsoft .NET Framework (for distributing reports)	4.6.1
Microsoft Excel	To distribute reports in .xls format, Microsoft Excel must be installed on the Core Services and Windows console computers. One of the following versions: ◆ 2016 ◆ 2013 ◆ 2010
Microsoft XML Parser	3.2

Category	Minimum and Recommended Requirements
Usage permissions	The Windows user account you use to run the Windows console must be one of the following: ◆ Member of the local Administrators group ◆ Account with write permissions to the `NetIQ\Secure Configuration Manager` folder and its subfolders If you are running the Windows 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.

6 Planning to Install Security Agents

This chapter provides information about installing the security agents.

Supported Agent Versions

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

Agent Computer Requirements

In Secure Configuration Manager, **platform** represents the type of endpoint. The requirements for agent computers vary depending on the platform.

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	*Secure Configuration Manager Windows Agent Installation and Configuration Guide*
UNIX and Linux	*Installation and Configuration Guide for NetIQ Security Agent for UNIX*

7 Planning to Install the Dashboard

This section provides requirements, details of supported configurations, and other information necessary for planning installation of the Secure Configuration Manager Dashboard.

Dashboard Computer Requirements

This section provides hardware, software, and permissions requirements for the Dashboard's website component. For more information about the requirements for the Analytics Database component, see "Database Computers Requirements" on page 23.

For the most recent recommendations, see the NetIQ Secure Configuration Manager Technical Information web page.

Category	Minimum and Recommended Requirements
Memory	8 GB
Processor	2 GHz or faster
Free disk space	100 GB
Operating system	One of the following versions: ◆ Windows Server 2016 ◆ Windows Server 2012 R2
Web browser	Latest version of the following versions: ◆ Google Chrome ◆ Microsoft Edge ◆ Microsoft Internet Explorer ◆ Mozilla Firefox
Ports	See the ports information in "Default Ports" on page 20.
Analytics Database	For more information, see "Database Computers Requirements" on page 23

Considerations for Installing the Dashboard

Before installing the Dashboard, review the following considerations:

- When you install the Dashboard, you must install the following components:
  - Dashboard infrastructure, which enables display in a Web browser
  - Analytics Database, which communicates with Core Services and the Secure Configuration Manager database to compile the results of assessments displayed in the Web console and Dashboard
- The user account you use to install the Dashboard must be a member of the Administrators local group on the computer.
- Web console users can launch the Dashboard without having to re-enter their credentials. To support a single sign-on process, provide one of the following scenarios in your environment:
  - Install the Dashboard on the Core Services computer. The Analytics Database component can be on a separate server. This scenario negates the need for specifying the Dashboard settings in the Web console.
  - In the Web console, specify the **Port** and the IP address or name of the Dashboard's **Host** server. This assumes that the Dashboard is installed in the same domain as Core Services.

  To support single sign-on between the Web console and the Dashboard, both URLs must use either an IP address or a host name. That is, if you specify a host name for the Dashboard's **Host** server, then you must also use a host name in the URL for the Web console. For example, `https://testing.company.com:8044/scm` and `https://testing.company.com:8045/dashboard`.

  If you install the Dashboard in a separate domain from Core Services, this single sign-on feature cannot function.

For more information about your server setup, see "Deployment Considerations" on page 17.

II Installing or Upgrading Secure Configuration Manager

This section provides instructions for installing or upgrading Secure Configuration Manager. For more information about a specific release, see the Release Notes.

8 Installing Secure Configuration Manager

This chapter provides guidance for determining the appropriate installation type and outlines the installation steps.

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 “Understanding Licensing” on page 16.
❑	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 “Implementation Checklist” on page 15.
❑	4. Install Secure Configuration Manager. For more information, see “Installing Core Services, Database, and the Consoles” on page 39.
❑	5. Install your agents. For more information, see Chapter 9, “Adding or Updating Security Agents,” on page 43.
❑	6. Run the AutoSync update service to download the latest security checks and policy templates. For more information, see “Updating Security Knowledge” on page 53.

Installing Core Services, Database, and the Consoles

The installation process creates an summary file, `C:\Program Files (x86)\NetIQ\Secure Configuration Manager\installconfig.txt`, which contains all the values you specify for installation parameters. You can use this file later for reference.

To install Core Services, database, and the consoles:

1. Log in as an administrator to the computer where you want to install the Secure Configuration Manager components. Ensure that the account you are using has write permissions to the installation directory.
2. Exit all programs on the computer.
3. Run the setup program, `Setup.exe`, from the root folder of the Secure Configuration Manager installation kit.
4. Click **Start Installation** to start the installation.

   Follow the instructions in the wizard to proceed with the installation.
5. (Optional) By default, the Core Services service runs using the local system account. If you want to specify a different service account, complete the following steps:
   - **5a** In the **Service Account** field, type the user name of the account you want to assign to the Core Services service.
   - **5b** In the **Password** field, type the password for the specified service account.
   - **5c** If you want to use a non-default port for Core Services, deselect the **Use Default Port** option, and specify the port in the **Core Port** field.
   - **5d** Click **Next**.

     The setup wizard validates the specified service account.
6. (Optional) To specify the SQL server connection, complete the following steps:
   - **6a** Specify the server name.
   - **6b** Specify the port number in the **Database Port** field if you want to use a non-default port.
   - **6c** Select the type of authentication you want use to connect to the SQL Server database. Provide user name and password if you select SQL authentication.
   - **6d** Click **Next**.

     The setup wizard validates the specified SQL server connection.
7. (Optional) By default, the Windows agent service runs using the local system account. If you want to specify a different service account, complete the following steps:
   - **7a** 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.

   - **7b** In the **Password** field, type the password for the specified service account.
   - **7c** Click **Next**.

     The setup wizard validates the specified service account.
8. Review the installation summary, and click **Install**.

   The silent installation process begins for Core Services, the database, and the Web console, and then automatically continues with installing the Windows agent followed by the Dashboard.
9. (Optional) Install the Dashboard.

   If you do not want to install the Dashboard on the current server, click **Cancel** when prompted.

   For more information about the Dashboard installation, see Chapter 10, “Installing the Dashboard,” on page 45.

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 and UNIX 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 following folders:
   - **32-bit systems:** `C:\Program Files\NetIQ\Secure Configuration Manager\Core Services\bin`
   - **64-bit systems:** `c:\Program Files (x86)\NetIQ\Secure Configuration Manager\Core Services\bin`
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 Windows console to see the registered agents.

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 *User's Guide for Secure Configuration Manager*.

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.

- “Installing the Standalone AutoSync Client” on page 42
- “Configuring the Standalone AutoSync Client” on page 42

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. Run the setup program from the root folder of the Secure Configuration Manager installation kit.
3. On the Component Selection window, select *only* the **Standalone AutoSync Client** component.
4. Follow the instructions in the wizard until you finish installing the standalone AutoSync client.

Configuring the Standalone AutoSync Client

After 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 *User's Guide for Secure Configuration Manager*.

9 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.

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 more information about the requirements for and capabilities of UNIX agents, see the *NetIQ Security Agent for UNIX*.

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, Network Attached Storage (NAS), and network device 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 Secure Configuration Manager Windows Agent Installation and Configuration Guide*.

10 Installing the Dashboard

You can install the Dashboard in one of the following two ways:

- As part of the overall Secure Configuration Manager installation or upgrade. For more information, see “Installing Core Services, Database, and the Consoles” on page 39.
- As a standalone installation with a Dashboard-only `.msi` file. This process requires an existing installation of Secure Configuration Manager.

Using the Standalone Installation Program for the Dashboard

To install the Dashboard on computers other than the Core Services or Windows console computers, you might want to use the standalone installation program.

1. Copy the Dashboard installer, `NetIQDashboard.msi`, from the Secure Configuration Manager installation kit to the computer where you want to install the Dashboard

   ---

   NOTE: If you have the Secure Configuration Manager installation setup in the computer where you want to install the Dashboard, you can also click **Install Dashboard** after you run the Secure Configuration Manager **Setup.exe**.

   ---

2. Run the `NetIQDashboard.msi` setup program.
3. In the NetIQ Secure Configuration Manager Dashboard Setup window, click **Next**.
4. Select the Dashboard components that you want to install. By default, both the Website and Database components are installed in the local hard drive, in the `C:\Program Files(x86)\NetIQ\Secure Configuration Manager\Dashboard` folder.
5. Click **Next**.
6. Provide or verify the following settings:
   - **Cluster Name**: Name of the Dashboard cluster for database configuration.
   - **Database Port**: Port used for communication with Dashboard Database. Default port is 9200.
   - **Website Port**: Port used for communication with Dashboard Website. Default port is 8045.
   - **Core Host Name**: IP address or name of the Secure Configuration Manager Core computer.

     This value is auto-populated if you are installing the Dashboard on a computer in which Secure Configuration Manager is already installed. Specify the host name if you are installing the Dashboard on a different computer.
   - **Core Port**: Port used for communication with Secure Configuration Manager Core computer. Default port is 8044.
   - **Protocol**: Select the type of protocol for communication between Secure Configuration Manager Core computer and the Dashboard.

NOTE: If you are installing the Dashboard in a distributed environment, and have selected only one of the components (either Website or Database), you will be prompted to specify the configuration information for only that component.

7 (Optional) Click **Test Connection** to test the connection with the specified Secure Configuration Manager Core computer IP address/name.

When you click **Next**, the program verifies connection with the specified Secure Configuration Manager Core computer. Installation proceeds only if the connection is established.

8 Click **Next**.

9 Review the installation summary, and click **Install** to start the installation.

Customizing the Installation

After installing the Dashboard, you can customize your installation by changing the default settings. To customize the Dashboard installation:

1 Go to the directory where you have installed the Dashboard. By default, the Dashboard is installed in the `C:\Program Files (x86)\NetIQ\Secure Configuration Manager\Dashboard` directory.

2 (Conditional) To customize the Analytics Database, go to the `Database\config` directory and open the `db.properties` file. You can change the protocol, Database port, and the Core computer name in this file.

Save the file.

3 (Conditional) To customize the Dashboard Website, go to the `Website` directory and open the `website.properties` file. You can change the Website protocol, Website port, Database protocol, and the Database port in this file.

Save the file.

4 Restart the **Elasticsearch 2.0.0 (NetIQDatabaseService)** and the **NetIQ Dashboard Website Service**, in that order.

Enabling the Web Console to Launch the Dashboard

If you install the Dashboard on the same server as the Core Services computer, users can launch the Dashboard from the Web console without having to re-enter their Dashboard credentials.

If the Dashboard resides on a separate computer from Core Services, update the Dashboard settings in the Web console to support single sign-on: Go to **Your_ID > Settings > Dashboard**.

For more information, see “Considerations for Installing the Dashboard” on page 36 and “Enabling Users to Launch the Dashboard” in the Help for the Web console.

11 Upgrading Secure Configuration Manager

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

Secure Configuration Manager Upgrade Checklist

Upgrade your Secure Configuration Manager installation using the following checklist.

	Checklist Items
❑	1. Review the latest Release Notes. For more information, see the Secure Configuration Manager documentation.
❑	2. Review the notes and considerations regarding the upgrade process. For more information, see "Considerations for Upgrading" on page 48.
❑	3. Back up the Secure Configuration Manager configuration data. For more information, see "Backing Up Configuration Data" on page 49.
❑	4. Close all Secure Configuration Manager consoles and shut down Core Services. For more information, see "Preparing to Upgrade" on page 49.
❑	5. (Conditional) If you are upgrading the Dashboard, ensure that all user sessions are closed.
❑	6. Using Microsoft SQL Server Enterprise Manager, ensure that no users are connected to the Secure Configuration Manager database. **IMPORTANT:** Before beginning to upgrade Secure Configuration Manager, close all the windows that are open against Vigilent database in SQL Server Management Studio.
❑	7. Back up your Secure Configuration Manager database. For more information, see the Microsoft SQL Server documentation.

	Checklist Items
❑	8. Ensure that the computers on which you want to upgrade Secure Configuration Manager components meet the specified requirements. For more information, see Part I, “Planning to Install Secure Configuration Manager,” on page 13.
❑	9. Stop all pending and scheduled jobs. For more information, see “Stopping Scheduled Jobs Before Upgrade” on page 51.
❑	10. 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 “Upgrading Secure Configuration Manager” on page 51.
❑	11. Upgrade each Windows console computer. Secure Configuration Manager displays a message if you attempt to log in to the Web or Windows console before the database upgrade process completes. For more information, see “Upgrading Secure Configuration Manager” on page 51 and the Release Notes.
❑	12. Restore all the Secure Configuration Manager data. For more information, see “Recovering Configuration Data” on page 55.
❑	13. Run the AutoSync update service to download the latest security checks and policy templates. For more information, see “Updating Security Knowledge” on page 53.
❑	14. Check the Micro Focus 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.
❑	15. (Conditional) If you do not have the latest version of an agent, download the appropriate software update from the web site and use the instructions provided in the installation kit to upgrade the agent or see “Updating Agent Content” in the *User's Guide for Secure Configuration Manager*.
❑	16. (Conditional) Upgrade the Dashboard, if it is on a separate server than the Core Services computer. For more information, see “Upgrading the Dashboard” on page 53.

Considerations for Upgrading

Before upgrading any Secure Configuration Manager components, review the following considerations:

- The upgrade process does not support upgrades from previous trial installations.
- When you upgrade Core Services, the process also upgrades the Web console and Secure Configuration Manager database as needed.

- The Web console requires the Analytics Database, which is a component of the Dashboard. Before you log in to the Web console, ensure that the Analytics Database has been installed or upgraded to the appropriate version. Use the `setup.exe` or `NetIQDashboard.msi` file for the Dashboard.
- 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.

Preparing to Upgrade

Before upgrading, you might want to back up the configuration settings for Secure Configuration Manager. You can also shut down running processes and ensure that users are not logged into the consoles or Dashboard.

- "Backing Up Configuration Data" on page 49
- "Preparing Your Environment for Upgrade" on page 50
- "Stopping Scheduled Jobs Before Upgrade" on page 51

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`.

Preparing Your Environment for Upgrade

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

1 Verify that the version of Secure Configuration Manager currently running in your environment is supported by the upgrade process. For more information, see "Secure Configuration Manager Upgrade Checklist" on page 47.

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.

Stopping 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.

Stopping Pending Jobs

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

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

Preventing Jobs from Starting

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**.

Upgrading Secure Configuration Manager

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

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 “Preparing Your Environment for Upgrade” on page 50.

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 Overview,” on page 15 and Step 6 on page 50 of “Preparing Your Environment for Upgrade” on page 50.

3 To upgrade Core Services, Web console, and the Secure Configuration Manager database, complete the following steps:

3a Log in 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.exe`, located by default in the `CDImage` directory 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.

3e Click **Upgrade**.

3f Follow the instructions in the wizard until you have finished upgrading the product.

3g (Conditional) For the **Dashboard Installation Requirement** page, if the Dashboard is not installed in your environment, you can either specify the IP address and host for the server where you plan to install the Analytics Database or click **Next** without entering values.

If you do not enter values, you can specify the settings after you install the Dashboard. Otherwise, the Web console will not function appropriately. For more information, see the Help for the Web console or "Configuring the Web Console" in the *User's Guide for Secure Configuration Manager*.

3h (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 *Secure Configuration Manager Windows Agent Installation and Configuration Guide*.

3i 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 Windows consoles, complete the following steps on each console computer:

4a Log in to the console computer with an administrator account.

NOTE: You must wait until the database upgrade completes before you can log in 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 Upgrade the Dashboard. Click **Cancel** when prompted if you do not want to upgrade the Dashboard on the current server.

6 When 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 "Updating Security Knowledge" on page 53 and the *User's Guide for Secure Configuration Manager*.

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.

Upgrading the Dashboard

You can upgrade the Dashboard in one of the following two ways:

- Upgrading the Dashboard along with Secure Configuration Manager

  You can upgrade the Dashboard while upgrading the Secure Configuration Manager version.
- Standalone upgrade of the Dashboard

To upgrade the standalone installation of the Dashboard:

1 Log out of all the Dashboard user sessions, and close the browser windows.

2 Copy the Dashboard installer, `CDImage\Intel\Deployment\Dashboard\NetIQDashboard.msi`, to the computer where you want to upgrade the Dashboard.

3 Double-click `NetIQDashboard.msi` to run the upgrade wizard.

4 Click **Next**.

5 Click **Upgrade** in the Installation Summary dialog box to start the upgrade.

6 Click **Finish**.

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 *User's Guide for Secure Configuration Manager*.

NOTE: Secure Configuration Manager downloads, but does not update, patch level database files during this process. For more information, see "Agent Considerations" on page 54 and the *User's Guide for Secure Configuration Manager*.

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.

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.

- “Windows Agent” on page 54
- “UNIX Agent” on page 55

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 *User's Guide for Secure Configuration Manager* and the *Secure Configuration Manager Windows Agent Installation and Configuration Guide*.

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 "Deploying UNIX Agents" on page 43, and the *Installation and Configuration Guide for NetIQ Security Agent for UNIX*.

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`.

---

12 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 consoles and Core Services.

Getting Started Checklist

This chapter guides you through the process of getting started with Secure Configuration Manager.

	Checklist Items
❑	1. (Optional) Configure Windows authentication for communication between Core Services and the database. For more information, see "Configuring Windows Authentication between Core Services and the Database" on page 58.
❑	2. Start Core Services. For more information, see "Starting Core Services" on page 58.
❑	3. Start the Windows console to connect to Core Services and set up additional users. For more information, see "Starting the Windows Console" on page 59.
❑	4. Start the Web console to connect to Core Services and the Dashboard. For more information, see "Starting the Web Console" on page 59.
❑	5. (Optional) Configure SQL authentication between the consoles and the database. For more information, see "Configuring SQL Authentication between the Database and the Consoles" on page 60.
❑	6. Configure the Dashboard. For more information, see "Configuring the Dashboard" on page 60.

Configuring Windows Authentication between Core Services and the Database

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.

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.

Starting Core Services

Core Services handles communication between the consoles 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.

Starting the Consoles

When you start Secure Configuration Manager for the first time after installation, log in to the Windows console first. 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 in to either console.

By default, Secure Configuration Manager uses Windows authentication for communication between the consoles 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 in to the console computer are allowed to use the database through Core Services.

You can also use SQL authentication. For more information, see "Configuring SQL Authentication between the Database and the Consoles" on page 60.

Starting the Windows Console

1. Start Secure Configuration Manager from the NetIQ Secure Configuration Manager program folder.
2. In the **Core Services** field, select the computer that hosts the Core Services that 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**.

Starting the Web Console

The Web console works in most browsers so your users can access Secure Configuration Manager from anywhere. The installation process supplies the URL address, including the Core Services port. For example, `162.99.123.45:8044/scm`.

For more information about supported browsers, see "Web Console Requirements" on page 29.

Configuring SQL Authentication between the Database and the Consoles

You can also use SQL authentication for communication between the consoles 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.

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 Windows 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**.

Configuring the Dashboard

The installation process configures the Dashboard so you can log in immediately. However, you might want to set up the Dashboard to perform in a distributed environment or customize settings.

In most environments, you can launch the Dashboard from the Web console. For more information, see "Launching the Dashboard from the Web Console" in the *User's Guide for Secure Configuration Manager*.

- "Configuring the Dashboard for a Distributed Environment" on page 60
- "Customizing the Dashboard Settings" on page 61

Configuring the Dashboard for a Distributed Environment

If you have installed the Dashboard in a distributed environment, you must configure **unicast discovery**. For more information about unicast discovery, see the Elasticsearch documentation. You must perform the following procedure on both the Dashboard website and Secure Configuration Manager Database host computers.

1. Open the `elasticsearch.yml` file, by default in the `C:\Program Files (x86)\NetIQ\Secure Configuration Manager\Dashboard\Database\config\` directory.
2. Uncomment the following line:

```
# discovery.zen.ping.unicast.hosts: ["host1", "host2"]
```

3 In the above line, add the IP addresses of the Dashboard website and Database hosts that you want to add for unicast discovery.

   For example:

   ```
   discovery.zen.ping.unicast.hosts: ["255.0.0.0", "127.0.0.1"]
   ```

4 Save the `elasticsearch.yml` file.

5 Restart the **Elasticsearch 2.0.0 (NetIQDatabaseService)** service.

Customizing the Dashboard Settings

After installing the Dashboard, you can change the default settings.

1 Go to the directory where you have installed the Dashboard, by default in the `C:\Program Files(x86)\NetIQ\Secure Configuration Manager\Dashboard` directory.

2 (Conditional) To change the properties for the Dashboard, complete the following steps:

   2a Open the `db.properties` file, by default in the `Database\config` directory.

   2b Change the protocol, Database port, and the Core computer name in this file.

   2c Save the file.

3 (Conditional) To customize the Dashboard Website, complete the following steps:

   3a Open the `website.properties` file, by default in the `Website` directory.

   3b Change the Website protocol, Website port, Database protocol, and the Database port in this file.

   3c Save the file.

4 Restart **Elasticsearch 2.0.0 (NetIQDatabaseService)**.

5 Restart **NetIQ Dashboard Website Service**.